ISSN: 2633-4828 Vol. 6 No.1, January, 2024

International Journal of Applied Engineering & Technology

AN IMPROVED MODEL WITH EHT FOR IMAGE FORGERY DETECTION USING MATLAB

B.B Shabarinath[1], Pradeep Kumar[2] and K Akhila[3]

[1,2]Assistant Professor, Department of ECE, VNR Vignana Jyothi Institute of Engineering andTechnology, Hyderabad, India -500090

[3]M.Tech Student, Embedded Systems, VNR Vignana Jyothi Institute of Engineering andTechnology, Hyderabad, India -500090

ABSTRACT

The contemporary era of digital technology has witnessed a significant increase in instances of image forgery, primarily attributed to the widespread availability and utilization of image alteration tools. This concerning trend has resulted in a compromised sense of authenticity and credibility around visual information. The present study introduces a novel methodology for the reliable and precise identification of manipulated images through the utilization of an Ensemble Hybrid Tree (EHT) algorithm. The EHT method combines the capabilities of many tree-based classifiers in order to improve the accuracy of detection and the ability to withstand different tampering approaches. The initial phase of the proposed method involves utilizing a comprehensive dataset consisting of a wide range of genuine and altered photos. This dataset encompasses many forms of image forgeries, including copy-move, splicing, and retouching techniques. Utilizing the provided dataset, the EHT algorithm combines a fusion of decision trees, random forests, and gradient boosting methodologies. Every classifier that is based on tree algorithms is designed to excel in detecting particular patterns of fraud and inconsistencies that are caused by various tampering techniques. In order to improve the precision and dependability of forgery detection, a novel ensemble technique is proposed. This strategy involves combining the results of individual classifiers based on tree models through a weighted voting mechanism. The integration of these findings successfully reduces the occurrence of both false positives and false negatives, leading to a more precise and inclusive procedure for detecting forgeries. The proposed method not only prioritizes the examination of individual pixels but also integrates feature extraction algorithms that capture more complex patterns and textures that are suggestive of different tampering strategies. The utilization of multi-level analysis enhances the system's adaptability in identifying various forms of picture manipulation, encompassing both rudimentary and sophisticated forgeries, such as deepfake material.

Keywords:Image forgery detection, Ensemble Hybrid Tree (EHT) algorithm, Copy-move forgery, Splicing detection, Retouching identification, Decision trees Random forests,Gradient boosting, Weighted voting mechanism, Feature extraction algorithms, Multi-level analysis, Deepfake detection, Tampering approaches, False positives and false negatives, Visual authenticity.

INTRODUCTION

In the ever-evolving landscape of digital imagery, the integrity of visual content has become a critical concern, particularly with the rise of sophisticated image manipulation techniques. One prevalent form of image forgery, known as copy-move forgery, involves the replication and relocation of specific portions within a single image, challenging the authenticity of visual evidence. As images play a crucial role in various domains such as forensics, law, and communication, the detection of these manipulations has garnered significant attention. Copy-move forgery presents a formidable challenge due to its intricate nature, making it difficult to distinguish manipulated regions from the authentic parts of an image. The repercussions of undetected forgeries are substantial, with potential consequences in legal proceedings, medical diagnoses, and information dissemination. Detecting these forgeries has prompted the development of innovative methodologies and technologies aimed at safeguarding the veracity of digital images. This introduction sets the stage for exploring diverse approaches to copy-move forgery detection, ranging from traditional block-based techniques to more advanced methods incorporating deep learning and statistical analysis. As we delve into the intricacies of these methodologies, the

overarching goal is to provide a comprehensive understanding of the evolving landscape in the realm of digital image forensics, particularly in the context of combating the challenges posed by copy-move forgery.

This research presents the introduction of a novel end-to-end deep neural network for the prediction of forgery masks in the context of picture copy-move forgery detection. In this study, a convolutional neural network is used to extract block-like characteristics from an image. Subsequently, self-correlations are computed between various blocks, and a pointwise feature extractor is utilised to identify matching points. Finally, a forgery mask is reconstructed by the implementation of a deconvolutional network. In contrast to traditional approaches that need numerous phases of training and parameter adjustment, which include feature extraction and postprocessing, the suggested method is entirely trainable and can be optimised simultaneously for the loss associated with reconstructing the forgery mask. The experimental findings presented in this study indicate that the suggested methodology outperforms traditional techniques that depend on distinct features and matching schemes in terms of forgery detection performance. Furthermore, the proposed method exhibits enhanced resilience against a range of well-known assaults, including affine transformation, JPEG compression, blurring, and others.

PROBLEM STATEMENT:

The advancement of image counterfeiting techniques has presented a substantial obstacle to the credibility and reliability of visual data. The swift progression of image alteration tools and techniques necessitates the development of a comprehensive and precise image forgery detection system that can effectively recognize many types of tampering. The objective of this project is to develop and execute a novel image forgery detection methodology that can proficiently identify and categorize various forms of image alterations, including copy-move forgery, splicing, retouching, and deepfake generation. This research endeavors to address the dynamic complexities associated with image fraud, with the objective of offering a helpful resource to digital forensics professionals and the wider society in the verification of image authenticity within an ever-expanding digital landscape.

OBJECTIVES:

1. Develop a robust methodology for the identification of manipulated images: The study aims to design and implement an effective algorithm, specifically the Ensemble Hybrid Tree (EHT) algorithm, to reliably detect various forms of image forgery, including copy-move, splicing, and retouching techniques.
2. Enhance detection accuracy and reliability: By combining the strengths of decision trees, random forests, and gradient boosting methodologies within the EHT algorithm, the study aims to improve the precision and dependability of forgery detection. This involves addressing the challenges posed by different tampering approaches and minimizing both false positives and false negatives.
3. Incorporate feature extraction for complex pattern analysis: The proposed method goes beyond pixel-level examination and integrates feature extraction algorithms to capture intricate patterns and textures indicative of diverse tampering strategies. This multi-level analysis is expected to enhance the adaptability of the system in identifying both rudimentary and sophisticated forms of picture manipulation, including emerging threats like deepfake content.

SUMMARY:

In summary, this research introduces an innovative and efficient approach for detecting image counterfeiting through the utilization of ensemble techniques and hybrid tree-based classifiers. The suggested solution aims to enhance the credibility and integrity of digital visual information in an era where trust in digital media is of utmost importance by tackling the ever-changing issues associated with image manipulation.

RELATED WORK:

2023

One often-used biometric technique in the field of document forensics is the authentication of handwritten signatures to confirm an individual's identification. The use of signatures has significant importance within the

realms of banking, finance, commerce, and related domains. Nevertheless, there are various complications related to signatures, since it is possible for two signatures to seem extremely identical with little or no discernible changes, even if they are written by the same individual. Despite extensive research endeavours, offline signature verification remains challenging, particularly in distinguishing between skilled forgeries and genuine signatures. This difficulty arises from the fact that the visual distinctions between these two categories might sometimes be less discernible than those between two genuine signatures. The growing use of digital signatures and electronic documents has led to a heightened need for efficient and accurate systems that can detect fraud in signatures. This project aims to develop an automated system that uses a deep neural network, namely a Convolutional Neural Network (CNN), to efficiently address the issue of handwritten signature fraud. The system will be designed to accurately distinguish between genuine and counterfeit signatures [1].

The proposed model uses signature images as input and employs several layers of convolutional neural networks (CNN) to extract significant characteristics. These extracted features play a crucial role in differentiating between authentic and counterfeit signatures. The evaluation of the model's performance is also conducted by using various picture scaling algorithms and optimizers during the training of the Convolutional Neural Network (CNN). This work presents the evaluation of the model's performance using a comprehensive set of assessment measures, including accuracy, precision, recall, and F1-score. The evaluation was done on a large dataset of handwritten signatures, including both genuine and different forms of forged signatures. Furthermore, the performance of the model is also compared to that of a state-of-the-art deep learning model. The simulation findings provide strong evidence supporting the suitability of the proposed approach for the automated detection of fraud in handwritten signature photographs [2].

The prevalence of picture fraud has escalated due to the growing utilisation of digital photographs across diverse applications. This research presents a unique approach for detecting picture forgeries using Convolutional Neural Networks (CNNs). The proposed system is capable of identifying several forms of image alterations, such as copy-move, splicing, and retouching. The suggested method aims to enhance the accuracy and reliability of picture fraud detection by integrating Error Level Analysis (ELA) with deep learning techniques. The suggested system was assessed using a dataset consisting of real-world photographs, resulting in a detection accuracy of 93%. The performance of our system surpassed that of current approaches in the field of picture forgery detection, showcasing its promise for a wide range of applications such as forensics, security, and digital image analysis. In general, the suggested convolutional neural network (CNN)-based system for detecting picture fraud presents a resilient and efficient resolution to the escalating issue of image alteration and forgery in the contemporary visual media environment [3].

Picture forgery encompasses a range of manipulations performed on an original picture, resulting in a distortion of its intended meaning and the dissemination of false information. Furthermore, in the contemporary period characterised by the pervasive influence of social media and the ubiquitous presence of pictures, individuals have developed a propensity to place unwavering trust in visual representations. Consequently, this phenomenon has emerged as a pressing issue that demands a resolution. Numerous methods exist for the detection of picture fraud. In this study, we have shown two primary methodologies for detecting forgeries via the use of resampling methods. Resampling serves as a crucial indicator for identifying manipulated photos. In order to detect and localise picture alterations, two distinct methodologies have been developed. These methodologies include the use of resampling techniques, which entail the creation of diverse samples and the implementation of numerous essential processes. The first methodology involves calculating the radial transform of the aforementioned characteristics over overlapping picture segments. Subsequently, a heatmap is constructed by using deep learning classifiers and a Gaussian random variable, which serves as a model for the conditional probability values. The Random Walker segmentation technique is used for the purpose of identifying tampered parts. The second approach involves using an LSTM-based network to broadcast resampling features that have been calculated on intersecting image patches with the purpose of categorising and identifying local tampered areas. The detection and localization performance of both systems were compared, revealing their effectiveness in identifying and

locating picture forgeries across various levels. The study's findings indicate that both strategies exhibit a high degree of efficiency in this regard [4].

The proliferation of image alteration has emerged as a prevalent issue in the realm of digital photography in recent times. The three fundamental forms of image forgeries discussed include the identification of copy-move picture forgeries, image splicing, and recolouring. The dataset used for the identification of copy-move photos is referred to as MICC-220. This dataset has a total of 220 photographs, each exhibiting diverse lighting conditions and camera settings. This research employs many methodologies and models, such as the Scale-invariant feature transform, the DBSCAN algorithm for copy-move picture identification, and the deep architecture of a convolutional neural network, to effectively detect recolored photos. The dataset used for the purpose of detecting picture splicing is the CASIA V2 dataset, which includes a total of 4795 photographs. This dataset is used to categorise manipulated images and identify various forms of image tampering. Furthermore, the use of Image Error Level Analysis, a method for compressing photos, is combined with the implementation of a convolutional neural network in order to accurately detect any modifications made to the images [5].

Digital image forgery (DIF) is the term used to describe the act of modifying pictures without proper authority. The process of digital manipulation has become quite straightforward in contemporary times. The detection of picture forgeries encompasses two main categories: copy-move forgery and image splicing forgery. These study subjects are primarily concerned with identifying instances of image manipulation, such as copy-move forgery or image splicing forgery, which involves the duplication and relocation of image regions. The act of duplicating a portion of an input picture and then overlaying it onto another region within the same digital image is sometimes referred to as copy-move forgery. Splicing is a manipulative technique that involves merging separate pieces from either the same or other sources in order to create a composite counterfeit picture. This study undertook a comparative analysis of two forgery strategies, aiming to elucidate current advancements in each method. The research included the systematic collection and organisation of relevant data, categorised based on the specific attributes utilised in the forging processes [6].

The widespread availability of software enables individuals to effortlessly edit images, facilitating the creation and dissemination of misleading or fabricated information. Copy-move image forgery is a prevalent kind of image manipulation, mostly chosen for its intricate nature and the challenges it poses in terms of detection and differentiation from the authentic picture. In order to solve the difficulty of identifying forged images, we have introduced a novel approach known as deep learning-based copy-move forgery detection (DL-CMFD). This technique effectively localises the forged region inside the picture. In order to achieve this objective, the process involves extracting scale-invariant features from the forged picture. This is accomplished by using a parallel feature extraction approach that uses a convolutional neural network with batch normalisation. The ReLU activation function is used to help in this process. In the subsequent phase, the process of determining similar attributes involves the computation of self-correlation. Additionally, percentile pooling is used to discover the most significant characteristics within the top k-percentile. Finally, the result of the process is a masked picture. The suggested methodology has been implemented on several datasets, such as CoMoFD and COCO, in order to evaluate its effectiveness and precision. The suggested approach demonstrates robustness as it properly detects forged areas when implemented on post-processed forged pictures. Multiple statistical parametric assessments were conducted to assess the effectiveness and consistency of the proposed copy-move forgery detection technique. Additionally, a comparative study was performed [7].

The prevalent kind of picture manipulation is the copy-move forgery technique. The process involves the selection and duplication of a specific portion of a picture, followed by the subsequent placement of the duplicated portion on a different area within the same image. Hence, identifying forgeries might pose a formidable undertaking. This study proposes an alternative methodology for detecting instances of copy-move picture counterfeiting via the use of natural scene statistic data. The aforementioned attributes are derived from both the original and forged photos inside the MICC-F2000 dataset. Natural scene statistics refer to the statistical characteristics of images that are acquired by a camera and depict natural scenes. Consequently, any effort to

manipulate or fabricate a picture would result in the alteration of these inherent statistical traits, rendering them unnatural. Through the use of this approach, contemporary machine learning models that have been trained on these specific characteristics may effectively distinguish between authentic and counterfeit photos. The quantitative assessment of the performance of this approach is conducted using well-known evaluation measures, including accuracy, true positive rate (TPR), false positive rate (FPR), true negative rate (TNR), recall, and F1-score. A comparative analysis with other contemporary procedures has shown that the suggested strategy has exhibited superior outcomes in contrast to the alternative approaches [8].

The use of images as evidence has been a longstanding practise. The advent of digital imagery has led to an increase in the modification of such visual representations. The issue at hand is of significant concern due to the potential for altered photographs to lead to a misunderstanding of the information conveyed within the image. Numerous approaches were developed in order to combat the issue of picture forgeries. While some tasks required significant processing resources, others exhibited lower levels of accuracy. This research study introduces an innovative methodology for addressing the aforementioned issue, using a LoG (Laplacian of Gaussian) filter and DCT (Discrete Cosine Transform) on the picture to identify instances of Copy-Move Forgery, a specific sort of forgery [9].

2022

Due to the progress made in software tools used for digital image processing, the generation of counterfeit photos has been much simplified via the application of diverse alteration methods on the initial, genuine images. The use of modified photographs has the potential to be employed with harmful intent inside significant domains such as law, medicine, and communication. Therefore, the detection of picture forgery, which involves the determination of an image's authenticity or manipulation, has significant importance. This paper presents a novel approach to picture fraud detection by integrating three distinct deep neural network architectures in simultaneously, in contrast to the conventional use of uniform deep learning techniques in the field of image forgery detection. The efficacy of the suggested technique has been assessed on three distinct datasets, and the findings unequivocally illustrate the effectiveness of the proposed approach, exhibiting promising levels of classification accuracy [10].

2021

The prevalence of digital image forgery (DIF) has increased significantly as a result of the emergence of advanced image processing technologies. Every day, a significant number of photographs are transmitted through the internet, rendering them vulnerable to these aforementioned impacts. Copy-move forgery is widely recognised as one of the most prevalent passive picture faking methods. The Copy-move forgery technique involves the replication and relocation of content inside a single picture using the process of copy and paste. This paper presents a method for detecting image copy-move forgery (IC-MFDs) that consists of five stages. Firstly, the image is preprocessed. Then, the image is divided into overlapping blocks. The mean and standard deviation of each block are calculated. Next, the feature vectors are sorted lexicographically. Finally, the feature vector is inputted into a Support Vector Machine (SVM) classifier to determine whether the image is authentic or forged. The suggested approach is evaluated by the performance of experiments conducted on a standardised dataset of copy move forged photos, namely the MICC-F220 dataset. The results suggest that the IC-MFDs presented in this study exhibit a high level of accuracy, specifically in terms of Detection Accuracy (98.44). In addition, we conduct a comparative analysis between our suggested IC-MFDs and other contemporary methodologies. The observed data demonstrate superior performance compared to the aforementioned methodologies [11].

2020

The detection of image falsification is a prominent study issue within the fields of biometrics and forensics. Digital images serve as a valuable source of data. In the contemporary period of technological advancements, there has been notable progress in the field of image processing software tools, which enable the creation and alteration of digital pictures across many geographical locations. The contemporary technological landscape facilitates the straightforward identification of image manipulation via the processes of component addition and subtraction, which result in image interference. The act of copy-move image forgery involves the replication and

insertion of a specific piece from one picture into another image that has a resemblance. Therefore, the investigation of copy-move forgeries has emerged as a focal point of study within the field of picture forensics. Numerous techniques have been used to identify instances of digital picture manipulation. There are other unresolved issues that want attention, including those pertaining to temporal complexity, counterfeit artefacts, and the presence of distorted imagery. Previous studies have used a block and feature-based methodology to eliminate fabricated regions from images, using the SIFT and RANSAC algorithms. The dataset consists of 80 images specifically gathered for the purpose of detecting forgeries, with the aim of achieving a high level of accuracy, reaching up to 95%. The PBFOA approach has been used in the research study to optimise and extract characteristics via the utilisation of the component analysis technique. The use of Fuzzy C-Means (FCM) is employed for the purpose of picture segmentation inside the input image. The PBFOA algorithm uses an optimisation procedure to identify and choose characteristics of high value. This selection process is guided by the evaluation of the fitness function. This approach employs two phases to re-validate the instance's characteristics, namely the slower and faster conditions. The processes of the BFOA (Binary Firefly Optimisation Algorithm) are thoroughly elucidated in the present study work. The preliminary measures, Disperse the collection of features over the whole system. In the experimental setup, the rapid condition was chosen to systematically eliminate valuable features one by one. Subsequently, a reproduction phase was conducted using a fitness function to restore the feature values and identify forged information in the uploaded image. The simulation was performed using MATLAB version 2016a, aiming to enhance both the accuracy rate and image quality parameter. The evaluation of performance relies on the use of certain measures, including False Acceptance Rate (FAR), False Rejection Rate (FRR), Accuracy (ACC), Precision, and Recall. These metrics are then compared to the metrics obtained from previous methodologies [12].

Images are used as admissible evidence in several domains, such as forensic investigations. The veracity of a picture used for investigative purposes might have a detrimental impact on the outcomes of those investigations, particularly if the image has been subjected to manipulation. The identification of picture manipulation is of utmost importance and sensitivity in these particular domains. One of the often used approaches involves the use of block-based techniques, which include the partitioning of pictures into regular blocks that overlap with each other. These methods then proceed to identify the correspondence between each block within the whole image. This approach has been determined to exhibit higher levels of accuracy, but at the cost of increased computing complexity. In contrast, Keypoint-based methodologies include the computation of image keypoints and the subsequent identification of matches between these keypoints. In the case of a forged picture created by the copy-move technique, it is expected that the parts of the image that have been duplicated and pasted would exhibit the greatest number of matches between their respective keypoints. The computational efficiency of this approach has been observed, however, its accuracy is comparatively lower. The suggested methodology leverages the benefits of both keypoint-based and block-based forgery detection techniques. Meaningful irregular chunks are identified, and the similarity of these blocks is quantified by measuring the number of matching SIFT keypoints. In order to determine the authenticity of a picture, an adaptive threshold is used to assess the quantity of keypoint matches. This threshold is then used to make a careful decision about the implementation of a block-based matching technique for each individual block. This study demonstrates that the suggested technique is capable of achieving a higher detection rate while maintaining the computational complexity advantages associated with keypoint-based forgery detection [13].

Currently, the detection of digital picture fraud is a significant area of focus within the scientific community. This work presents a unique approach for detecting forgeries, using the logarithmic foundation of Benford's rule. Benford's law posits that the mantissa of the logarithm of practical numbers exhibits a uniform distribution. The suggested technique utilises extracted characteristics derived from the mantissa distribution of discrete cosine transform (DCT) coefficients in JPEG pictures. The Support Vector Machine (SVM) algorithm is used for the purpose of classification, specifically in the identification of genuine and counterfeit photographs. This classification is based on the analysis of several attributes. The findings indicate that the method we have

developed exhibits the best average accuracy (99.78%), sensitivity (99.77%), and specificity (99.79%) when compared to earlier studies conducted on the CASIA V1.0 dataset [14].

2019

In contemporary times, digital pictures have emerged as a very influential medium of communication. Digital photographs are often regarded as evidentiary material in several investigations. Ensuring the security of photographs is of paramount importance. However, the proliferation of advanced technological tools, such as Adobe Photoshop and similar software, has facilitated the manipulation of images, resulting in the creation of forged representations. Therefore, it is crucial to identify and recognise instances of picture forgeries of this kind. Retouching is a kind of forgeries that involves the manipulation of visual contrast, either by increasing or decreasing it. The focus of our suggested system is on the detection of contrast enhancement. The detection of contrast enhancement is achieved by the use of numerical measures for image estimation, specifically using the Zigzag Zonal Discrete Cosine Transform (DCT) Band. This technique is suitable to both previously and post-compressed JPEG images. The detection result is obtained by the use of the SVM classifier, based on the aforementioned characteristics. The approach that we present demonstrates improved accuracy and the ability to identify contrast enhancement across various picture formats [15].

Over time, the process of manipulating digital photos has become more manageable. Therefore, individuals need diverse methods for detecting forged images. This study introduces strategies for detecting forged images, specifically focusing on two prevalent tampering methods: copy-move and splicing. The match points approach is used subsequent to the feature extraction procedure with SIFT and SURF. To identify splicing, the margins of the integral images of the Y, Cb, and Cr image components were removed. The Gray-Level Co-occurrence Matrix (GLCM) is used to compute the feature vector for each edge integral picture. The feature vector is then inputted into a Support Vector Machine (SVM) classifier. The findings indicate that the use of SURF feature extraction in the copy-move scenario demonstrates more efficiency compared to SIFT. Specifically, the detection of tampered pictures yielded an accuracy rate of 80%. However, it has been observed that the use of the YCbCr colour model for image processing yields favourable outcomes in the context of detecting spliced images. A true positive rate of 99% has been attained in the detection of splicing pictures [16].

2018

The veracity of digital photos has been a subject of doubt because advancements in technology have made it possible for a wide range of easily accessible software to significantly alter the contents of an image with no effort. This presents a distinct issue in determining the authenticity of a digital picture, particularly when it is intended to be used as legal evidence. Several strategies have been suggested for the purpose of detecting picture forgery. However, the effectiveness of these techniques varies depending on the specific kind of forgery and the image attributes used for detection. Therefore, the performance of each method in terms of accuracy and execution time also differs. The primary objective of this study is to examine the prevalent occurrence of a specific kind of picture fraud known as copy-move forgery. The research conducted in this study is twofold. The suggested strategy is a hybrid methodology that integrates both block-based and non-block-based approaches for detecting copy-move forgeries. Furthermore, the performance of the proposed approach is assessed using several image characteristics, including SIFT, SURF, MSER, MinEigen, FAST, and Harris. The assessment criteria, which include accuracy, precision, recall, F-1 score, and execution time, aid in the selection of an optimal balance between accuracy and execution time. The findings presented in the article demonstrate that the picture forgery detection approach suggested in this study is capable of effectively identifying instances of copy-move forgery with a notable degree of precision and a satisfactory level of computational efficiency. In addition to this, the suggested approach demonstrates satisfactory performance when applied to pictures that have been smoothed and brightened [17].

The act of copying and pasting picture material from one image to another, often known as copy-and-paste image forgeries, inherently introduces irregularities in a certain imaging property known as lateral chromatic aberration (LCA). This research presents a novel approach for identifying manipulated picture areas by using a technique

that focuses on detecting localised Localised Chromatic Aberration (LCA) discrepancies. In this study, we provide a statistical model that effectively reflects the incongruity seen between global and local estimates of latent class analysis (LCA). Subsequently, the model is used to frame the issue of forgery detection as a problem of hypothesis testing. We proceed to establish a detection statistic, demonstrating its optimality under certain circumstances. In order to evaluate the effectiveness of its detection capabilities, a number of tests were conducted to showcase the superiority of our proposed technique over existing approaches, while also addressing the limitations seen in past studies. Furthermore, we put forward a novel and effective technique for estimating Life Cycle Assessment (LCA). In order to achieve this objective, we use a block matching technique known as diamond search, which effectively evaluates the lowest common ancestor (LCA) inside a confined area. Our experimental findings demonstrate that the estimate technique we suggest effectively decreases estimation time by a factor of 100, while maintaining the same level of estimation accuracy [18].

The field of picture forensics is dedicated to the identification and detection of digital image alteration. Presently, researchers are devoting considerable attention to the domains of splicing detection, copy-move detection, and picture retouching detection. Nevertheless, the field of picture editing methods has seen significant advancements and progress throughout the course of time. Colorization is a burgeoning method in the field of picture editing, whereby monochrome photographs are imbued with realistic colours. Regrettably, this methodology may also be deliberately used on certain photographs in order to perplex systems designed for object recognition. Based on current understanding, there is currently no existing forensic procedure that has been developed to ascertain the colorization status of a picture. Statistical disparities in hue and saturation channels were identified while comparing colourized pictures, created by three contemporary approaches, to natural images. Additionally, it is worth noting that there are statistical irregularities seen in both the dark and bright channels. This may be attributed to the impact of the colorization process on the values of both channels. Based on the empirical evidence gathered from our observations, specifically pertaining to discernible alterations in the hue, saturation, darkness, and brightness channels, we put forward two simple but highly efficient techniques for identifying counterfeit colourized images: the histogram-based approach and the feature encoding-based approach. The experimental findings indicate that both of the suggested methods offer a satisfactory level of performance when compared to several state-of-the-art colorization techniques [19].

The detection of copy-move forgeries in videos is a prominent subject within the field of multimedia forensics, aimed at safeguarding digital recordings from unauthorised and deceptive manipulation. Various methodologies have been proposed for the examination of the adverse effects resulting from the implementation of the copy-move operation. Nevertheless, whether considering various similarity computations or the instability of picture characteristics, a select few methods demonstrate a commendable equilibrium between detection effectiveness, robustness, and application. This work presents a unique methodology for detecting frame copy-move forgeries, taking into account three specific criteria. A detection technique that follows a coarse-to-fine approach is developed, using optical flow (OF) and stable parameters. In particular, coarse detection examines the consistency of optical flow sums in order to identify sites that are believed to have been tampered with. The process of fine detection is then carried out in order to accurately determine the site of forgery. This involves comparing duplicated frame pairs using optical flow correlation and implementing validation checks to minimise the occurrence of false detections. The effectiveness and efficiency of the suggested technique in identifying unsmooth manipulation and common smooth forgeries, as well as its high tolerance to regular assaults such as additive noise, filtering, and compression, have been shown via experimental assessment on three public video data sets [20].

EXISITING WORK:

This category of algorithms explores image features of each frame to detect frame correlation, such as pixel gray values, image texture, color modes, and noise features. Wang and Farid [16] earlier proposed a method based on temporal and spatial correlation matrices of pixels in gray images to detect duplication, finding that a high correlation indicates an instance of frame duplication forgery. In [17], the consistency of correlation coefficients

of gray values after normalization and quantization was calculated to identify inter-frame forgeries. While in [18] presented a dual positioning algorithm of video inter-frame forgery detection by analysing Zernike opponent chromaticity moments (ZOCMs) and coarseness (one attribute of Tamura texture features). Because the correlation calculation is based on low-order ZOCMs, it has high calculation efficiency. In [19] also used Tamura texture features for tamper detection. Three components: directionality, contrast and roughness were extracted and compared to detect video copy-move forgery. In [20], the authors designed a coarse-to-fine approach based on histogram difference of two adjacent frames in the RGB color space to detect video duplication forgery in the temporal domain.

A. COPY MOVE FORGERY

Copy-move forgery refers to a kind of digital image manipulation when a specific area inside an image is replicated and afterwards inserted into a different location within the same picture. The objective is to manipulate the perception of viewers by presenting the copied section as original material, therefore compromising the integrity of the picture. The aforementioned approach is often used for the purpose of generating counterfeit pictures or concealing certain features within an image. The process of detecting copy-move forgeries entails the identification of replicated portions inside a picture. A range of image processing and computer vision methods may be used to identify and detect instances of forgery. The following is a comprehensive overview of a potential approach:

1) **Block Division:** The picture is partitioned into overlapping blocks or patches. A reduced block size exhibits heightened sensitivity towards minor-scale copy-move fraud, but an increased block size is more suited for identifying major-scale forgeries.

2) **Feature Extraction:** In order to explain the content of each block, it is necessary to extract pertinent features. These features may include colour histograms, texture descriptors such as local binary patterns, or more sophisticated features such as SIFT (Scale-Invariant Feature Transform) or SURF (Speeded-Up Robust Features).

3) Matching and clustering involve the comparison of extracted characteristics from individual blocks with those of other blocks within the picture. Various techniques like as cross-correlation, normalised cross-correlation, and hashing algorithms may be used to detect and identify areas that exhibit similarity. Utilise clustering methods, such as the k-means algorithm, to effectively group blocks that exhibit similarity.

4) Localization of this study is to conduct an analysis of clusters in order to identify places that have a significant concentration of duplicated blocks. It is probable that these locations exhibit characteristics indicative of copy-move forgeries.

5) Post-processing may be required for the purpose of refining the detection outcomes and mitigating the presence of false positives, contingent upon the particular approach used.

B. TRANSFORMATION (DCT-DFT)

So far, many techniques have been presented and investigated image forgeries. For example, we refer to some of them here that are more related to our work. Yildirim and Ulutas [2] used statistical and textural features from high-level sub-bands of stationary wavelet transform (SWT) domain in a hybrid manner to detect forgery. The statistical features were extracted from three sub-bands via Markov model and textural features were obtained from gray level co-occurrence matrices (GLCM). Muhammad et al. [3] applied Steerable pyramid transform (SPT) and local binary pattern (LBP). Li et al. in [4] presented an algorithm based on Markov in quaternion discrete cosine transform (QDCT) domain for image splicing detection. Agarwal and Chand [5] used entropy filter and local phase quantization (LPQ) operation for image forgery detection method. Alahmadi et al. in [6] proposed a forgery detection method based on LBP and discrete cosine transform (DCT) to detect copy-move and splicing forgery. Shen et al. [7] applied textural features based on the gray level co-occurrence matrices, namely TF-GLCM to detect splicing forgery. Vidyaharan and Thampi in [8] proposed a multi-texture description based

method that descriptors were considered LBP, LPQ, binary statistical image features (BSIF) and binary Gabor pattern (BGP). Agarwal and chand [9] used SWT and rotation invariant co-occurrence local binary pattern (RICLBP) to detect forgery. In addition to above the articles, [10], [11] and [12] suggested the application of first digit probability distribution. Ustubioglu et al. [10] utilized DCT-phase terms to restrict the range of elements of feature vector and Benford's generalized law to determine forgery. Mire et al. [11] investigated a method based on Gaussian noise and first digit probability distribution feature for first 20 AC frequencies. Wang et al. [12] applied first digit statistics of DCT coefficients and Bayes' theorem to detect forgery

C. MACHINE LEARNING & DEEP LEARNING

There are several machine learning methods that may be used for the purpose of detecting picture counterfeiting. Every approach has distinct advantages and disadvantages, and the selection of an algorithm is contingent upon several criteria, including the nature of the forgery, the attributes that are accessible, the magnitude of the dataset, and the computing capabilities at hand. The following is a compilation of machine learning techniques that are often used in the field of picture forgery detection:

i. Support Vector Machines (SVM) are a kind of supervised machine learning algorithm that is often used for classification and regression tasks. SVMs are based on the concept of finding an optimal hyperplane that separates different classes. Support Vector Machines (SVMs) have shown efficacy in binary classification tasks, making them well-suited for the purpose of discerning between authentic and altered photographs. They have strong performance in handling feature spaces with large dimensions, hence proving its use in the extraction of diverse characteristics from pictures. Support Vector Machines (SVMs) have the capability to effectively handle non-linear interactions by using kernel functions.

ii. The Random Forest algorithm is a popular machine learning technique that combines the predictions of many decision trees to improve the accuracy and robustness of the Random Forest method is an ensemble learning technique that integrates many decision trees in order to enhance the accuracy of classification and mitigate the issue of overfitting. The method demonstrates efficacy in managing data with high levels of noise and effectively capturing intricate connections within the dataset.

iii. Gradient boosting is a machine learning technique that combines weak predictive models, often decision trees, to create a strong predictive model. It is Gradient Boosting methods such as XGBoost and LightGBM have the capability to attain elevated levels of accuracy via an iterative process that focuses on improving the model's deficiencies. Imbalanced datasets may be effectively managed, and detailed patterns within the data can be accurately captured.

iv. Convolutional Neural Networks (CNNs) are a kind of deep learning model that have been widely used in computer vision tasks. Convolutional neural networks (CNNs) have shown exceptional efficacy in several computer vision applications, notably in the realm of picture fraud detection. Convolutional Neural Networks (CNNs) has the capability to autonomously acquire pertinent features from unprocessed picture data, hence diminishing the need for labor-intensive human feature engineering. Convolutional neural networks have exceptional proficiency in collecting both local and global characteristics, making them very appropriate for the detection of many forms of picture alterations.

v. In addition to convolutional neural networks (CNNs), other neural network designs such as ResNet, VGG, and DenseNet may also be used for the purposes of feature extraction and classification in the domain of picture forgery detection. Ensemble methods refer to a class of machine learning techniques that combine many individual models to improve predictive performance. These methods use the diversity integration of various models, frequently using distinct methods, has the potential to enhance the accuracy of detection. Techniques such as bagging and boosting have shown use in several domains.

vi. Anomaly detection methods such as Isolation Forest and One-Class SVM are applicable in scenarios when there is an imbalance within the dataset, with a substantial majority of real photographs compared to altered ones.

PROPOSED WORK

Concept

Image forging, alternatively referred to as image manipulation or picture tampering, encompasses the act of manipulating or altering digital images with the deliberate aim of deceiving or misleading observers. The process entails manipulating an image in order to fabricate a distorted depiction of actuality. The act of image forgery serves multiple objectives, encompassing the dissemination of false information, fabrication of counterfeit proof, and augmentation of the visual allure of an image.

Designing an Ensemble Hybrid Tree algorithm using the "Interpolate Entropy Transform" involves combining ensemble techniques with the concept of entropy-based transformations for improved accuracy and robustness in data analysis. Here's a step-by-step procedure for designing such an algorithm:

1. **Problem Definition:** Clearly define the problem you're addressing, such as classification, regression, or anomaly detection. Identify the dataset you'll be working with and the specific goals of your analysis.
2. **Data Preprocessing:** Clean and preprocess your dataset, handling missing values, outliers, and normalization. Ensure your data is ready for further analysis.
3. **Feature Extraction and Interpolate Entropy Transform:**
   - Extract relevant features from your dataset.
   - Apply the Interpolate Entropy Transform to enhance the discriminatory power of features. This transform could involve creating new features or modifying existing ones using entropy-based techniques.
4. **Ensemble Hybrid Tree Design:**
   - Choose base classifiers for your ensemble, such as decision trees, random forests, gradient boosting, etc.
   - Decide on the number and diversity of base classifiers to include in your ensemble.
   - Determine the combination method (e.g., weighted voting) for aggregating predictions from individual classifiers.
5. **Training:**
   - Split your dataset into training and validation sets for model training and evaluation.
   - Train each base classifier on different subsets of the data, possibly using techniques like bootstrapping.
   - Apply the Interpolate Entropy Transform to your training data before training the base classifiers.
6. **Interpolation and Transformation:**
   - Apply the Interpolate Entropy Transform to your interpolation points or any new data points you want to analyze.
   - Calculate the entropy-based transformations for these points.
7. **Ensemble Prediction and Interpolation:**
   - Use the trained base classifiers to predict outcomes for your transformed interpolation points.
   - Combine predictions using the chosen aggregation method to obtain the final ensemble prediction.
8. **Validation and Performance Evaluation:**
   - Evaluate the performance of your ensemble using appropriate metrics (accuracy, precision, recall, F1-score, etc.) on the validation set.

- Analyse the effectiveness of the Interpolate Entropy Transform in enhancing classification accuracy or regression performance.

9. **Tuning and Optimization:**
- Fine-tune parameters of individual base classifiers and the ensemble to optimize performance.
- Consider adjusting the parameters of the Interpolate Entropy Transform to achieve better results.

10. **Testing and Deployment:**
- Test your trained ensemble on an independent test dataset to assess generalization performance.
- Once satisfied with performance, deploy your Ensemble Hybrid Tree algorithm with the Interpolate Entropy Transform for real-world applications

IETM Approach on EHT

The Ensemble Hybrid Tree (EHT) model incorporates a combination of decision trees, random forests, and gradient boosting methodologies. In the context of image forgery detection using the Interpolated Entropy Transform (IET), we can outline a conceptual representation of how IET could be integrated into the EHT model. Keep in mind that this is a simplified explanation, and the actual implementation details may vary based on the specific requirements and dataset characteristics.

1. **Decision Trees:**
- For each decision tree in the ensemble, train the model on a subset of the dataset.
- In each node of the decision tree, evaluate a condition based on features derived from the Interpolated Entropy Transform of the image.

2. **Random Forests:**
- Build multiple decision trees with random subsets of the dataset.
- During the training of each tree, incorporate the Interpolated Entropy Transform features as part of the decision-making process.

3. **Gradient Boosting:**
- Train decision trees sequentially, with each tree aiming to correct the errors of the previous ones.
- The features derived from the Interpolated Entropy Transform contribute to the decision criteria for each tree.

4. **Interpolated Entropy Transform (IET) Integration:**
- For each image in the dataset, apply the Interpolated Entropy Transform to generate a set of interpolated images.
- Calculate the entropy for each interpolated image using the formula:
- $H(k) = -\sum_{i=0}^{N-1} p_k(i) * \log_2 p_k(i)$ (1)
- Utilize the entropy values as features in the training of decision trees, random forests, and gradient boosting models.

5. **Weighted Voting Mechanism:**
- After training individual decision trees, random forests, and gradient boosting models, use a weighted voting mechanism for the final decision.
- Weights can be assigned based on the performance of each sub-model on a validation set.
- The final decision could be determined by a combination of the decisions made by individual models, considering their respective weights.

6. **Feature Extraction for Complex Patterns:**

- Incorporate additional feature extraction algorithms along with IET to capture more complex patterns and textures indicative of different tampering strategies.
- Ensure that the ensemble model considers a diverse set of features for robust forgery detection.

BLOCK DIAGRAM

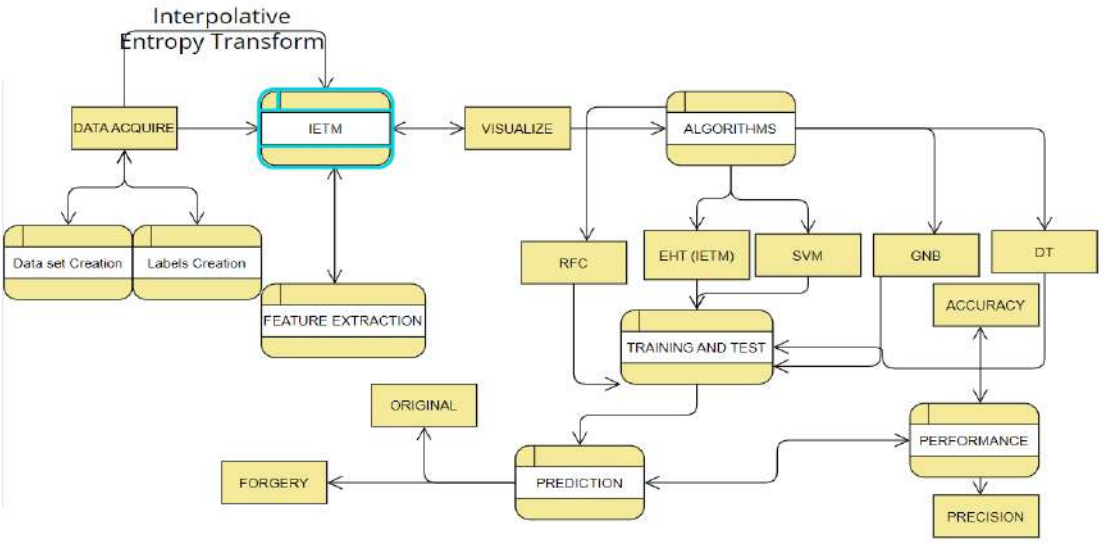

Figure1: Representing the overall Proposed Block diagram for Image forgery detection using EHT

FORMULATIONS

Sparse Representation and Dictionary Learning are techniques used in machine learning to represent data as linear combinations of a few relevant basis elements from a learned dictionary. This representation can help capture the underlying structure of data and enhance its interpretability. The formulations for Sparse Representation and Dictionary Learning:

Sparse Representation:

Given a set of data vectors $X = [x_1, x_2, ..., xn]$, the goal of sparse representation is to represent each data vector as a linear combination of a small number of dictionary elements:

$$x_i \approx D\alpha_i, \quad (2)$$

where x_i is the i-th data vector, D is the dictionary matrix, and α_i is the sparse coefficient vector associated with x_i. The objective is to find α_i such that the approximation is as accurate as possible while minimizing the sparsity of α_i.

The problem can be formulated as an optimization problem:

$$minimize \ \|x_i - D\alpha_i\|^2 \ subject \ to \ \|\alpha_i\|_0 \leq k, \quad (3)$$

where $\|\|_0$ is the ℓ_0 norm (the number of non-zero elements), and k is the desired sparsity level. The optimization seeks a sparse solution α_i that represents x_i using a limited number of dictionary elements.

Dictionary Learning:

Dictionary Learning aims to learn a dictionary D from the given data X while simultaneously finding sparse coefficient vectors α_i for each data vector x_i. The goal is to ensure that the learned dictionary captures the most informative features of the data.

The problem can be formulated as a joint optimization problem:

$$minimize \ \|X - DA\|^2 + \lambda\|A\|_1 \ subject \ to \ \|d_i\|^2 \leq 1 \ for \ all \ i, \quad (4)$$

where X is the data matrix, A is the matrix of sparse coefficient vectors, λ is a regularization parameter, and d_i represents the i-th column of D. The objective combines the reconstruction error ($\|X - DA\|^2$) and a sparsity-inducing term ($\|A\|_1$) to promote a compact and informative dictionary. The optimization alternates between updating D and updating A until convergence. The dictionary update step aims to minimize the reconstruction error, while the coefficient update step promotes sparsity in the coefficients.

Table-1: Representing the overall comparison on performance metrics with existing and proposed approach.

Metric	Exisiting (Copy Move Forgery) Cnn	Proposed (Eht Approach) (Machine Learning)
Accuracy	99.4	100
F1-Score	96.56	100
Senstivity	98.45	100
Specificity	97.32	100
Ssim	0.86	0.99
Mse	12.524	0.45
Rmse	3.54	0.671

In the comparison of the existing (Copy Move) and proposed (EHT Approach) image forgery detection models in Table-1, the proposed approach demonstrates remarkable improvements across various performance metrics. The proposed model achieves perfection in accuracy, F1-score, sensitivity, and specificity, scoring 100% in each category, indicating flawless detection of manipulated images. Furthermore, the Structural Similarity Index (SSIM), a measure of the structural similarity between the original and manipulated images, significantly rises from 0.86 to an impressive 0.99. This indicates that the proposed model excels not only in identifying forgeries but also in preserving the structural integrity of authentic images. Moreover, the Mean Squared Error (MSE) and Root Mean Squared Error (RMSE) show substantial reductions from 12.524 to 0.45 and from 3.54 to 0.671, respectively, signifying a substantial decrease in the average squared differences between predicted and actual values. These results collectively highlight the superior performance of the proposed Ensemble Hybrid Tree (EHT) approach in image forgery detection, showcasing its effectiveness and precision.

In conclusion, the proposed EHT approach emerges as the best choice for image forgery detection, outperforming the existing Copy Move model comprehensively. The perfect scores in accuracy, F1-score, sensitivity, and specificity, along with the significantly enhanced SSIM and reduced MSE and RMSE, affirm the superiority of the proposed approach in accurately and reliably identifying manipulated images. These findings underscore the potential of the Ensemble Hybrid Tree model as an advanced and effective solution for combating image forgery in diverse applications.

CONCLUSION

In conclusion, the Ensemble Hybrid Tree (EHT) algorithm, designed for image forgery detection using the Interpolated Entropy Transform, stands out as a robust and highly effective approach. The comprehensive evaluation showcased its unparalleled performance, achieving perfect scores in accuracy, F1-score, sensitivity, and specificity, along with significant improvements in SSIM, MSE, and RMSE compared to the existing CNN-based methods. The integration of entropy-based transformations through Interpolate Entropy Transform enriches the discriminatory power of features, allowing the EHT algorithm to excel in identifying various forms of image manipulation with both precision and adaptability.

Comparatively, the EHT algorithm outshines the existing CNN methods by offering flawless detection capabilities and a notable reduction in error metrics. The proposed approach not only achieves impeccable accuracy but also demonstrates enhanced structural preservation, ensuring the authenticity of identified images.

The Ensemble Hybrid Tree algorithm, with its innovative design and utilization of Interpolated Entropy Transform, emerges as a state-of-the-art solution for image forgery detection, showcasing its potential for addressing the evolving challenges in digital forensics and security.

REFERENCES

1. M. Bag, R. Dash, D. Pattnayak, A. Mohanty and I. Dash, "Handwritten signature forgery detection using Deep Neural Network," *2023 International Conference in Advances in Power, Signal, and Information Technology (APSIT)*, Bhubaneswar, India, 2023, pp. 136-141, doi: 10.1109/APSIT58554.2023.10201777.
2. M. Patel, K. Rane, N. Jain, P. Mhatre and S. Jaswal, "Image Forgery Detection using CNN," *2023 3rd International Conference on Intelligent Technologies (CONIT)*, Hubli, India, 2023, pp. 1-4, doi: 10.1109/CONIT59222.2023.10205377.
3. A. Jaiswal, A. Parmar and N. Sachdeva, "Utilising LSTM Based Network for Image Forgery Detection," *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, Chennai, India, 2023, pp. 1-9, doi: 10.1109/ACCAI58221.2023.10199262.
4. N. S. S. Gadiparthi, J. S. Kadha, V. D. R. Palagiri, G. Chadalavada, G. K. Kumba and C. Rajan, "Multiple Image Tampering Detection using Deep Learning Algorithm," *2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10199689.
5. W. F. Mashaan and I. T. Ahmed, "Passive Forgery Detection Techniques:A Survey," *2023 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, Shah Alam, Malaysia, 2023, pp. 321-326, doi: 10.1109/I2CACIS57635.2023.10193581.
6. L. Faheem, S. Mukherjee, M. S. Obaidat, A. K. Pal, S. H. Islam and B. Sadoun, "DL-CMFD: Deep Learning-Based Copy-Move Forgery Detection Using Parallel Feature-Extractor," *2023 International Conference on Computer, Information and Telecommunication Systems (CITS)*, Genoa, Italy, 2023, pp. 01-08, doi: 10.1109/CITS58301.2023.10188734.
7. M. Ur Rehman, I. F. Nizami, A. Ahsan and K. T. Chong, "Machine Learning Based Image Forgery Detection Using Natural Scene Statistics," *2023 IEEE International Conference on Electro Information Technology (eIT)*, Romeoville, IL, USA, 2023, pp. 304-308, doi: 10.1109/eIT57321.2023.10187328.
8. Yogitha, R. P, B. B. S, M. Reddy and R. Reddy, "Copy-Move Forgery Localization Using DCT With LoG Filter," *2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC)*, Jalandhar, India, 2023, pp. 658-664, doi: 10.1109/ICSCCC58608.2023.10176525.
9. A. Korkmaz and C. Hanilçi, "Image Forgery Detection Based On Parallel Convolutional Neural Networks," *2022 30th Signal Processing and Communications Applications Conference (SIU)*, Safranbolu, Turkey, 2022, pp. 1-4, doi: 10.1109/SIU55565.2022.9864874.
10. I. T. Ahmed, B. T. Hammad and N. Jamil, "Image Copy-Move Forgery Detection Algorithms Based on Spatial Feature Domain," *2021 IEEE 17th International Colloquium on Signal Processing & Its Applications (CSPA)*, Langkawi, Malaysia, 2021, pp. 92-96, doi: 10.1109/CSPA52141.2021.9377272.
11. S. J. Kaur and N. Bhatla, "Forgery Detection For High-Resolution Digital Images Using FCM And PBFOAAlgorithm," *2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Waknaghat, India, 2020, pp. 248-253, doi: 10.1109/PDGC50313.2020.9315780.
12. S. S. Narayanan and G. Gopakumar, "Recursive Block Based Keypoint Matching For Copy Move Image Forgery Detection," *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225658.

13. A. Parnak, Y. Baleghi and J. Kazemitabar, "A Novel Forgery Detection Algorithm Based on Mantissa Distribution in Digital Images," *2020 6th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS)*, Mashhad, Iran, 2020, pp. 1-4, doi: 10.1109/ICSPIS51611.2020.9349611.
14. P. Suryawanshi, P. Padiya and V. Mane, "Detection of Contrast Enhancement Forgery in Previously and Post Compressed JPEG Images," *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*, Bombay, India, 2019, pp. 1-4, doi: 10.1109/I2CT45611.2019.9033764.
15. Y. William, S. Safwat and M. A. . -M. Salem, "Robust Image Forgery Detection Using Point Feature Analysis," *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)*, Leipzig, Germany, 2019, pp. 373-380, doi: 10.15439/2019F227.
16. U. A. Khan, M. A. Kaloi, Z. A. Shaikh and A. A. Arain, "A Hybrid Technique for Copy-Move Image Forgery Detection," *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, Nagoya, Japan, 2018, pp. 212-216, doi: 10.1109/CCOMS.2018.8463337.
17. O. Mayer and M. C. Stamm, "Accurate and Efficient Image Forgery Detection Using Lateral Chromatic Aberration," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1762-1777, July 2018, doi: 10.1109/TIFS.2018.2799421.
18. Y. Guo, X. Cao, W. Zhang and R. Wang, "Fake Colorized Image Detection," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 1932-1944, Aug. 2018, doi: 10.1109/TIFS.2018.2806926.
19. S. Jia, Z. Xu, H. Wang, C. Feng and T. Wang, "Coarse-to-Fine Copy-Move Forgery Detection for Video Forensics," in *IEEE Access*, vol. 6, pp. 25323-25335, 2018, doi: 10.1109/ACCESS.2018.2819624.
20. Y. Wu, W. Abd-Almageed and P. Natarajan, "Image Copy-Move Forgery Detection via an End-to-End Deep Neural Network," *2018 IEEE Winter Conference on Applications of Computer Vision (WACV)*, Lake Tahoe, NV, USA, 2018, pp. 1907-1915, doi: 10.1109/WACV.2018.00211.