e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

DOCUMENT IMAGE FORGERY AND DETECTION METHODS USING IMAGE PROCESSING TECHNIQUES – A REVIEW

Asha Shinde[*1], Gayatri Patil[*2], Sathish Kumar[*3]

[*1]Student, Department Of Computer Science, Rani Channamma University, Belagavi, Karnataka, India.

[*2,3]Research Scholar, Department Of Computer Science, Rani Channamma University, Belagavi, Karnataka, India.

DOI : https://www.doi.org/10.56726/irjmets29313

ABSTRACT

Nowadays, papers are taken, stored, and shared more frequently in digital format. At the same time, document image altering software also gets more and more powerful as there is an increasing concern about the authenticity of documents. Texts on real estate agreements, for instance, can be changed to make an illegal deal, and the date on a plane ticket can be changed to get past security and into airport terminals. This study provides an overview of various image processing methods to spot document forging in order to stop such illegal actions. As digital image processing gains popularity in scientific and technical applications and forgery techniques develop quickly, the aim of forgery detection is to maximize the extraction of information from altered photos, particularly noisy and post-processed images. In order to create a new strategy for a future forensic science investigation, the major focus is on various sorts of forgery detection in digital image processing with the aid of all transform approaches and comparing their best results for further improvement.

Keywords: Document Image, Dataset, Forgery Detection Methods, Image Forgery And Image Processing Techniques.

I. INTRODUCTION

It is now quite easy to change scanned documents and make new ones with different information that are very difficult to differentiate between the original and the fake one thanks to new, powerful, sophisticated digital printers and a variety of software tools. Following the events of 2003, document fabrication became a widespread and pervasive issue throughout the world, but particularly in Iraqi society. Many people utilize this method to obtain employment unlawfully by falsifying their credentials, or even in the sale or purchase of real estate [1]. The meaning of a document can be altered. As a result, document forensics are becoming crucially significant and are needed in many different types of crimes. Document forensics' primary objective is to identify altered information in documents in order to determine whether they are genuine or fake. Three types of document tampering can be distinguished: addition, which involves adding new text, alteration, which involves modifying some of the contents, and erasure, which involves concealing some of the contents. A document can be fabricated using a number of techniques, then printed after being digitally altered [3].

A new area of image processing called "digital image forensics" aims to gather quantitative proof of the authenticity and source of a digital image. Image tampering detection is one of the main duties of image forensics. To interact with something in order to harm it or make unlawful changes is known as tampering [2]. Digital forensics is a group of scientific techniques for forgery detection that includes identification, analysis, interpretation, content authentication, classification, and documentation from digital sources. It denotes the who, what, and why of the situation. Investigations into images utilising various transform techniques to evaluate statistical binary patterns rely heavily on forensic science. Using computer programming skills, forensic image processing is a novel method for enhancing digital photos from surveillance, closed-circuit TV, and many other applications. Digital filters used in these systems can block a variety of noise, including Gblur noise, Pepper noise, Salt noise, Gaussian White Noise, Motion Noise, Multiplicative Spectrum, Poisson, and Filter Dilation, among others [7].

There are two different types of image forensics techniques: active and passive/blind. Traditional methods for hiding data or verifying signatures using active approaches include watermarking or digital signatures. Passive approaches or blind forensic approaches use image statistics or content of the image to verify its authenticity.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

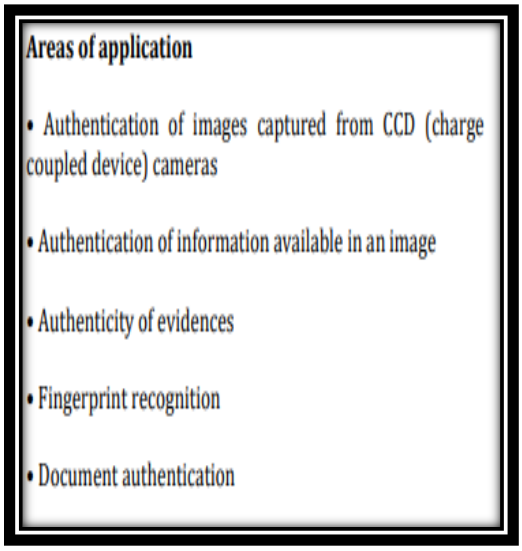
Digital images are used all over the world today, so this method is often reliable. Document exchange is a common practice in today's world. There is a chance of forgery when exchanging documents of this kind. Image Forgery is the process of making illegal changes to an image's information. The figure 1. Represents the example of document forgery where fig (a) original document and (b) forger document of original image. In figure (b) from naked eyes it is difficult to find the forger area in the image.

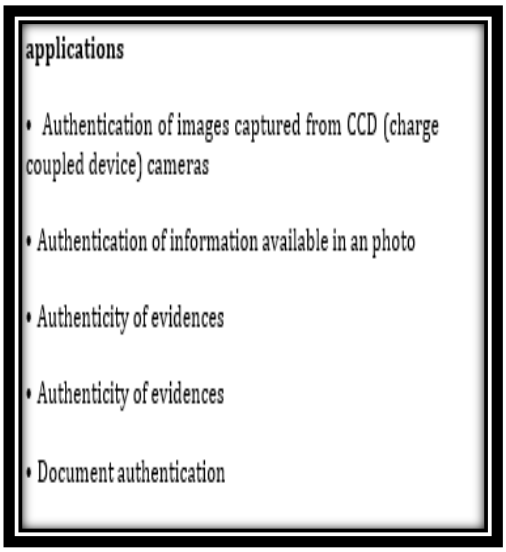
Applications:

- The authentication of images captured from CCD cameras.
- Authentication of information in an image.
- The authenticity of the evidences is an important factor in determining the validity of a hypothesis.
- Fingerprint recognition is a technology that is used to identify people by their fingerprints.
- Document authentication is the process of verifying the authenticity of a document.

There are two main categories of forgery detection techniques: active and passive. Non-active methods of image processing don't work with images from unknown sources. One of the drawbacks of using an active digital watermarking method is that it is susceptible to being removed or altered by the user. The passive method can be used to analyze binary information of a digital image without any prior information.

Image forgery detection methods are commonly used in a wide range of image processing applications. These methods can be used to compress, recognize, classify, transform, transmit, and retrieve images. Nowadays, the wide spread of image processing software and tools has made it easier to create fake images even by someone who has little knowledge of photography, and this method identifies five categories of image falsification as follows: (1) image transmission falsification; (2) image linkage; (3) photo retouching; (4) transform the image; and (5) image enhancement [13].





(a) Original Image **(b) Forged Image**

Figure 1. An Example of Document Image Forgery :(a) Original image and (b) Forged Image

II. LITERATURE WORK

This section outlines many methods that have been used to identify fake documents in images in earlier related publications. To the best of our knowledge, there aren't many techniques on this topic in the literature. As a result, we view the techniques for identifying fraudulent documents and detecting forgeries by printer source identification as being related work.

Shaimaa H et al [1] have proposed a way to detect forgery of official scanned documents. This method is based on the pixel properties of a grayscale image and applies the Discrete Wavelet Transform (DWT) and Principal Component Analysis (PCA) to extract features. Varsha Sharma et al [2] have explained techniques for detecting tampering with all types of images based on different approaches. This method is used in block matching or block cultivation algorithms and is the most commonly used method for detecting duplicates in an image, and

DCT is used to characterize overlapping blocks. Amr Megahed et al [3] have proposed a method to detect handwritten forgery using image processing instead of the traditional method. This detection method detects the manipulated position based on the RMSE of the adjacent feature vector. Features are extracted using RGB channels (mean, standard deviation, skewness). Zhipeng Chen et al [4] have presented an effective method of blur detection based on quality assessment without reference. The features are extracted from the mean subtraction contrast normalization (MSCN) coefficient and supplied to the SVM, which can distinguish the operating area. Abhisek et al [5] have describes different methods proposed by different authors to detect fake images. And all the approaches and methods described in this document can detect fraud. Mohamed Lamine Bouibed et al [6] describes a new system of writer search based on the dichotomy, which aims to improve writer search by learning the function of difference within and between writers. The proposed system uses an SVM decision designed to indicate the probability that two documents belong to the same author. Monika et al. [7] explains that the purpose of counterfeit detection is to maximize the extraction of information from manipulated images, especially noisy post-processed images. Therefore, the main focus is to compare and further improve various types of counterfeit detection in digital image processing using all conversion techniques and their best results, creating a new approach for future forensic research. Is to do. Lokesh Nandanwar et al [8] proposed a new way to detect changed text by applying DCT coefficients in various ways to get the merged image of the input image. This method extracts features from the merged image based on quality measurements and histogram-based features. Francisco et al [9] have presented a classification-based approach to counterfeiting detection. It uses a uniform local binary pattern (LBP) to capture identifiable texture features that are common in fake areas. The results of using a Support Vector Machine (SVM) for patch classification show that different types of documents can detect multiple types of counterfeiting. Seung-Jin et al [10] have presented a scheme for detecting malicious documents created by printers. 17 image quality measurements are applied to distinguish between genuine and counterfeit documents, and an SVM classifier is used to determine counterfeit documents. K.S. Raghunandan et al [11] have described a new approach to classifying a particular document as old or new. It can be used to identify malicious documents in the case of forensic crime applications. The proposed approach defines a new rule for classifying a given image as old and new based on the average contrast feature value.

F. Battisti et al [12] have presents a digital image forgery detection method that addresses the unconventional use of image quality evaluation. The proposed system is based on a combination of image quality degradation evaluation systems. Saif alZahir et al [13] have presented a method for detecting blind image tampering using a controllable pyramid decomposition technique and a copula ensemble. This method can accurately detect fakes in a small area of 16 pixels, which is the smallest size reported in the literature. Peng Ye et al [14] have outlines research on document quality evaluation. First, a detailed analysis of the types and causes of document degradation is given. Describes objective measurements and subjective experiments used to document image quality. Shilpa due et al [15] have introduced a new forensic detector that can handle splicing and copy move counterfeiting at the same time. The extracted features are used for classification by Support Vector Machine (SVM). Riaz A. Khan et al [16] have proposes a comprehensive review of techniques aimed at creating heat-resistant physical documents published over the last 20 years. Ying Chen et al [17] have presented a pattern recognition method for identifying handwritten counterfeiters, and for the first time detected handwritten counterfeit drawings using the Convolutional Neural Network (CNN) method. Also, two feature extraction methods commonly used in image processing (LBP and GIST). Amr Ahmed et al [18] have explained that several approaches are being considered to improve the accuracy of model-based document forgery and the average time it takes to classify incoming documents. The document is filtered based on the content and various parts have been removed. The disadvantage of this method is that it is time consuming and depends on the size of the training set. Ramzi M et al [19] has suggested a way to detect forgery of scanned text documents. This detection method is based on using the texture feature to identify the source scanner. As experiments have shown, the proposed method is robust to JPEG compression and provides recognition accuracy in excess of 90%. Khizar Hayat et al [20] have presented a forgery detection method applicable in the case of copy / move forgery. The proposed transformation domain method is based on both the Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). The goal is to reduce functionality through the first DWT and get an approximate subband. Joost van Beusekom et al [21] have proposes an approach to counterfeit detection using

text line information. When examining suspicious documents, rotating and arranging lines of text can be important clues for detecting tampered documents. And this paper proposes a two-line text feature. Zhipei Luo et al [22] have introduced a method to identify whether the local image area contains pixels of one or two inks and to distinguish the pixels belonging to each type of ink. Use of outlier estimation methods in combination with traditional clustering techniques. Romain Bertrand et al [23] have presented an automatic forgery detection method based on the unique functionality of the document at the character level. This method is based on the detection of outliers in the discriminant feature space on the one hand and the detection of exactly similar characters on the other. Justin picard et al [24] have discussed a virtually fraud-proof identity document based on a combination of three different data hiding technologies: watermarking, 2D barcodes, copy identification patterns, and additional biometric protection. As we will see later, this combination of data hiding technologies protects documents from counterfeiting, in principle, without the need for other security features. palainhanakote Shivakumara et al [25] have presented a new fusion-based method that uses the R, G, and B color components to detect fake IMEI numbers. The proposed method extracts features based on sparsity, number of connected components, and average strength values of the edge components of each R, G, and B component to generate 6 features. Olivier Augereau [26] has explained a new way to classify document images by combining text features extracted with the Bag of Words (BoW) technique with visual features extracted with the Bag of Visual Words (BoVW) technique. Lokesh Nandanwar et al [27] have presented a new expert system for detecting fake IMEI numbers and modified ticket images. This method is also used for the Discrete Cosine Transform (DCT) and Fourier Transform (FT) to get the IMEI number and the phase spectrum of the flight ticket image. Then, on the premise of the combination of functions, the phase statistics of the phase spectrum are extracted. Hongjun et al [28] have proposed a non-reference image quality evaluation method based on a statistical model of natural images in the wavelet transform domain. The generalized Gaussian density model is used to summarize the marginal distribution of the wavelet coefficients in the test image, so correlation parameters are needed to evaluate image quality.

Alireza et al [29] have described how to evaluate the quality of a blind document to solve DIQA issues in real-world scenarios, as reference images are not always available. It is first sampled into a series of patches to measure the quality of the document. Sayani Kundu et al [30] have proposed a new way to detect fake handwritten words from blurry, noisy, ordinary words. The proposed method examines the spectral density and variability to extract features based on the fact that the width and amplitude in the spectral direction are sensitive to the distortion produced by spurious manipulation, blurring, and noise. Nicolas Sidere et al [31] have introduced a new set of digitized documents representing pay slips. This work is intended to suggest that people working in the areas of fraud detection and word recognition be free to use common public datasets. Shize Shang et al [32] have describes how to detect document forgery based on DMGP using translational and rotational distortion parameters. This method is suitable for checking both Chinese and English documents, it can check documents character by character, is robust against JPEG compression, and is effective even for low resolution documents. Apurba Gorai et al [33] have proposes an efficient way to detect malicious documents. Histogram matching is performed to analyze the document, taking into account texture features such as local binary patterns and Gabor filters. The texture features and RGB color information for each word in the document is extracted. Dominic et al [34] have compared the performance of various image contrast methods suitable for real-world applications. These experimental methods are mainly histogram fitting methods. lokesh Nandanwar et al [35] introduced a new method by investigating the combination of the Chebyshev Harmonized Fourier Moment (CHFM) and the Deep Convolutional Neural Network (D-CNN). The proposed method is based on inconsistencies and irregular changes generated by counterfeit operations. Zohaib Khan et al [36] have presented the use of hyperspectral imaging to detect ink inconsistencies in handwritten notes. We propose a new joint thin band selection method that selects useful bands from hyperspectral images to detect accurate ink inconsistencies. The downside is that it is difficult to detect imbalanced ink mismatches due to the problem of imbalanced clustering.

Muhammad khan et al [37] have proposed an efficient automatic ink mismatch detection technique using multispectral image analysis. Ink pixels are segmented using local thresholds and fuzzy C-means clustering (FCM) is used to transform the spectral response vector of the ink pixels into different clusters associated with

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

the different inks used in the document. Divide into. Sung-Hyuk et al [38] have published an experiment using an automatic counterfeit detection system. As a result of the experiment, it was found that many subjects can successfully forge the handwriting of others in terms of shape and size by observing the ease of forgery of the handwriting and tracing the real handwriting. Monica Gariup et al [39] have states that verifying the authenticity of travel documents is the basis of border control. Due to increasing border pressures and the complexity of modern document security, border control authorities need to quickly and easily determine whether a presented document is genuine or fake. Henry S. Baird [40] has suggests work on document quality. In this work, they used their own dataset for this experiment. This method works according to Canungo's bootstrap method. Benjamin et al. [41] have discussed an approach to quickly extract information from the relevant 137 pieces of information from a set of objects, in the form of an experiment on 138 fake ID profiling. It demonstrates a specific application of Transversal Model 139 that leverages image processing techniques from a forensic intelligence perspective. Mohammed Javed et al [42] have presented research on document image analysis techniques in terms of image processing, image compression, and compressed domain processing. The motivation for directly investigating compressed document images was discussed. Chin-Shyurang Fahn et al [43] have presented a branchlet feature and a text-independent handwriting counterfeit detection system based on GMM. Then, the branch point of the skeleton image is determined for feature extraction. Santoshini Panda et al [44] have outlines the latest techniques in various passive counterfeit detection techniques proposed by different authors.

Mohd Dilshad Ansari et al. [45] have proposed and discussed various approaches to pixel-based detection of fake images. All the methods and approaches described in this post can detect fakes. However, some algorithms are not effective at detecting real fake areas. Navpreet Kaur Gill et al [46] have argues that counterfeiting detection using passive counterfeiting detection techniques is one of the fastest growing areas of research. We introduced several passive methods and compared them in terms of result accuracy. The main drawback of existing methods is automation. That is, the answer can only be interpreted by human intervention. Amandeep Kaur et al. [47] have proposed feature extraction using principal component analysis and an optimization algorithm (ant colony optimization) to detect fake images in JPG images. The optimization approach of classifying features to match training features will detect fake images in JPG images if the training and testing features match. Imam Riadi et al [48] have presented an analytical measurement of forensic image similarity using the distance function method, but image manipulation is especially used in image splicing. Shruti Ranjan et al [49] have described a computer-operated legal document for forensic examination using implemented image processing techniques. In addition, feature extraction with GLCM implemented in MATLAB Image Processing Toolbox R2015a provided the necessary results for the investigation and comparison of the original and morphed legal documents. Asad Abbas et al. [50] have states that ink analysis techniques based on hyperspectral separation have been proposed for the detection of ink inconsistencies. Our main focus is to distinguish visually similar inks that are mixed in different proportions to form an unbalanced clustering problem. Chandandeep Kaur et al [51] have outlines various techniques for detecting passive image tampering. A comparative analysis of various counterfeit detection techniques is also presented. This white paper also describes different types of datasets used by different counterfeit detection approaches. Tanzeela Qazi et al [52] have introduces several promising techniques that represent a reasonable improvement in counterfeit detection methods. Still, these improvements are far from perfect and have certain drawbacks that need to be eliminated for effective results, and this method is used for DCTs and PCAs. Keshao D. Kalaskar et al [53] have focused on the key challenges faced in preprocessing document images for document image analysis. Preprocessing is the first step in document image analysis and includes representation, denoising, binarization, skew estimation / detection, zoning, and character segmentation.

Akram Hatem Saber et al [54] have presented various image forensic approaches to identify counterfeiting made in digital images. The techniques described in this article are digital signatures, watermarks, copy moves, image splicing, and image cloning. Gayatri et al [55] have proposes a new forensic imaging technique for detecting the presence of fakes in compressed and other formats of images. The proposed method is based on contour transformation (NSCT) without subsampling. Devi Mahalakshmi et al [56] have proposes a way to identify counterfeit attacks caused by blurring overlapping areas in an image. In the proposed method, the area

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

of interest was segmented from the entered fake image. Peng zhou et al [57] have proposed a new network that uses both RGB and noise streams to learn a wide range of features for image manipulation detection. It extracts noise characteristics through an SRM filter layer adopted from the ridge analysis literature, allowing the model to capture noise discrepancies between the manipulated and real regions. MandeepKaur et al [58] have outlined various approaches to manipulation detection in digital images. The main limitation of the available tamper detection methods is the inability to distinguish between malicious tampering and the real processing operations performed on the image. Wei Wang et al [59] have proposed a passive color image splicing detection method based on the analysis of image color components. After feature extraction, feature selection was performed to reduce the dimensions of the feature. The recognition accuracy with feature reduction was not worse than without it. Pradyumna Deshpande et al [60] have explained the classification of image forgery detection techniques and describes two key techniques for pixel-based forgery detection.

Malathi et al [61] have proposed a two-phase mandatory change path to address monitoring of the direct learning feature when referencing images modified in different aspect ratios. And I used the Discrete Cosine Transform (DCT) method. Tiago José de et al [62] have presented a new way to detect fake images of people based on the color of the light source. Statistical Gray Edge Method and Inverse Intensity-Estimates bright colors using a physics-based method that utilizes a chromaticity color space. Tamana Sharma et al [63] have describes a technique for detecting fake composite images using a machine learning classifier. Use a support vector machine and a least squares support vector machine and a perceptron with color lighting. G. Reddy Swetha et al [64] have discussed forensic photography. Extract the GLCM function, which is an LBP function, for detection. And finally, the SVM classifier predicts the result. Our method gives better results than existing systems. S.L.Jothilakshmi et al [65] have presented a new way to detect counterfeit images of people based on the color of the lamp. Statistical Gray Edge Method and Inverse Intensity-Estimate bright colors using a physics-based method that utilizes chromaticity color space. Sumaira Bibi et al [66] have discussed the implementation procedure of the proposed framework for forgery detection of digital images. The proposed approach solves the time complexity problem and can effectively detect all kinds of fake and compressed images. This is the main issue with how to detect false images. And the CNN classifier was used. Kalyani kadam et al [67] have discussed image tampering with a deep learning approach. It also focuses on collecting XAI of images. Explainable artificial intelligence research focuses on different types of XAI technologies in deep learning frameworks that help interpret decisions. And 83.3% accuracy. Nick F. Ryman-Tubb et al [68] have explained how the research community can turn research towards detecting payment card fraud and break away from the current unacceptable level of payment card fraud.

III. CHALLENGES AND ISSUES

The previous research shows that numerous academics have made an effort to identify document forgeries using both standard datasets and their own custom datasets. These techniques might not be effective in all situations, including those involving low-quality photos, images with noise and unclear surroundings, forgery involving numerous forging procedures, etc. This demonstrates the necessity for a comprehensive mechanism to identify document picture counterfeiting and its understanding and development. Therefore, in order to solve the issue, the writers have mentioned certain difficulties and problems from the literature review. The following are the difficulties and problems.

- Find counterfeits in all kinds of printed document images.
- One of the biggest challenges is the complexity of time.
- Quality measurements alone may not be sufficient to obtain better results for detecting altered text in document images.
- Challenge to recognize the changed text in the document.
- Difficult issues that require additional investigation of other types of features to extend this method to more difficult counterfeit cases.
- One of the main issues in developing an automatic counterfeit detection system is the wide range of locations where counterfeit products are located.
- Forgery detection in both printed and handwritten documents of any script.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

- Authenticity verification is a difficult problem, especially if the verification system is not provided with support information.
- DIQA is an important and difficult issue in document image analysis, but relatively little attention has been paid to this area.
- If the tampered and scanned document is indistinguishable from the real document, some legal issues may arise.
- The type of digitization of paper documents, the number of documents to be digitized, and the size of the information system that manages the digital copy.
- You need to process different types of documents (invoices, pay slips, support documents) from different sources.
- Tracking lost mobile phones with a unique IMEI number can be a daunting task for criminals.
- In many cases, it is difficult to apply research techniques in the context of industry.
- Detecting fake IMEI numbers or changed tickets is a difficult problem.
- Finding the right distortion measurements between the reference and distorted images based on a set of features can be a daunting task.
- Providing human-based subjective ground truth for such training data is a daunting task.
- Forgery of manuscripts poses research challenges as it is part of a criminal application.
- Detecting counterfeit documents is a difficult task in forensics.
- Issues such as noise reduction, degradation and blurring.
- Algorithm solutions are presented to address specific challenges in camera-based hyperspectral document capture.
- Poor quality document images pose serious technical challenges to current recognition techniques.
- Trace the original information in a compressed representation.
- Detecting fake and separating fake images from innocent real images is a challenge for image analysts.
- The hardest task is to develop an integrated algorithm that can detect all kinds of counterfeiting.
- The research in this treatise addresses this need and seeks to provide insights into this difficult problem.
- Issues such as noise reduction, degradation and blurring.
- Poor quality document images pose serious technical challenges to current recognition techniques.
- Trace the original information in a compressed representation.
- Detecting fake and separating fake images from innocent real images is a challenge for image analysts.
- The hardest task is to develop an integrated algorithm that can detect all kinds of counterfeiting.
- The research in this treatise addresses this need and seeks to provide insights into this difficult problem.
- The challenge is to determine the authenticity of multimedia content.
- Blind splice detection is a difficult problem.
- Passive image forensics is a daunting task in image processing techniques.
- It is becoming increasingly difficult to distinguish between real and manipulated images.
- Image tampering detection makes image forensics a very important research topic.
- Manipulating compressed images.
- Noisy manipulated image.
- Forgery detection is one of the tough issues with inside the virtual picture era.
- A tampering choice with the aid of using evaluating the color distributions with inside the facial regions.

IV. DATASET DESCRIPTION

- **UCID**: For testing, the well-known image dataset UCID is presented. The 1338 uncompressed TIFF photos in the UCID dataset cover a wide range of subjects, including both indoor and outdoor natural settings and man-made artefacts. Keep in mind that 250 random photographs are chosen, and they are all transformed to grayscale in the same way.
- **CVL**: The Computer Vision Lab (CVL) database is made for author retrieval, word recognition, and author identification. 309 writers contributed to its collection. Five separate texts—one in German and four in English—are produced by each author.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

- **ICDAR-2011:** This benchmarking dataset was suggested for the 2011 ICDAR writer identification competition. It was created by the computational intelligence research team at Greece's Demokritos national Centre for scientific research. 8 pages with text in four languages were provided by 26 authors (English, French, German and Greek). Another collection was created from this dataset that just includes the first two lines of each text. Due to its lack of extensive information regarding writing style, this corpus makes it more difficult to solve the writer retrieval problem. The first dataset is currently referred to as original, whereas the second dataset is referred to as cropped.
- **KHATT:** It is an offline collection of handwritten text that was compiled by 1000 individual authors from various Arabic-speaking backgrounds, including age, education, gender, and left- or right-handedness. Each author completed a four-page form that was scanned at resolutions of 200, 300, and 600 dpi [22]. Samples from this corpus are shown in Figure 12.
- **ICPR 2018**: ICPR's 2018 Fraud Detection Contest (FDC), a benchmark dataset, provides altered text at the character level. The majority of the papers included in this dataset are receipts, which are regarded as fraudulent documents because the price has been changed. The primary issue with this dataset is that it just contains strings of numerals with a currency sign and the text is too short. The data becomes more complicated and difficult when only one character in a string of a few digits is changed. The dataset offers 602 photos for testing, with 300 samples for the original text and 302 examples for the changed text.
- **IMEI number dataset:** 1000 photos were used in the evaluation of the IMEI number detection. This dataset offers photos with IMEI numbers that were extracted from mobile images. The IMEI number is often pasted inside the phone or occasionally on the outside of the case. In this instance, character-level image manipulation uses the same operations. The photographs in this dataset differ from those in other datasets because the background complexity is dependent on the mobile device being used, whereas the backgrounds of the images in other datasets are plain because they were taken from documents.
- **Google-LIFE-Magazine:** Five classes of the 1930, 1940, 1950, 1960, and 1970 decades are included in the Google-LIFE-Magazine data. There are a total of 200 printed document images, with 40 in each class. We take into account a new class of our data with five classes of these data for testing.
- **CoMoFoD dataset**: The CoMoFoD database contains forgeries that have been created utilising a variety of manipulations and post-processing methods, including image transformation (translation, scaling, and rotation) as well as other image processing alterations like compression, adding noise, or varying illumination. The 260 forged photos in the CoMoFoD database are divided into two categories based on their size: tiny 512 512 pixels and large 3000 2000 pixels. There are 200 photos in the 512 x 512 group and 60 in the larger group. The 512 by 512 image set has 5 subgroups. 40 photos are included in each subgroup. Translation, rotation, and scale are among the manipulations included in these photos.
- **CASIA v1.0 and v2.0 dataset:** Developed by the Institute of Automation of the Chinese Academy of Sciences, CASIA v1.0 and v2.0 are considered to be a more sophisticated and realistic dataset for tamper detection. CASIA v1.0 has a total of 1721 images, 800 of which are real and 921 are manipulated color images of 384 x 256 size, all in JPEG format without post-processing. CASIA v2.0, on the other hand, consists of images of multiple sizes with various post-processing applied to the entire edge. CASIA v2.0 consists of 7491 real color images measuring 240 x 160-900 x 600 pixels and 5123 fake color images. In addition, images are available in a variety of quality elements, both uncompressed and in JPEG format.
- **UWA HYPERSPECTRAL DOCUMENTS Dataset**: UWA hyperspectral document dataset in our work. This database consists of 70 hyperspectral images of handwritten notes written by 7 subjects using 10 different inks, including 5 blue and 5 black inks.
- **TID2008 database:** The TID2008 database contains 25 reference images and 1700 distorted images (25 reference images x 17 distortion type's x 4 distortion levels).
- **CISQ database:** The CISQ database consists of 30 original images and their distorted counterparts with 6 different distortions with 4-5 different degrees of distortion.

V. COMPARATIVE AND ANALYSIS

This article represents the most advanced technique for document image forgery detection. Table1. compares the relative accuracy of various methods and lists the benefits and drawbacks of each.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

Table 1: Comparative analysis of different Document Image Forgery and Detection Methods.

S/No	Author	Method	Classifier	Dataset	Result	Advantage	Disadvantage
1	Shaimaa H et al [1]	DCT,PCA	SVM	20 original official documents and 20 tampered official document.	Design a quick and most efficient system.	Most efficient system. Removing noise.	The development of digital image processing software and editing tools.
2	Varsha Sharma et al [2]	DCT, Block matching algorithm	Thresholding classification	Own created data Set.	The proposed method has addressed the issue successfully and is considerably faster than the existing method.	Faster than the exiting method.	Time complexity. it shows robust -ness against.
3	Amr Megahed et al [3]	RGB color Channels.	KNN	Own created data Set.	An accuracy of 59%.	Saves humans effort and cost. 2. high-efficiency detection.	Poor accuracy.
4	Zhipeng Chen et al [4]	MSCN	SVM	UCID (Uncompressed Color Image Dataset).	Image blur detection.	High accuracy.	Time-consuming, inconvenient and expensive for practical situations.
5	Abhishek et al [5]	Pixel based	NMF	Own created dataset.	The accuracy is 99.5%	High efficient	Few algorithm are not visible regarding identifying actual forged region. Time

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:08/August-2022 Impact Factor- 6.752 www.irjmets.com

							complexity.
6	Mohamed Lamine Bouibed et al [6]	HOG, GLBP, LDF, RLF	SVM,CNN	CVL(Computer Vision Lab), ICDAR-2011, KHATT	The accuracy is 94.75%	Feature extraction.	Computation complexity.
7	Monika et al [7]	Segmentation, Histogram	Thresholding classification	Own created dataset.	Identify new methodologies and ideas for future investigators.	Identify new methodology	High complexity. Expensive and lower quality factor. Low accuracy.
8	Lokesh Nandanwar et al [8]	DCT	CNN	Own dataset and IMEI and ICPR 2018 Fraud contest dataset.	The accuracy is 88.6%	Highest average.	Data more complex and challenging. 2. Poor quality Image.
9	Francisco et al [9]	Local Binary Patterns(LBP), Intrinsic	SVM	Own created dataset.	True positive rate 7.38% and false positive rate 0.05%.	Reduce the noise.	Detect several types of forgeries with low ratio of false positives.
10	Seung-Jin et al [10]	IQM	SVM	Own created dataset.	The result obtained were presumed to accurate.	Achieves accurate results.	Printers are commonly used device to make fraud documents.
11	K.S.Raghunandan et al [11]	Divide and Conquer	divide and conquer	Own Created Dataset, Google LIFE Magazine	The accuracy is 78.5%.	Used for both printed and handwritten documents of any scripts.	Poor result.
12	F. Battisti et al [12]	DCT	SVM	Own created	Improve the	Features extracted	Loss of high frequency.

				dataset.	localization of tampered areas.	from the image into the image itself.	
13	Saif alZahir et al [13]	DWT, Steerable pyramid, Copulas ensemble	KNN	CoMoD (copy move database).	An accuracy of 95.6%.	High efficiency. High accuracy.	Low quality factor.
14	Peng Ye et al [14]	OCR (Optical Character Recognition).	Binary classifier	IQA (Image Quality Assessment)	Discuss objective measures and subjective experiments.	Minimize cost.	Reduce the information or visual quality with respect to the original source.
15	Shilpa due et al [15]	DCT	SVM	Image dataset, CASIA	An accuracy of 98%.	Features extraction.	Time complexity.
16	Riaz A. Khan et al [16]	PCA	Binary classifier	IPFS	Address the open issues and challenges.	Improves response time and accuracy requirement	RFID tags are very complex. 2. Low storage.
17	Ying Chen et al [17]	LBP (Local Binary Pattern), GIST (Global Feature Descriptor)	CNN,SVM	Normal handwriting , Forged handwriting	An accuracy of 95.35%.	Improve detection efficacy. Reduce network complexity.	Loss value overflow caused the network to not coverage.
18	Amr Ahmed et al [18]	RAST (Recognition by Adaptive Subdivision of Transformation) Algorithm	KNN	DocAlign it consist of 40 genuine documents. 40 copied documents and 12 forged documents.	An accuracy of 98%.	The true positive rates have increased compared to the base line of the reproduced results.	Method is that it takes a lot of time in addition to being dependent on the size of the training set.
19	Ramzi M et al [19]	LDA, GLCM (Graylevel Co-	SVM	Own created dataset.	An accuracy of 90%.	The system will extract a set of features	Some difficulties in filtering the scanned

		occurrence Matrix)				from each group of characters.	image in either the pixel or transform domain.
20	Khizar Hayat et al [20]	DCT,DWT	SVM	Own created dataset.	An accuracy of 94.74%.	The detection method was its viability for both copy/move and splicing based forgeries.	The main problem is that undermines the credibility of digital image as photographic evidence.
21	Joost van Beusekom et al [21]	Text-line skew variation model, Txt-line alignment model	Bayesian classifier.	Own created dataset, TP300 and PPC300, TPLJ and TPCLJ DTL.	An accuracy of 89%.	Reduce the error rate, especially the false positive rates.	No public statically data are available giving an insight into how people forge document.
22	Zhipei Luo et al [22]	LOF, COF, INFLO	Morphgological Operation	UWA Hyperspectral Documents dataset.	An accuracy of 80%.	Highest accuracy.	Their relative proportions in the inspected image are roughly equal.
23	Romain Bertrand et al [23]	SEP (Scan-Edit and Print) technique.	Bayesian classifier.	Own created dataset.	An accuracy of 82%.	Reduce the print and scan noise issue.	Time Complexity.
24	Justin Picard et al [24]	Digital watermarking, 2-D bar codes, Copy Detection Pattern.	SVM	Own created dataset.	An accuracy of 85%.	Digital security mechanism for all parts of the verification .	The accuracy of all biometric systems is a trade-off problem between false-acceptances and false-rejections.

25	palainhanakote Shivakumara et al [25]	RGB	K-culster	Own created dataset.	An accuracy of 80%.	Extract the effect of loss of edges, noisy components.	Forged IMEI number detection in mobile images is still a research issue.
26	Olivier Augereau[26]	BoW (Bag of Words), BoVW (Bag of Visual Words)	SVM	1925 document image industrial database.	An accuracy of 90%.	BoW has very good performance.	Manually labeling the documents is very time-consuming.
27	Lokesh Nandanwar et al [27]	DCT,FT	SVM	Own created dataset. ICPR 2018 FDC dataset.	An accuracy of 90%.	High quality. Low cost.	Time-consuming.
28	Hongjun et al. [28]	Statistic model, Wavelet Transform, Domain (WTD), Quality assessment method.	K-means clustering.	TID2008 , CISQ, JPEG2000, JPEG, WGN, GB.	An accuracy of 85%.	Reduce the algorithm complexity.	Method is insensitive.
29	Alireza et al [29]	IQA, FR IQA , NA IQA	K-culster.	ITESOFT, TID2008, CSIQ, LIVE, ITESOFT.	An accuracy of 86%.	MQAC is fast and does not need subjective image quality provided by human for learning.	Very time consuming and inconvenient for both service providers and clients. Low quality.
30	Sayani Kundu et al [30]	Fourier Spectral Density.	CNN	Own created dataset, IMEI number dataset.	The proposed method achieves the 100% classificatio	Achieves the better result compared to the other exiting	The variations in handwriting make the problem more complex and

					n rate.	methods and proposed methods for all three combinations.	challenging.
31	Nicolas Sidere et al [31]	DWT	ANN	Public dataset.	Detect fraudulent document at text-line level.	One possible solution to avoid this problem was to erase or blur sensitive data.	Drawback of breaching the possible confidentiality of the document.
32	Shize Shang et al [32]	JPEG compression.	SVM	Own created dataset.	The effectiveness of our method on low JPEG compression quality and low resolution.	Robust to JPEG compression.	Time complexity in proposed method. Reduce the accuracy in tampering detection.
33	Apurba Gorai et al [33]	RGB color, TLC, GLCM feature, LBP, GF.	SVM	Own created dataset.	The method is found to be very efficient.	Less time-consuming.	Needs more attention.
34	Dominic et al [34]	Contrast-Limited Adaptive Histogram Equalization (CLAHE).	Bayesian classifier.	Own created dataset.	An accuracy of 93%.	The histogram equalization method has less computational complexity.	Poor local performance in terms of detail preservation . .Histogram Equalization, do not always produce good results.

35	lokesh Nandanwar et al [35]	Chebyshev-Harmonic-Fourier-Moments (CHFM).	CNN	Own created dataset, ACPR 2019, ICPR 2018 FCD, IMEI datasets.	An accuracy of 82.1%.	Feature extraction.	Low redundancy for noisy and blurred images.
36	Zohaib Khan et al [36]	PCA	SVM	Public dataset.	An accuracy of 89%.	Increase the accuracy. Reducing the acquisition time.	Not feasible in time critical scenarios. Time consuming.
37	Muhammad khan et al. [37]	TLC, FCM, K-mean Clustering.	Thresholding classification.	UWA Writing Inks Dataset.	95.9%with false positive of 4.54%.	The system was very robust and effective.	Very time consuming, sensitive to temperature and destructive.
38	Sung-Hyuk et al [38]	HOG	ANN	Own created dataset.	An accuracy of 89%.	Increase the training and testing set sizes. The exact speed and acceleration is impossible to forge.	Time Complexity.
39	Monica Gariup et al [39]	Binary classifier	KNN.	Own created dataset.	The main findings of the Document Challenges.	Time minimizing false rejections.	The detection of abnormal printing techniques is very difficult for the machines.
40	Henry S. Baird [40]	Kanungo's Bootstrapping Method.	Bayesian classifier.	Own created dataset.	An accuracy of 90%.	More efficient. Less Data-hungry procedure.	Less sensitive to specific types of image degradation.

41	Benjamin et al [41]	HOG	SVM	Own created dataset.	Identify the false document for forensic intelligence.	Flexible method.	False identity documents are frequently involved in human trafficking
42	Mohammed Javed et al [42]	Image Compressed.	SVM	ICDAR2009	Study on different image analysis and image compression techniques.	The pre-processing stage improves the quality of the image.	Today word spotting is a challenging problem in historical documents, handwritten documents.
43	Chin-Shyurang Fahn et al [43]	Branchlet features. Gaussian mixture models (GMM).	Binary classifier.	IAM Handwriting Database	An accuracy of 95%.	High accuracy.	The computer vision technique does not have such restrictions.
44	Santoshini Panda et al [44]	OLBM, DWT,SVD, PCA.	K-dimensional tree	Own created dataset	improve the time complexity of the algorithm	Reduce noise.	High time complexity.
45	Mohd Dilshad Ansari et al [45]	Pixel-based techniques.	QCD	Own created dataset	The various methods discussed.	Accurate image forgery detection algorithms	Some algorithms are not effective. Some algorithms have a very high time complexity.
46	Navpreet Kaur Gill et al [46]	DCT	SVM	Own created dataset	Compare the various different techniques based on their accuracy.	Shows good performance.	Methods is computationally expensive.
47	Amandeep Kaur et al	Principle component	K-mean clustering.	Own created	An accuracy of	Reduce computatio	It is very durable, if

	[47]	analysis (PCA).		dataset.	92%,	n time.	impossible, for the human eye to detect digital manipulation at face value.
48	Imam Riadi et al [48]	Joint Photographic Experts Group (JPEG).	CNN	Own created dataset.	An accuracy of 95%.	Image forensics is a study that identifies the origin and verifies the authenticity of an image.	Error rate will increase on re-save operation.
49	Shruti Ranjanet al [49]	ANN, GLCM , DWT, SVD.	SVM,CNN	Own created dataset.	An accuracy of 96.4%.	Good efficiency and accuracy.	Increase the time to run the algorithm.
50	Asad Abbas et al [50]	Hyperspectral document images, Hyperspectral unmixing, Thin Layer Chromatography (TLC).	SVM	UWA dataset.	An accuracy of 99.96%	Reducing the overall complexity.	Time consuming and sensitive to temperature changes as well.
51	Chandandeep Kaur et al [51]	DCT,DWT	SVM	MICC-F2000 MICC-F220 MICC-F600 CoMoFoD	An accuracy of 90.01%	Robust method to identify any type of forgery in the image is needed.	The discussed methods until now is that they do not succeed in differentiating malicious tampering from innocent retouching.
52	Tanzeela Qazi et al [52]	DCT, DWT, Scale	SVM	Own created dataset	surveyed detection techniques	Extract features. The	High complexity. Low

		invariant feature transform (SIFT).			for three of the most common forgery types	accuracy rate is very high	reliability with small copied images
53	Keshao D. Kalaskar et al [53]	DIA	Bayesian Classifier.	Own created dataset.	An accuracy of 97%.	Noise reduction.	Not feasible.
54	Akram Hatem Saber et al [54]	Pixel based.	CNN	Own created dataset.	Reduced complexity and increased accuracy.	Reduced complexity. Increase accuracy	Time complexity.
55	Gayatri et al [55]	No subsampled contoured transform (NSCT), DCT.	NSCT	Own created dataset.	Comparison between DCT and NSCT. NSCT gives better accuracy than DCT.	Maximum accuracy than the previous existing method.	Very poor in accuracy and correction of a result. digital tampering is difficult to detect
56	S. Devi Mahalakshmi et al [56]	Statistical Region Matching (SRM).	SVM	MICC-F220 Dataset.	An accuracy of 90%.	Feature extraction.	Method does not work for most of the cases.
57	Peng Zhou et al [57]	RGB channels. SRM.	SVM	Columbia dataset, NIST16	An accuracy of 93%.	Reduce contrast differences are challenging for the RGB stream.	Current standard datasets do not have enough data for deep neural network training.
58	MandeepKaur et al [58]	Scientific Working Group on Imaging Technology (SWGIT).	SVM	Own created dataset.	An accuracy of 85%.	Very high probability of tamper detection. Low cost. More effective.	Inability to distinguish malicious tampering and genuine processing operations.
59	Wei Wang et al [59]	Gray level co-occurrence matrix (GLCM).	SVM	Public image dataset.	An accuracy of 88%.	Reduce the computational complexity	Detection rate was also not high and they are

						of training and testing.	time consuming for feature extraction.
60	Pradyumna Deshpande et al [60]	Pixel based, DWT	K-dimensional.	Own created dataset.	An accuracy of 90%.	More efficient.	It takes more issues like rotation and noise. Robust forgery detection is still difficult.
61	J.Malathi et al [61]	Pixel based, DCT	SVM,ML	Columbia Image Splicing dataset	Improved forgery detection framework.	Feature extraction.	low-level procedures
62	Tiago José de et al[62]	physics-based and statistics-based color constancy methods	SVM	Own created dataset.	An accuracy of 86%.	Reduce complexity. Minimum amount of human interaction and provides a crisp statement on the authenticity of the image.	Very time-consuming.
63	Tamana Sharma et al [63]	Pixel based, format based.	SVM,LSSVM	Own created dataset.	An accuracy of 80%.	Extract image features. Less complexity.	The insertion of watermark at the time of recording, which requires the existence of well-equipped digital camera.
64	G.Reddy Swetha et al [64]	GLCM	SVM, binary classifier.	Own created dataset.	Our method provides the better result than the existing	Rather than the rough location, precise boundaries	If the given image was in same contrast, we cannot find the forgery

					system.	of the fake object are extracted.	region.
65	S.L.Jothilakshmi et al [65]	Color-based method	SVM, meta-fusion classifier	DSO-1, DSI-1	Propose a new algorithm based on edge-points	Reduce image noise.	Poor result
66	Sumaira Bibi et al [66]	JPEG compressed images.	CNN	CASIA dataset.	achieved 95.9% accuracy	Reduce time.	Photographic images, security and authenticity were the main problems. Greater computational complexity and cannot be applied in real-time systems.
67	Kalyani Kadam et al [67]	JPEG-based, CMFD.	CNN	Scopus, Web of Science, ACM Digital Library	83.3%	High accuracy.	The disadvantage is that this method cannot differentiate legitimate and invalid operations in the image.
68	Nick F. Ryman-Tubb et al [68]	Expert systems/Decision Tree	HMM,SVM	Own created dataset.	An accuracy of 80%.	Reducing the growing payment card fraud problem.	Academic work in this area is difficult and marginalized in terms of funding.

VI. CONCLUSION

In this research, we investigated various approaches for identifying forged document images using image processing tools. In order to build trust in all photos and photographs, authors examined the various varieties of image counterfeiting. The strategy for detecting any type of document image forgery, which is based on many approaches, was also researched by other writers. The comparison of the various approaches reveals that there is still room for improvement in terms of identifying and detecting artefacts in document images.

VII. REFERENCES

[1] Hameed, S., Shakir, S. H., & Zwyer, N. (2018). "Forgery Detection Based Image Processing Techniques". Article in International Journal of Scientific and Engineering Research, (November). Retrieved from https://www.researchgate.net/publication/328860701.

[2] Sharma, V., Jha, S., & Kumar Bharti, R. (2016). "Image Forgery and its Detection Technique: A Review". International Research Journal of Engineering and Technology. Retrieved from www.irjet.net.

[3] Megahed, A., Fadl, S. M., Han, Q., & Li, Q. (2018). "Handwriting forgery detection based on ink colour features". In Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS (Vol. 2017-November, pp. 141–144). IEEE Computer Society. https://doi.org/10.1109/ICSESS.2017.8342883.

[4] Chen, Z., Zhao, Y., & Ni, R. (2013). "Forensics of blurred images based on no-reference image quality assessment". In 2013 IEEE China Summit and International Conference on Signal and Information Processing, ChinaSIP 2013 Proceedings (pp. 437–441). https://doi.org/10.1109/ChinaSIP.2013.6625377.

[5] Kashyap, A., Parmar, R. S., Agarwal, M., & Gupta, H. (2017). "An evaluation of digital image forgery detection approaches". International Journal of Applied Engineering Research, 12(15), 4747–4758.

[6] Bouibed, M. L., Nemmour, H., & Chibani, Y. (2022). "SVM-based writer retrieval system in handwritten document images". Multimedia Tools and Applications, 81(16), 22629–22651. https://doi.org/10.1007/s11042-020-10162-7.

[7] Monika, & Bansal, D. (2020). "Forensic Science Research Summary for Forgery Detection of Digital Images". International Journal of Engineering and Advanced Technology, 9(3), 1608–1618. https://doi.org/10.35940/ijeat.b2563.029320.

[8] Nandanwar, L., Shivakumara, P., Pal, U., Lu, T., Lopresti, D., Seraogi, B., & Chaudhuri, B. B. (2021). "A New Method for Detecting Altered Text in Document Images". International Journal of Pattern Recognition and Artificial Intelligence, 35(12). https://doi.org/10.1142/S0218001421600107.

[9] Cruz, F., Sidere, N., Coustaty, M., D'Andecy, V. P., & Ogier, J. M. (2018). "Local Binary Patterns for Document Forgery Detection". In Proceedings of the International Conference on Document Analysis and Recognition, ICDAR (Vol. 1, pp. 1223–1228). IEEE Computer Society. https://doi.org/10.1109/ICDAR.2017.202.

[10] Ryu, S. J., Lee, H. Y., Cho, I. W., & Lee, H. K. (2008). "Document forgery detection with SVM classifier and image quality measures". In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 5353 LNCS, pp. 486–495). https://doi.org/10.1007/978-3-540-89796-5_50.

[11] Raghunandan, K. S., Shivakumara, P., Navya, B. J., Pooja, G., Prakash, N., Kumar, G. H., … Lu, T. (2016). "Fourier coefficients for fraud handwritten document classification through age analysis". In Proceedings of International Conference on Frontiers in Handwriting Recognition, ICFHR (Vol. 0, pp. 25–30). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICFHR.2016.0018.

[12] F. Battisti," Image forgery detection by using No-Reference quality metrics", February 2012 proceedings of SPIE – The International Society for Optical Engineering. DOI:10.1117/12.910778.

[13] AlZahir, S., & Hammad, R. (2020). "Image forgery detection using image similarity". Multimedia Tools and Applications, 79(39–40), 28643–28659. https://doi.org/10.1007/s11042-020-09502-4.

[14] Ye, P., & Doermann, D. (2013). "Document image quality assessment: A brief survey". In Proceedings of the International Conference on Document Analysis and Recognition, ICDAR (pp. 723–727). https://doi.org/10.1109/ICDAR.2013.148.

[15] Dua, S., Singh, J., & Parthasarathy, H. (2020). "Image forgery detection based on statistical features of block DCT coefficients". In Procedia Computer Science (Vol. 171, pp. 369–378). Elsevier B.V. https://doi.org/10.1016/j.procs.2020.04.038.

[16] Riaz A. Khan," A comprehensive study of document security system, open issues and challenges", Department of Computer Science and Engineering, Islamic University of Science and Technology (IUST), Kashmir, (J&K) 192122, India, DOI:https://doi.org/10.1007/s11042-020-10061.

[17] Ying, C., & Shuhui, G. (2020). "Forgery numeral handwriting detection based on fire module convolutional neural network". Laser and Optoelectronics Progress, 57(22). https://doi.org/10.3788/LOP57.221019

[18] Ahmed, A. G. H., & Shafait, F. (2014). "Forgery detection based on intrinsic document contents". In Proceedings - 11th IAPR International Workshop on Document Analysis Systems, DAS 2014 (pp. 252–256). IEEE Computer Society. https://doi.org/10.1109/DAS.2014.26

[19] Abed, R. M. (2015). "Scanned Documents Forgery Detection Based on Source Scanner Identification". American Journal of Information Science and Computer Engineering (Vol. 1, pp. 113–116). Retrieved from: http://www.aiscience.org/journal/ajiscehttp://creativecommons.org/licenses/by-nc/4.0/

[20] Hayat, K., & Qazi, T. (2017). "Forgery detection in digital images via discrete wavelet and discrete cosine transforms". Computers and Electrical Engineering, 62, 448–458. https://doi.org/10.1016/j.compeleceng.2017.03.013

[21] Van Beusekom, J., Shafait, F., & Breuel, T. M. (2013). "Text-line examination for document forgery detection". International Journal on Document Analysis and Recognition, 16(2), 189–207. https://doi.org/10.1007/s10032-011-0181-5

[22] Luo, Z., Shafait, F., & Mian, A. (2015). "Localized forgery detection in hyperspectral document images". In Proceedings of the International Conference on Document Analysis and Recognition, ICDAR (Vol. 2015-November, pp. 496–500). IEEE Computer Society. https://doi.org/10.1109/ICDAR.2015.7333811

[23] Bertrand, R., Gomez-Kramer, P., Terrades, O. R., Franco, P., & Ogier, J. M. (2013). "A system based on intrinsic features for fraudulent document detection". In Proceedings of the International Conference on Document Analysis and Recognition, ICDAR (pp. 106–110). https://doi.org/10.1109/ICDAR.2013.29

[24] Picard, J., Vielhauer, C., & Thorwirth, N. (2004). "Towards fraud-proof ID documents using multiple data hiding technologies and biometrics". In Security, Steganography, and Watermarking of Multimedia Contents VI (Vol. 5306, p. 416). SPIE. https://doi.org/10.1117/12.525446

[25] Shivakumara, P., Basavaraja, V., Gowda, H. S., Guru, D. S., Pal, U., & Lu, T. (2018). "A new RGB based fusion for forged IMEI number detection in mobile images". In Proceedings of International Conference on Frontiers in Handwriting Recognition, ICFHR (Vol. 2018-August, pp. 386–391). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICFHR-2018.2018.00074

[26] Augereau, O., Journet, N., Vialard, A., & Domenger, J. P. (2014). "Improving classification of an industrial document image database by combining visual and textual features". In Proceedings - 11th IAPR International Workshop on Document Analysis Systems, DAS 2014 (pp. 314–318). IEEE Computer Society. https://doi.org/10.1109/DAS.2014.44

[27] Nandanwar, L., Shivakumara, P., Kanchan, S., Basavaraja, V., Guru, D. S., Pal, U., Blumenstein, M. (2021). "DCT-phase statistics for forged IMEI numbers and air ticket detection". Expert Systems with Applications, 164. https://doi.org/10.1016/j.eswa.2020.114014

[28] Li, H., Hu, W., & Xu, Z. neng. (2016). "Automatic no-reference image quality assessment". SpringerPlus, 5(1). https://doi.org/10.1186/s40064-016-2768-2

[29] Alaei, A., Conte, D., Martineau, M., & Raveaux, R. (2018). "Blind document image quality prediction based on modification of quality aware clustering method integrating a patch selection strategy". Expert Systems with Applications, 108, 183–192. https://doi.org/10.1016/j.eswa.2018.05.007.

[30] Kundu, S., Shivakumara, P., Grouver, A., Pal, U., Lu, T., & Blumenstein, M. (2020). "A New Forged Handwriting Detection Method Based on Fourier Spectral Density and Variation". In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 12046 LNCS, pp. 136–150). Springer. https://doi.org/10.1007/978-3-030-41404-7_10

[31] Sidere, N., Cruz, F., Coustaty, M., & Ogier, J. M. (2017). "A dataset for forgery detection and spotting in document images". In Proceedings - 2017 7th International Conference on Emerging Security

Technologies, EST 2017 (pp. 26–31). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/EST.2017.8090394

[32] Shang, S., Kong, X., & You, X. (2015). "Document forgery detection using distortion mutation of geometric parameters in characters". Journal of Electronic Imaging, 24(2), 023008. https://doi.org/10.1117/1.jei.24.2.023008

[33] Gorai, A., Pal, R., & Gupta, P. (2016). "Document fraud detection by ink analysis using texture features and histogram matching". In Proceedings of the International Joint Conference on Neural Networks (Vol. 2016-October, pp. 4512–4517). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/IJCNN.2016.7727790

[34] Asamoah, D., Ofori, E., Opoku, S., & Danso, J. (2018). "Measuring the Performance of Image Contrast Enhancement Technique". International Journal of Computer Applications, 181(22), 6–13. https://doi.org/10.5120/ijca2018917899

[35] Nandanwar, L., Shivakumara, P., Kundu, S., Pal, U., Lu, T., & Lopresti, D. (2020). "Chebyshev-Harmonic-Fourier-Moments and deep CNNs for detecting Forged handwriting". In Proceedings - International Conference on Pattern Recognition (pp. 6562–6569). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICPR48806.2021.9412179

[36] Khan, Z., Shafait, F., & Mian, A. (2015). "Automatic ink mismatch detection for forensic document analysis". Pattern Recognition, 48(11), 3615–3626. https://doi.org/10.1016/j.patcog.2015.04.008

[37] Khan, M. J., Yousaf, A., Khurshid, K., Abbas, A., & Shafait, F. (2018). "Automated forgery detection in multispectral document images using fuzzy clustering". In Proceedings - 13th IAPR International Workshop on Document Analysis Systems, DAS 2018 (pp. 393–398). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/DAS.2018.26

[38] Cha, S. H., & Tappert, C. C. (2002). "Automatic detection of handwriting forgery". In Proceedings - International Workshop on Frontiers in Handwriting Recognition, IWFHR (pp. 264–267). https://doi.org/10.1109/IWFHR.2002.1030920

[39] Gariup, M., & Piskorski, J. (2019). "The challenge of detecting false documents at the border: Exploring the performance of humans, machines and their interaction". International Journal of Critical Infrastructure Protection, 24, 100–110. https://doi.org/10.1016/j.ijcip.2018.10.005

[40] Baird, H. S. (1999). "Document image quality: Making fine discriminations". In Proceedings of the International Conference on Document Analysis and Recognition, ICDAR (pp. 463–466). IEEE Computer Society. https://doi.org/10.1109/ICDAR.1999.791824

[41] Talbot-Wright, B., Baechler, S., Morelato, M., Ribaux, O., & Roux, C. (2016). "Image processing of false identity documents for forensic intelligence". Forensic Science International, 263, 67–73. https://doi.org/10.1016/j.forsciint.2016.03.054

[42] Javed, M., Nagabhushan, P., & Chaudhuri, B. B. (2018). "A review on document image analysis techniques directly in the compressed domain". Artificial Intelligence Review, 50(4), 539–568. https://doi.org/10.1007/s10462-017-9551-9

[43] Fahn, C. S., Lee, C. P., & Chen, H. I. (2016). "A text independent handwriting forgery detection system based on branchlet features and Gaussian mixture models". In 2016 14th Annual Conference on Privacy, Security and Trust, PST 2016 (pp. 690–697). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/PST.2016.7906952

[44] Panda, S., & Mishra, M. (2018). "Passive techniques of digital image forgery detection: Developments and challenges". In Lecture Notes in Electrical Engineering (Vol. 443, pp. 281–290). Springer Verlag. https://doi.org/10.1007/978-981-10-4765-7_29

[45] Ansari, M. D., Ghrera, S. P., & Tyagi, V. (2014). "Pixel-Based Image Forgery Detection: A Review". IETE Journal of Education, 55(1), 40–46. https://doi.org/10.1080/09747338.2014.921415

[46] Gill, N. K., Garg, R., & Doegar, E. A. (2017). "A review paper on digital image forgery detection techniques". In 8th International Conference on Computing, Communications and Networking Technologies, ICCCNT 2017. Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCCNT.2017.8203904

[47] Kaur, A. (2017). "AUTHENTICATION BASED IMAGE FORGERY DETECTION USING OPTIMIZED FEATURES IN JPEG IMAGES". International Journal of Advanced Research in Computer Science, 8(7), 616–621. https://doi.org/10.26483/ijarcs.v8i7.4316

[48] Riadi, I., Fadlil, A., & Sari, T. (2017). "Image Forensic for detecting Splicing Image with Distance Function". International Journal of Computer Applications, 169(5), 6–10. https://doi.org/10.5120/ijca2017914729

[49] Ranjan, S., Garhwal, P., Bhan, A., Arora, M., & Mehra, A. (2019). "Framework for Image Forgery Detection and Classification Using Machine Learning". In Proceedings of the 2nd International Conference on Intelligent Computing and Control Systems, ICICCS 2018 (pp. 1872–1877). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCONS.2018.8663168

[50] Abbas, A., Khurshid, K., & Shafait, F. (2018). "Towards Automated Ink Mismatch Detection in Hyperspectral Document Images". In Proceedings of the International Conference on Document Analysis and Recognition, ICDAR (Vol. 1, pp. 1229–1236). IEEE Computer Society. https://doi.org/10.1109/ICDAR.2017.203

[51] Kaur, C., & Kanwal, N. (2019). "An analysis of image forgery detection techniques". Statistics, Optimization and Information Computing, 7(2), 486–500. https://doi.org/10.19139/soic.v7i2.542

[52] Qazi, T., Hayat, K., Khan, S. U., Madani, S. A., Khan, I. A., Kołodziej, J., Xu, C. Z. (2013). "Survey on blind image forgery detection". IET Image Processing, 7(7), 660–670. https://doi.org/10.1049/iet-ipr.2012.0388

[53] Kalaskar, Keshao D., and Mahendra P. Dhore. "Preprocessing Challenges in Document Image Analysis." Proceedings published by International Journal of Computer Applications® (IJCA) ISSN: 0975–8887, MPGI National Multi Conference 2012 (MPGINMC-2012). 2012.

[54] Saber, A. H., Khan, M. A., & Mejbel, B. G. (2020). "A survey on image forgery detection using different forensic approaches". Advances in Science, Technology and Engineering Systems, 5(3), 361–370. https://doi.org/10.25046/aj050347

[55] Dakhode, G., & Chourey, Asst. Prof. P. K. (2017). "Forensic Technique for Detection of Image Forgery". International Journal of Advanced Engineering Research and Science, 4(1), 189–193. https://doi.org/10.22161/ijaers.4.1.31

[56] S. Devi Mahalakshmi," IMAGE FORGERY DETECTION", International Journal of Pure and Applied Mathematics Volume 118 No. 11 2018, 775-781, DOI: 10.12732/ijpam.v118i11.100.

[57] Zhou, P., Han, X., Morariu, V. I., & Davis, L. S. (2018). "Learning Rich Features for Image Manipulation Detection". In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (pp. 1053–1061). IEEE Computer Society. https://doi.org/10.1109/CVPR.2018.00116

[58] KAUR, M., & GUPTA, DR. S. (2014). "An investigation of approaches for image forgery detection". IJARCCE, 8714–8719. https://doi.org/10.17148/ijarcce.2014.31213

[59] Wang, W., Dong, J., & Tan, T. (2009). "Effective image splicing detection based on image chroma". In Proceedings - International Conference on Image Processing, ICIP (pp. 1257–1260). IEEE Computer Society. https://doi.org/10.1109/ICIP.2009.5413549

[60] Deshpande, P., & Kanikar, P. (2012). "Pixel Based Digital Image Forgery Detection Techniques". International Journal of Engineering Research and Applications, 2(3), 539–543.

[61] Malathi, J., Narasimha Swamy, B., & Musunuri, R. (2019). "Image forgery detection by using machine learning". International Journal of Innovative Technology and Exploring Engineering, 8(6 Special Issue 4), 561–563. https://doi.org/10.35940/ijitee.F1116.0486S419

[62] Carvalho, T. J. D., Riess, C., Angelopoulou, E., Pedrini, H., & Rocha, A. D. R. (2013). "Exposing digital image forgeries by illumination color classification". IEEE Transactions on Information Forensics and Security, 8(7), 1182–1194. https://doi.org/10.1109/TIFS.2013.2265677

[63] Tamana Sharma, Er.Mandeep Kaur " Forgery Detection of Spliced Images Using Machine Learning Classifiers and color Illumination", International Journal of Innovative Research in Science, Engineering and Technology Vol. 5, Issue 6, June 2016, ISSN(Online): 2319-8753, DOI:10.15680/IJIRSET.2015.0506186.

[64] G.Reddy Swetha, Mr.Ravi Kishore" Machine-Learning Algorithm for Digital Image Forgeries by Illumination Color Classification", International Journal of Innovative Research in Electronics and Communications (IJIREC) Volume 2, Issue 6, August 2015, PP 7-14 ISSN 2349-4042.

[65] S L, J., K, V., A, V., A, S. nathiya, & A, S. priya. (2014). "Automatic Machine Learning Forgery Detection Based On Svm Classifier". International Journal of Mechanical Engineering, 1(1), 1–5. https://doi.org/10.14445/23488360/ijme-v1i1p101

[66] Bibi, S., Abbasi, A., Haq, I. U., Baik, S. W., & Ullah, A. (2021). "Digital Image Forgery Detection Using Deep Autoencoder and CNN Features". Human-Centric Computing and Information Sciences, 11. https://doi.org/10.22967/HCIS.2021.11.032

[67] Kadam, K., Ahirrao, S., & Kotecha, K. (2021, October 1). "AHP validated literature review of forgery type dependent passive image forgery detection with explainable AI". International Journal of Electrical and Computer Engineering. Institute of Advanced Engineering and Science. https://doi.org/10.11591/ijece.v11i5.pp4489-4501

[68] Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018, November 1). "How Artificial Intelligence and machine learning research impacts payment card fraud detection": A survey and industry benchmark. Engineering Applications of Artificial Intelligence. Elsevier Ltd. https://doi.org/10.1016/j.engappai.2018.07.008