International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

A Study of Image Tampering Detection

Sreepriya S[1], Dr.Asha T.S[2]

[1]PG Student, Dept. of ECE,NSS College of Engineering, Kerala, India
[2]Professor, Dept. of ECE, NSS College of Engineering, Kerala, India

---

Abstract - *Images and videos have evolved into the primary data transporters in the modern era. The simplest video in TV news is frequently acknowledged as a confirmation of the accuracy of the reported news. Similarly, video observation and recordings can be used as primary trial material in a formal courtroom. Along with undeniable benefits, the availability of advanced visual media has a significant disadvantage. Image processing experts can undoubtedly access and alter image content in such a way that its significance is preserved. Outwardly noticeable follows are lost. Furthermore, with the ease of access to editing tools, the craft of modifying, and Forging visual substance is no longer confined to specialists. As a result, image manipulation for malicious purposes has increased. Digital forensics is the process of discovering and translating electronic data. The procedure's goal is to detect any proof in its most basic structure whereas conducting an organized examination by gathering, distinguishing, and approving computerized data for the purpose of procreating past affirmation. Forgery detection methodologies are typically classified into two types: active forensics and passive forensics, with digital watermarking and digital signatures being examples of active techniques. In contrast to these approaches, passive image forensics techniques work in the absence of a watermark or signature. These methods are based on the idea that, while digital forgeries may leave no visible signs of tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be divided into five categories: 1) pixel-based methodologies for detecting statistical anomalies introduced at the pixel level, 2) format-based techniques that take advantage of statistical correlations introduced by a specific lossy compression scheme,3) camera-based methods that take advantage of artifacts introduced by the camera lens, sensor, or on-chip post processing, 4) physically-based techniques that explicitly model and detect anomalies in the three-dimensional interaction of physical objects, light, and the camera, and 5) geometric-based techniques that make measurements of objects in the world and their positions relative to the camera.*

Key Words*: *Image tampering detection, Image tampering localization, journal, Image forgery detection, Image forensics.

1. INTRODUCTION

Individuals and organizations have frequently sought ways to manipulate and modify images in order to deceive the viewer since the invention of photography. Originally a difficult task requiring many hours of work by a professional technician, the advent of digital photography has made it possible for anyone to easily modify images, and even easier to achieve professional-looking results. This has resulted in far-reaching social issues ranging from the veracity of images reported by the media to the doctoring of photographs of models in order to improve their appearance or body image. The advancement of photo manipulation techniques is a mixed blessing. On one hand, it facilitates the beautification of image and thereby encourages human beings to explicit and proportion their thoughts on visual arts of image editing; On the other hand, it is a great deal less difficult to forge the content of a given photo without leaving any seen clues and for this reason helps forgers to deliver fake information. Image retouching, image splicing, and copy and move attacks are all examples of image forgery. Image retouching is regarded as the least harmful type of digital image forgery. Image splicing is a simple process that allows you to copy and paste regions from different sources. This technique is known as paste-up, and it is formed by adhering images together using digital tools. This technique involves combining two or more images to create a fake image. One of the most common and difficult image tampering techniques is the copy and move attack. It was necessary to use the cover portion of a similar image to add or remove the information. The goal of a copy and move attack is to conceal some information in the original image. It is extremely difficult to distinguish a forged image from an original. The human eye cannot draw a distinction between a tampered region from a forged image. Typically, image forgery detection techniques encompass JPEG quantization tables, Chromatic Aberration, Lighting, Camera Response Function(CRF), Bi-coherence and higher-order statistics, and Robust matching. The digital cameras encode the images based on JPEG compression, which configures the devices at various compression levels. Then, the sign of image tampering is evaluated by analyzing the inconsistency of lateral chromatic aberration. In which, the average angular between the local and global parameters is computed for every pixel in the image. If the average value exceeds the threshold, it is stated that the deviation in the image is unpredictable due to image forgery. The inconsistencies and the illuminating light source are then detected for each object in the image to identify the forgery . Various measurements, such as infinite, local, and multiple, are typically used to calculate the error rate. The CRF is then

primarily used to expose the image splicing implemented on the image's geometry invariant. In which the suspected boundary is identified within each region of the image and validated for identifying inconsistencies [3]. The bi-coherence features [4] are widely used for detecting splicing on images that estimate the mean of magnitude and phase entropy for augmenting the images. Furthermore, it extracts the features for the authentic counterpart and incorporates them to capture the characteristics of various object interfaces. Finally, the exact replicas are identified by matching the features pertaining to the block size, which is accomplished through the use of robust matching [5]. However, human intervention is required to interpret the output of replicas detection [6]. In general, region duplication is performed on an image based on geometrical and lighting adjustments. It is a very simple operation that involves copying and pasting a continuous portion of pixels to another location in the image. In this survey, we will look at common image tampering scenarios and prominent frameworks for detecting and localizing tampered regions in an image

2. SURVEY

The field of digital image forgery detection has grown significantly in order to combat the issue of image distortion in various areas such as legitimate administrations, medical sciences, and legal sciences [7]. For both Copy-Move and spliced images, Image Forgery Detection (IFD) techniques were used. The classification of Copy-Move images is dependent on variations in processing input images with or without transformation before extracting image features. Groups of detection techniques based on image features or camera features are summarized for the spliced images [8]. The identification of forgeries determines the authenticity of images. There are two types of image forgery detection techniques. They are as follows:

I.Active Forgery Identification Techniques

Pre-extracted or pre-embedded data is required for an active forgery detection method. Digital watermarking and digital signature [9,10] are well-known methods used in the active approach [16].

A. Image Watermarking

This type of image forgery adds a partially visible watermark to the photo. The attached information will be more or less transparent, making it difficult to see the watermark. Ferrara et al. [11] proposed a new forensic tool based on an interpolation process for analyzing original images and fake areas.A conditional co-occurrence probability matrix (CCPM) [12] that uses third-order statistical features in counterfeit detection can detect image splicing. Watermarking methods are usually classified as either reversible or irreversible. By using reversible watermark technology, irreversible image distortion based on the characteristics of the original image is avoided. Watermarks can be used primarily to identify the source of an image or an authorized consumer. This is a bit pattern inserted into digital media to identify the author [13]. Semi-vulnerable, vulnerable, and content-based watermarking technologies are primarily used in image authentication applications. Li et al. [14] advanced a brand new technique for detecting reproduction flow forgery that used the Local Binary Pattern (LBP) to extract round blocks. Preprocessing, characteristic extraction, characteristic matching, and submit processing are the levels concerned on this system. It is said right here that it's miles extraordinarily hard to hit upon forgeries while the place is circled at distinct angles. Hussain et al. [15] proposed a multi resolution Weber Local Descriptors (WLD) for detecting picture forgeries primarily based totally on chrominance issue features. The WLD histogram additives are computed right here, and the Support Vector Machine (SVM) classifier is used to hit upon forgery. In this paper, kinds of forgeries, specifically splice and reproduction-flow, are detected the usage of the multi-decision WLD approach.

B. Digital Signature

One of the active ways to detect forgery or tampering with an image is with a digital signature. Protecting the reliability of a digital document using a mathematical format is called a digital signature. Robust bits are extracted from the original image of the digital signature. Recipients can believe that the message was created by a recognized sender based on a valid signature. As a result, digital signatures are widely used in financial transactions, contract management software, and software distribution [17]. Digital signatures usually contain some secondary information derived from the image. In the early stages of this method [18], unique features are extracted from the image and used to verify the reliability of the image.

II. Passive Forgery Detection Techniques

Passive methods, also known as blind methods, rely solely on the image's authenticity and integrity [19]. The method assumes that, while there may be no visible signs of tampering in the image, tampering may disrupt the underlying statistics property due to noise inconsistency, image blurring, image sharpening [20], forgery through copy-move [21], and image inpainting [22], among other things. Forgery-dependent techniques are proposed to distinguish only specific types of forgeries, such as splicing, which are dependent on the type of forgery carried out on the picture [23].Forgery independent techniques detect forgeries that are not based on fraud but on artifact traces left behind by sharpening, blurring, and inconsistencies caused by shading and light effects. The

following passive forgery detection techniques are available:

A. Pixel-Based

Physical evidence of all kinds is analyzed in traditional forensic sciences. The pixel, the underlying building block of a digital image, is the focus of attention in the digital domain. Four techniques for detecting various types of tampering are examined here, each of which directly or indirectly analyses pixel-level correlations that arise from a specific type of tampering.

a.Splicing Method

Image splicing is a type of forgery detection method that creates a single image from the combination of two or more images [24]. It is also known as image composition because it involves various image manipulation operations.Many inconsistencies in image features are typically created as a result of the splicing operation. The composition between the two images is estimated and incorporated in this technique to create a bogus image. The difference between the illumination and reference illuminate color is estimated based on the image block content. It is extremely difficult to extract the exact shape of the image in this digital image forgery. Image splicing methods [25] are typically divided into two types: boundary-based and region-based. For verifying the authenticity of digital images, Alahmadi et al [26] proposed a passive splicing forgery detection mechanism. The features from the chromatic channel are extracted here in order to capture the tampering artifacts. For detecting splicing in digital images, Kakar et al [27] used a forgery detection approach. Small inconsistencies in motion blur are detected here by analyzing the special properties of image gradients [28]. Image subdivision, motion blur estimation, smoothing, blur computation, interpolation, and segmentation are the stages involved in this detection [29].

b. Copy-Move Method

Among other forgery methods, the copy-move method is a popular type of image tampering in which a specific portion is copied and pasted on another region [30]. The primary goal of this method is to conceal a significant element or highlight a specific object. Bayram et al. [31] developed an effective method for detecting copy-move forgery. The block matching procedure, according to the authors, is used to detect this type of forgery by separating the image into overlapping chunks. It also identifies duplicated connected image blocks by calculating the distance between neighbor blocks [32]. Because natural images contain many similar blocks, detecting duplicate blocks alone is insufficient for making a forgery decision [33]. Furthermore, the Fourier Mellin Transform (FMT) is used to perform operations such asImage forgery detection using scaling, translation, and rotation[34]. Mahdian et al. [35] made use of a detection technique for detecting copy-move forgery based on the invariants of the blur moment This discovery methodology can detect blur degradation, noise, and some other phenomena arbitrary changes in duplicate image regions, such as Gamma correction and noise addition Gamma is a nonlinear function. Individual pixel values can be adjusted. The procedures involved in this Methods include image tiling with overlapping images and representation blur moment invariants, transformation, similarity analysis, and the creation of a map for the detection of duplicate regions.

c. Image Retouching

Compared to other image forgeries, image retouching is regarded as the least dangerous forgery technique, as it allows for some image enhancement. It is also widely used in photo editing software and in magazines. For detecting copy-move forgery, Muhammad et al. [36] proposed an undecimated dyadic wavelet transformation technique. More sophisticated tools are typically available for creating this type of forgery by using a soft touch on the edges. As a result, distinguishing the color and texture of the stimulated and unoriginal parts is extremely difficult. Furthermore, because there are two or more identical objects in the same image, forgery detection becomes extremely difficult. As a result, the authors of this paper used similarity measurements to detect this forgery, in which the noisy inconsistency between the copied and moved parts is analyzed. Transformation methods such as FMT, Scale Invariant Feature Transform (SIFT), and Discrete Wavelet Transform (DWT) are claimed to be capable of detecting forgery in a highly compressed image. For detecting copy-move forgery, Ghorbani et al [37] proposed a Discrete Cosine Transform Quantization Coefficients Decomposition (DCT-QCD).Verifying the integrity and authenticity of digital images, particularly those used in news articles, medical records, and court cases, is a difficult process. Because for those types of images, a copy-move forgery could be created.

d. Statistical

There are a total of $256^{n\wedge 2}$ 8-b gray-scale images of size n x n that can be created. There are 10^{240} possible images with as few as n = 10 pixels (more than the estimated number of atoms in the universe). We would be extremely unlikely to obtain a perceptually meaningful image if we drew at random from this vast space of possible images. These findings imply that photographs have specific statistical properties[41]. The authors of [38] use a wavelet decomposition to compute first- and higher-order statistics. The frequency space was divided into multiple scale and orientation subbands using this decomposition. The statistical model is made up of the first four statistical moments of each wavelet subband as well as higher-order

statistics that capture the correlations between the different subbands. To classify images based on these statistical features, supervised pattern classification is used.

Fig- 1: Image splicing example where a is the authentic image, and b is the spliced image [60]

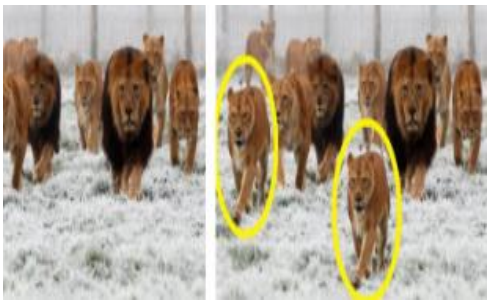

Fig- 2:.Example of copy–move forgery (a) Original image, (b) Forged image (duplicated object highlighted)[59]

(a) (b)

Fig- 3: Image retouching forgery: a original, b retouched image[61]

B. Format Based

The first rule of forensic analysis must definitely be maintenance of evidence. In this respect, irreversible image compression methods such as JPEG can be considered the worst enemy of forensic analysts. Therefore, it is ironic that the unique properties of lossy compression can be used for forensic analysis. This section describes three forensic techniques for detecting tampering with compressed images. Each technique explicitly uses the details of the irreversible JPEG compression scheme.

a. JPEG Quantization

The JPEG format is used by the majority of cameras to store images. This lossy compression scheme gives you some control over how much compression you get. Manufacturers typically configure their devices differently in order to balance compression and quality in accordance with their own needs and preferences. The standard JPEG compression scheme, given a three-channel color image (RGB), proceeds as follows: First, the RGB image is converted to luminance/chrominance space (YCbCr). When compared to the luminance channel, the two chrominance channels (CbCr) are typically subsampled by a factor of two (Y). The channels are then divided into 8 x 8 pixel blocks. These values are unsigned integers that have been converted to signed integers. A 2-D discrete cosine transform is used to convert each block to frequency space (DCT). Each DCT coefficient, c, is then quantized by an amount q:[c/q] depending on the frequency and channel.This is the main source of compression. The full quantization is specified as a 192-value table—a set of 8 x 8 values for each frequency, for each of three channels (YCbCr). These values tend toward 1 for low compression rates and increase for higher compression rates. JPEG encoders in digital cameras and photo-editing software use the above sequence of steps, with some variations. The choice of quantization table is the primary source of variation in these encoders. As a result, each JPEG image contains a sort of signature. As described in [39], the quantization tables can be extracted from the encoded JPEG image or blindly estimated from the image.

b. Double JPEG

Any digital manipulation necessitates the loading of an image into a photo-editing software programme and the resave of the image. Because the majority of images are stored in JPEG format, it is likely that both the original and manipulated images are stored in this format. The manipulated image is compressed twice in this scenario. Because the JPEG image format is lossy, this double compression introduces artifacts that are not present in singly compressed images. As a result, the presence of these artifacts can be used as evidence of manipulation [40], [42]. It should be noted that double JPEG compression does not always indicate malicious tampering.

c. JPEG Blocking

The block DCT transform serves as the foundation for JPEG compression. Because each 8 x 8 pixel in the image block is individually transformed and quantized, artifacts appear as horizontal and vertical edges at the border of neighboring blocks. These blocking artifacts may be disturbed when an image is manipulated.The authors of [43] use pixel value differences within and across block

boundaries to characterize the blocking artifacts. These differences are typically smaller within blocks than they are across blocks. When an image is cropped and recompressed, it may introduce new blocking artifacts that do not always align with the original boundaries. Within- and across-block pixel value differences are calculated using four-pixel neighborhoods that are spatially offset from each other by a fixed amount, with one neighborhood entirely within a JPEG block and the other bordering or overlapping a JPEG block.

C. Camera Based

Grooves in gun barrels give the projectile spin, which increases accuracy and range. These grooves impart slightly distinct markings to the fired bullet and can thus be used to associate a bullet with a specific handgun. In the same vein, several image forensic techniques that specifically model artifacts introduced by various stages of the imaging process have been developed. I'll go over four methods for modeling and estimating various camera artifacts. Any inconsistencies in these artifacts can then be used to prove tampering.

a. Chromatic Aberration

Light passes through the lens and is focused on a single point on the sensor in an ideal imaging system. Optical systems, on the other hand, deviate from such ideal models in that they fail to focus light of all wavelengths perfectly. Latitudinal chromatic aberration, in particular, manifests itself as a spatial shift in the locations where light of different wavelengths reaches the sensor. The authors show in [44] that this lateral aberration can be approximated as an expansion or contraction of the color channels in relation to one another.

b. Color Filter Array

A digital color image is made up of three channels, each of which contains samples from different bands of the color spectrum, such as red, green, and blue. Most digital cameras, on the other hand, have a single CCD or CMOS sensor and capture color images with a color filter array (CFA). The majority of CFAs use three color filters (red, green, and blue) that are placed atop each sensor element. Because only one color sample is recorded at each pixel location, the other two must be estimated from neighboring samples to produce a three-channel color image. CFA interpolation for demosaicing is the process of estimating the missing color samples. Kernel-based demosaicing methods that act on each channel independently are the most basic. To avoid blurring salient image features, more sophisticated algorithms interpolate edges differently from uniform areas. CFA interpolation, regardless of implementation, introduces specific statistical correlations between a subset of pixels in each color channel. These correlations are periodic because the color filters in a CFA are typically arranged in a periodic pattern. At the same time, the originally recorded pixels are unlikely to exhibit the same periodic correlations. As a result, these correlations can function as a type of digital signature. If the specific form of the periodic correlations is known, determining which pixels are correlated with their neighbors should be simple. On the other hand, if the pixels that are correlated with their neighbors are known, the specific form of the correlations can be easily determined. Of course, neither is known in practice[41].

c. Camera Response

Because most digital camera sensors are nearly linear, the amount of light measured by each sensor element and the corresponding final pixel value should be linear. Most cameras, on the other hand, use point wise nonlinearity to improve the final image. [44] describes how to estimate this mapping, known as a response function, from a single image. To detect tampering, differences in the response function across the image are used. Consider an edge where the pixels below it are the same color C_1 and the pixels above it are a different color C_2. If the camera response is linear, the intermediate pixels along the edge should be a linear combination of the adjacent colors. The camera response function is estimated using the deviation of these intermediate pixel values from the expected linear response. A maximum a posteriori (MAP) estimator is used to calculate the inverse camera response function, which restores the pixel colors to a linear relationship. Edges are chosen to stabilize the estimator so that the areas on either side of the edge are similar, the variances on either side of the edge are small, the difference between C_1 and C_2 is large, and the pixels along the edge are between C_1 and C_2. The estimated camera response function is also subject to constraints: it must be monotonically increasing with at most one inflection point and must be similar for each of the color channels. Because the camera response function can be estimated locally, significant differences in this function across an image can be used to detect tampering.

D. Physics Based

It is critical to capture a light image. Another significant issue in creating substantial spliced images is that the light-source side of the images being merged is paired. This light variation is used to demonstrate tampering in a photograph. Images are merged at the time of modification in this technique, which is acquired in various lighting conditions. By combining these images, it becomes difficult to match up the lighting state. The lighting inconsistency in the mixed images could be used to demonstrate the tempered portions of image forgery. Johnson and Farid [45] pioneered a method for dealing with these issues for the first time. They discover a method for assessing the side of a lighting source in the first degree of freedom in

order to demonstrate the effects of tampering. Johnson and Farid build a classifier to detect forgery that is dependent on lighting anomaly in[46] by assessing the direction and magnitude of the light source. This technique is inspired by an earlier technique[47], even though this generalized classifier assesses extra complex illuminating and may be adapted to a single illuminating resource. It evaluates model parameters based on a single image.

a. Light Direction(2D and 3D)

The authors of [48] describe a model for assessing the 3-D lighting environment using a low-dimensional model. It evaluates model parameters based on a single image.In [49], the researcher proposes a method for displaying the results of forged image parts that are dependent on anomalies in light direction. Using blind identification methods, the above method was used to estimate the plane normal matrix of the image. The researcher obtained 87.33 percent accuracy for forgery detection using this model.In [50], researchers used a 2D lighting system to develop a method that relies on the tempering part of image detection. It does not estimate the object's 3-D shape.In [52], researchers describe a model for detecting tempered images that is based on anomalies in lighting color. On images of identical material, knowledge is applied via a physical or statistically-based illuminate assessor. The SVM meta-fusion model is used. The researcher obtained an accuracy of 86 percent for forgery detection using this method. The advantages of this approach are that it creates lighting anomalies within the forged image, which are easily visible.

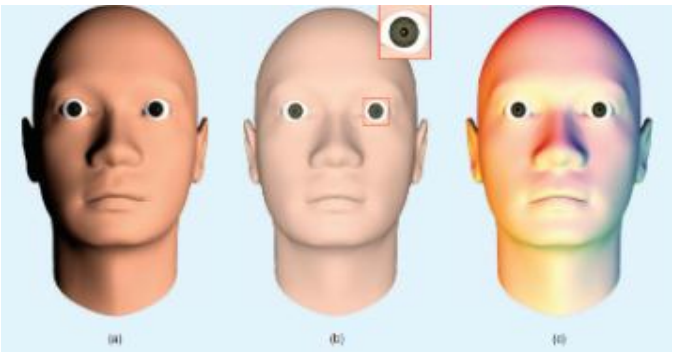

Fig-.4: The direction to a single light source can be determined from (a) the lighting gradient across the face or (b) the position of the specularity (white dot) on the eye. More complex lighting environments consisting of multiple colored lights (c) can be modeled as piecewise continuous functions on the sphere.[41]

b. Light Environment

The two preceding sections assumed a simplified lighting model with a single dominant light source. In practice, however, lighting a scene can be complicated: any number of lights can be placed in any number of positions, resulting in various lighting environments. The authors of [51] explain how to estimate a low-parameter representation of such complex lighting environments.

E. Geometric Based

The image is transformed into geometric primitives such as angle movement curves and points to yield a geometric method. Variations of the calculated principal point throughout the image may be used to demonstrate the picture's originality.

a. Principle Point

The principal point (the projection of the camera center onto the image plane) is near the image's center in authentic images. When a person or object in the image is translated, the main point is moved proportionally. Variations in the estimated principal point across the image can thus be used to detect tampering. The authors of [52] described how to estimate the principal point of a camera from the image of a pair of eyes (i.e., two circles) or other planar geometric shapes. They demonstrated how translation in the image plane corresponds to a shift of the principal point. Inconsistencies in the main point across an image can then be used to demonstrate tampering.

b. Metric Measurement

The authors of [53] review several projective geometry tools that allow for the rectification of planar surfaces and, under certain conditions, the ability to make real-world measurements from a planar surface. Three methods for rectifying planar surfaces imaged with perspective projection are described. Each method only necessitates the use of a single image. The first method makes use of prior knowledge of polygons of known shape. The second method necessitates knowledge of two or more vanishing points on a plane as well as, for example, a pair of known plane angles. The third method necessitates the use of two or more coplanar circles. In each case, the world-to-image transformation is estimated, allowing planar distortions to be removed and metric measurements to be taken on the plane.

III .Deep Learning Based Method

Researchers were inspired by advances in GPU technology and the success of deep learning (DL) [54] technology in computer vision to detect image corruption using DL models. DL is a combination of feature extraction and classification. This technique is data-driven and allows you to learn the abstract and complex functions needed to identify the manipulated area. In addition, you can save the time and effort required to find handmade features from manipulated images.Deep learning model training,

on the other hand, is difficult and necessitates a large amount of computational power as well as a large amount of data. There are numerous DL models, including Convolutional Neural Networks (CNN), Deep Neural Networks (DNN), and Recurrent Neural Networks (RNN) (RNN). Among these DL models, Convolutional Neural Networks (CNN) are popular. CNN includes a convolution layer that serves as a discriminator and feature extractor.CNNs typically extract features based on image content rather than image processing capabilities. By suppressing image content, Bayar etc. [55] proposed a new convolution layer to learn image manipulation functions. This layer considers the local structural relationships between pixels, not the content of the image, as the operation modifies some local relationships. This allows you to detect multiple instances of tampering in a single image. The limitation of updated recognition methods is that you can provide satisfactory results for some operating attacks. In addition, most of the work is interested in JPEG images in which the operating range is detected in a large number of JPEG compression operations to find the operation area. Using a frequency domain as input, CNN makes use of DCT coefficients for every patch. Using a frequency domain CNN is made from convolutional layers, pooling layers, and 3 complete connections. Multi-area CNN combines the outputs of those networks' absolutely related layers and classifies the patch into certainly considered one among 3 categories: uncompressed, single compressed, or double compressed.[55] proposes the use of residual noise features to detect and locate image tampering. CNNs are used to extract noise residual-based features from images, and SVMs are used for classification. Rao et al. [57] suggested using CNN to detect image copying and splicing. The first convolution layer of the CNN is used for pretreatment to determine the impact of the tampering operation. CNNs were trained using marked path samples extracted from training images. We then applied a pre-trained CNN to the test image and used an SVM classifier to detect tampering. Bi et al. [58] propose a CNN-based method for image splicing detection called Ringed Residual U-Net (RRU-Net), which is an end-to-end image segmentation network. RRU-Net aims to improve CNN learning by utilizing the human brain's recall and consolidation mechanisms. The residual propagation technique is used to recall the input feature information in order to solve the degradation problem in the deeper network; the residual feedback technique consolidates the input feature information in order to distinguish between authenticated and forged regions.

3. ANALYSIS OF IMAGE FORGERY DATASET

The dataset, which includes both authentic and forged images, is required to assess the performance of the image tampering algorithm. There are two kinds of image tampering algorithms: I algorithms that generate binary output (as original/tampered at the image level), without localization of the tampered region, and (ii) algorithms that generate localization of the tampered region (at the pixel level).

Columbia Gray, the first publicly available online dataset, was published in 2004. This dataset contains grayscale blocks extracted from 322 photos. To overcome this limitation, the Columbia team published a new dataset with color images in 2006, but it contains images with unsatisfactory tampering effects.

Dataset	Authentic image	Tampered Image	Image Size	Format	Mask
Columbia Gray	933	912	128*128	BMP	No
Columbia Color	183	180	757*568 (authentic) 1152*768(tampered)	TIFF	Yes
CASIA V1.0	800	921	384*256	JPEG	No
CASIA V2.0	7491	5123	240*160 (authentic) 900*600 (Tampered)	TIFF/JPEG	No
MICC-F220	110	110	722*480 (Authentic) 800*600 (Tampered)	JPEG	No
MICC-F200	1300	700	2048*160	JPEG	No
IMD	48	48	3000*2300	JPEG/PNG	Yes
MICC-F600	440	160	800*533 (Authentic) 3888*2592(Tampered)	JPEG/PNG	Yes
CoMoFoD	5200	5200	512*512	JPEG/PNG	Yes
Carvalho	100	100	2048*1536	PNG	Yes

Table - 1: Publically available image forgery dataset

The CASIA team published two tampering datasets in response to the growing demand for larger datasets. The Columbia datasets only include spliced images, whereas the CASIA datasets include both copy-move and spliced images. The MICC datasets, like the Columbia datasets, contain images with visible tampering effects. The tampered regions in the images are regions that were chosen at random from the same images.

4. CONCLUSIONS

This paper examined various image forensics approaches for detecting forgeries on digital images. This paper investigates digital signature, digital watermarking, copy-move, image splicing, image cloning techniques, pixel based etc. The majority of the authors stated that image forgery detection is a highly complicated process due to the introduction of various technologies. Tools for manipulation and editing The feature is also making an appearance. Because the features are so important in forgery detection, Some forgery operations are acutely vulnerable.

REFERENCES

[1] V. Christlein, C. Riess, and E. Angelopoulou "On rotation invariance in copy-move forgery detection"2010 IEEE International Workshop on Information Forensics and Security, 2010.

[2] E. Kee and H. Farid "Exposing digital forgeries from 3-D lighting environments", IEEE International Workshop on Information Forensics and Security (WIFS), 2010

[3] M. Kobayashi, T. Okabe, and Y. Sato, "Detecting forgery from static scene video based on inconsistency in noise level functions", IEEE Transactions on Information Forensics and Security, vol. 5, pp. 883-892,

[4] Z. He, W. Sun, W. Lu, and H. LuDigital image splicing detection based on approximate run length Pattern Recognition Letters, vol. 32, pp. 1591- 1597, 2011

[5] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Accurate and robust localization of duplicated region in copy–move image forgery Machine vision and applications", vol. 25, pp. 451-475, 2014.

[6] D. Cozzolino, D. Gragnaniello, and L. Verdoliva "Image forgery detection through residual-based local descriptors and block-matching",IEEE International Conference on ICIP 2014

[7] B.Mahdian and S.Saic, (2010), "Blind methods for detecting image fakery." IEEE Aerospace Electron System Management, pp.18-24.

[8] Shwetha B and S V Sathyanarayana, (2017), "Digital image forgery detection techniques: a survey." ACCENTS Transactions on Information Security, Vol.2 (5).

[9] C.S.Lu and H.Y.Mark Liao, (2003), "Structural digital signature for image authentication: An incidental Distortion Resistant Scheme." IEEE Transactions on multimedia.

[10] H.Bin Zang, C.Yang and X.Mei Quan, (2004), "Image authentication based on digital signature and semi-fragile watermarking." Journal of Computer and Technology.

[11] P. Ferrara, T. Bianchi, A. De Rosa, and A. Piva, "Image forgery localization via fine-grained analysis of CFA artifacts," IEEE Transactions on Information Forensics and Security, vol. 7, pp. 1566- 1577, 2012

[12] A. Kashyap, R. S. Parmar, M. Agrawal, and H. Gupta, "An Evaluation of Digital Image Forgery Detection Approaches," arXiv preprint arXiv:1703.09968, 2017.

[13] S. Mushtaq and A. H. Mir, "Digital image forgeries and passive image authentication techniques: A survey," International Journal of Advanced Science and Technology, vol. 73, pp. 15-32, 2014

[14] L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, "An efficient scheme for detecting copy-move forged images by local binary patterns," Journal of Information Hiding and Multimedia Signal Processing, vol. 4, pp. 46-56, 2013.

[15] M. Hussain, G. Muhammad, S. Q. Saleh, A. M. Mirza, and G. Bebis, "Image forgery detection using multi-resolution Weber local descriptors," in 2013 IEEE EUROCON, , 2013, pp. 1570-1577

[16] Z.Zhang,Y.Ren.X.J.Ping,Z.Y.He and S.Z.Zhang, "A survey on passive blind image forgery by doctor method detection." International conference on Machine learning and cybernetics,2008, pp.3463-3467

[17] S. Mushtaq and A. H. Mir, "Digital image forgeries and passive image authentication techniques: A survey," International Journal of Advanced Science and Technology, vol. 73, pp. 15-32, 2014

[18] T. Mahmood, T. Nawaz, R. Ashraf, M. Shah, Z. Khan, A. Irtaza, et al., "A survey on block based copy move image forgery detection techniques," in Emerging Technologies (ICET), 2015 International Conference on, 2015, pp. 1-6.

[19] H.Farid, (2006), "A survey of image forgery detection." IEEE Signal Processing Magazine, pp.6- 25.

[20] Z.Y. and N.R.Cao Gang, (2009), "Detection of image sharpening based on histogram aberration and ringing artifacts." IEEE ICME, pp.1026-1029.

[21] F.Peng,Y.Nie and M.Long, (2011) "A complete passive blind image copy-move forensics scheme based on compound statistics features." International journal of Forensic science, pp.21-25

[22] Y.Q.Zhao, M.Liao, F.Y.Shih and Y.Q.Shi, (2013), "Tampered region detection of inpainting JPEG images." International Journal on light electron optics, pp.2487-2492.

[23] Z.Zhou and X.Zhang, "Image splicing detection based on image quality and analysis of variance." International Conference on education technology and computer (ICETC)2010, pp.242-246.

[24] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey on Keypoint Based Copy-move Forgery Detection Methods on Image," Procedia Computer Science, vol. 85, pp. 206-212, 2016/01/01/ 2016.

[25] T. Huynh-Kha, T. Le-Tien, S. Ha-Viet-Uyen, K. Huynh-Van, and M. Luong, "A Robust Algorithm of Forgery Detection in Copy-Move and Spliced Images," International Journal of advanced Computer SCience and Applications, vol. 7, pp. 1-8, 2016.

[26] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," in Global Conference on Signal and Information Processing (GlobalSIP), 2013 IEEE, 2013, pp. 253-256.

[27] P. Kakar, N. Sudha, and W. Ser, "Exposing digital image forgeries by detecting discrepancies in motion blur," IEEE Transactions on multimedia, vol. 13, pp. 443-452, 2011

[28] A. C. Gallagher and T. Chen, "Image authentication by detecting traces of demosaicing," in Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on, 2008, pp. 1-8.

[29] J. G. Han, T. H. Park, Y. H. Moon, and I. K. Eom, "Efficient Markov feature extraction method for image splicing detection using maximization and threshold expansion," Journal of Electronic Imaging, vol. 25, p. 023031, 2016

[30] Z. Mohamadian and A. A. Pouyan, "Detection of duplication forgery in digital images in uniform and non-uniform regions," in Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on, 2013, pp. 455-460

[31] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.

[32] M. Jaberi, G. Bebis, M. Hussain, and G. Muhammad, "Improving the detection and localization of duplicated regions in copy-move image forgery," in Digital Signal Processing (DSP), 2013 18th International Conference on, 2013, pp. 1-6.

[33] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, R. Ramli, R. Salleh, S. Shamshirband, et al., "Copy-move forgery detection: Survey, challenges and future directions," Journal of Network and Computer Applications, vol. 75, pp. 259-278, 2016.

[34] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," Forensic science international, vol. 171, pp. 180-189, 2007.

[35] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digital Investigation, vol. 9, pp. 49-57, 2012

[36] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on, 2011, pp. 1-4

[37] H. Farid and S. Lyu, "Higher-order wavelet statistics and their application to digital forensics," in Proc. IEEE Workshop on Statistical Analysis in Computer Vision (in conjunction with CVPR), Madison, WI, 2003

[38] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," IEEE Trans. Image Process., vol. 12, no. 2, pp. 230–235, 2003.

[39] J. Lukas and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in Proc. Digital Forensic Research Workshop, Cleveland, OH, Aug. 2003.

[40] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in Proc. 6th Int. Workshop on Information Hiding, Toronto, Canada, 2004, pp. 128–147.

[41] Farid, Hany. "Image Forgery Detection A survey". Signal Processing Magazine, IEEE. 26. 16 - 25. 10.1109/MSP.2008.931079,2009

[42] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in Proc. IEEE Conf. Acoustics, Speech and Signal Processing, Honolulu, HI, 2007, pp. 217–2

[43] M. K. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in Proc. ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006, pp. 48–55

[44] Z. Lin, R. Wang, X. Tang, and H-V Shum, "Detecting doctored images using camera response normality and consistency," *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, 2005, pp. 1087-1092 vol. 1, doi: 10.1109/CVPR.2005.125.

[45] J. Lukas and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in Proc. Digital Forensic Research Workshop, Cleveland, OH, Aug. 2003

[46] J. Lukás, J. Fridrich, and M. Goljan, "Digital camera identification from sensor noise," IEEE Trans. Inform. Forensics Security, vol. 1, no. 2, pp. 205–214, 2006.

[47] E. Kee and H. Farid, "Exposing digital forgeries from 3-D lighting environments," in 2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010, 2010, vol. 03755, pp. 1–6, doi: 10.1109/WIFS.2010.5711437

[48] Y. Lv, X. Shen, and H. Chen, "An improved image blind identification based on inconsistency in light source direction," pp. 50–67, 2011

[49] W. Fan, K. Wang, F.-S. H, and C. Science, "3D LIGHTING BASED IMAGE FORGERY DETECTION USING SHAPE FROM-SHADING GIPSA-Lab , 11 rue des Math ´ eres Cedex , France," 2012, no. 2011602067, pp. 1–5.

[50] T. J. De Carvalho et al., "Exposing Digital Image Forgeries by Illumination Color Classi fi cation," vol. 8, no. 7, pp. 1182–1194, 2013, doi: 10.1109/TIFS.2013.2265677.

[51] M. K. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Trans. Inform. Forensics Security, vol. 3, no. 2, pp. 450– 461, 2007.

[52] Johnson, Micah & Farid, Hany. (2007). Detecting Photographic Composites of People. 19-33. 10.1007/978-3-540-92238-4_3.

[53] M. K. Johnson and H. Farid, "Metric measurements on a plane from a single image," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2006- 579, 2006.

[54] Y. Zhang, J. Goh, L. L. Win, and V. L. Thing, "Image region forgery detection: A deep learning approach.," in SG-CRC, pp. 1–11, 2016.

[55] B. Bayar and M. C. Stamm, "A deep learning approach to universal image manipulation detection using a new convolutional layer," in Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, pp. 5–10, ACM, 2016.

[56] D. Cozzolino and L. Verdoliva, "Single-image splicing localization through autoencoder-based anomaly detection," in 2016 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–6, IEEE, 2016.

[57] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in 2016 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–6, IEEE, 2016.

[58] X. Bi, Y. Wei, B. Xiao, and W. Li, "Rru-net: The ringed residual u-net for image splicing forgery detection," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 0–0, 2019.

[59] Dixit, Rahul & Naskar, Ruchira." Review, Analysis and Parameterization of Techniques for Copy-Move Forgery Detection in Digital Images" IET Image Processing. 11. 10.1049/iet-ipr.2016.0322,2017

[60] Moghaddasi, Zahra & Jalab, Hamid & Md. Noor, Rafidah," Image splicing forgery detection based on low-dimensional singular value decomposition of discrete cosine transform coefficients". Neural Computing and Applications. 31. 10.1007/s00521-018-3586-y,2019

[61] alZahir, Saif & Hammad, Radwa. (2020). "Image forgery detection using image similarity". Multimedia Tools and Applications. 79. 10.1007/s11042-020-09502-4.