Active and Passive Detection of Image Forgery: A Review Analysis

Md. Ashif Raja
Department ofCS & IT
Maulana Azad National Urdu University,
Hyderabad India-500032

***Abstract*:- Image Forgeries are very old issue.The issue is being continued fromprimitive time to till time for a mankind. Images are being used as evidence or events from ancient times. Now the current time, by using image preprocessing tools and low-cost hardware, images can forgedwithout difficultiesto obtainlawlessbenefiteither making false propaganda or getting own selfish objectives . So, to analyze perceptibly that the picture is forged or original is very difficult for a human. Technology has been modernizedto test the authenticity and reliability of digital pictures.To solve these issues lots of research has been proposed. In this survey paper, enormous literature reviews of state-of-the-art methods of passive technique have been discussed and it types that has been explained for exposing the temper part of image.**

Keywords:- Digital image, Digital Image Forgery, Copy-Move Image forgery, Image Forgery Detection, Tampering, splicing,post-processing, resampling Digital Forensics, Duplication Forgery. Detection.

INTRODUCTION:

Forgeries are very old problem for a mankind. It is Universal truth that image speaks more truth compare to words. Due to advancement of technology no one can easily trust that is provided as a proof of evidence. These days'imagesperform avitalcontribution in communication media. The advancement technologies develop better editing tools and software to manipulate images easily.The most popular image editing software tools like Cameran360, Adobe Imageshop, SkylumLuminarACDSeeImageShop Pro, Corel PaintShop pro etc. are available using which any given image can be easily tempered. Which can lead to seriousconsequences, these tampered images can be presented as a part of evidence in court that makewrong results.

Digital imageforgery isthepart of image forensicin whichwe studyimages of a specific scenario to demonstrategenuineness and reliability by different techniques.

These manipulated imagesincrease on internet and multimedia very expeditiously. The advanced new digital technologies, easy availability with low cost of processing devices and tools, widespread transmissions overmany website like Facebook, Twitter, Telegram Pinterest etc., broadcasting news, these totally uplift a dangerous and seriouscase for the world.This also shows a big problem and increases the impurity of digital images. In this consideration forgery detection of image is main objective of image forensic. Therefore, tocheck the originality of the images is more compulsory, specifically,considering theseimages are submitted as proof of a person in a Court of justice, a person's overall authentic records(Aadhar card, Id card, Bank passbook), as financial documents, as newspapers, as a part of medical records orEducation records of a person in school, college or University.In addition, imagegraphs are constantly recompressed and re-sized, making this easier to share them over the Internet due to the proliferation of cloud-based image sharing and editing platforms like Picasa and Flickr, brought on by social media apps such as WhatsApp, Instagram and Snapchat.

Various aspects of image forgery detection are introduce in this review paper;Adetailed explanation of differentimage forgeries;theirkinds and algorithm and methodswhich is for finding the forged results of images. Thissurvey gives the drawback of differentcontentious temperingwhich have occurred in history. It provides arelativesurvey of present methods with its pros and cons. To show the detection of tempering is one of the ways of authentication, which means that the realimages has fewimplicit patterns. It also outlines the good points and bad points of imagetempering detection techniquespresently in use.

2.Literature review: The image forgery categorization is depends on whether taken images are real or fake. Forgery detection approach are mainlygrouped into two types[1]. These are as follows:

A. Active authentication

B. Passive authentication

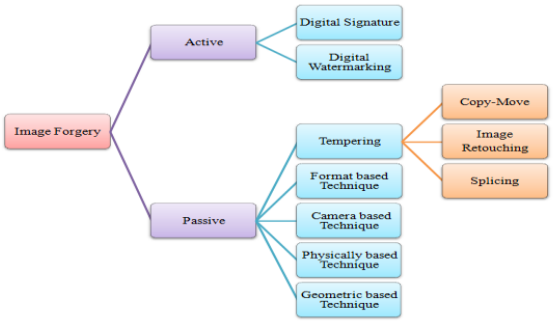


Fig: DIGITAL IMAGE FORGERY DETECTION TECHNIQUE

A.) Active authentication: In this perspective, digital pictureneed of preprocessing of picture like watermark insertedor createda signature on picture, thatrestrict theirsusage in practice[3]. Digital Signatures and process of authentication. Further,Activeauthentication technique is classified into two ways: first one is digital signature and second is

watermarking.It done during the time of checks out the code and validate the originality of the image.

1) Digital signature: This one is mathematical approachapplied to confirm the integrity and authenticity. Digital signature comes under active methods applied for detection of image forgery.Digital Signature equivalent to the handwritten signature in which itpossess a key or signature, a digital signature provideexcessimplicit security.A secret key X is applied to produceYarbitrary matrices with entries homogeneously divide up in the range [0, 1] in Digital Signature.In [2] authors proposed a method of a low phase filter usedforevery random matrix recurrently to acquired X random pattern.The model generates a digital signature using through the signing operation to the image. Imagesigningoperation contains the under-mentioned phase:-

i) By applying parameterized wavelet feature images are decomposed.

ii) Extract the Standard Digital Signature.
iii) The crypto signature producesthrough the private key and hash the extracted the Standard Digital Signature Cryptographically.

iv) Digital images along with crypto signature are delivered to the client.

(2.) Digital watermarking:The word watermarking is coined from the conventional use of placing a visible

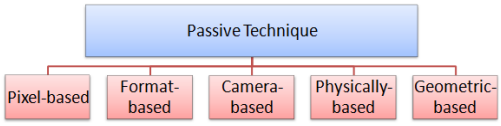


Figure: Passive-Based Technique of Image Forgery Detection

(1)Pixel-based technique- In this technique,the detection of forgeries involves pixels of the digital images. Pixel-based are four types.
(2) Format basedtechnique- In this technique, the detection of forgeries based on JPEG Extension. Format based Are three types.
(3) Camera-based technique- In this technique,pictures or imagesare captured by digital camera after that a sequence of processing including JPEG compression, white balancing, colour correlation, texture, quantization, filtering, gamma correction, blurring, and cropping steps applying on images.
(4) Physically-based technique- In this technique,it involve

Watermarks method based on active technique for image forgery detection generally make use of data hiding. Inactive authentication methods before knowledge about the imageare not dispensable to the watermark on paper.This one is apply for imagetempering detection. Digital Watermarking possess certain qualities like imperceptibility and robustness.While Others technique merge a maximum distance There is another which merge a maximum distance linear shift register range to the pixel data after thatrecognize this watermark throughevaluating by spatial cross-correlation function to the series.This formulatesto be hidden in with camera.These are partially visible watermarks but visible watermarks as well exist. Except this, a visually unidentifiable watermarking pattern is as wellexistthatmayshow the variation in one pixels and it can showswhere the variationoccurs [4]. At the time of creating digital image the watermarks are embedded on it. Active technique has some limitations because itneededfew human interference andespecially equipped cameras. Reducing these issuesof image forgery a passive authentication proposed.It is also behave as non-blind detection.

(B). Passive authentication: In this the identity of the client is checked and confirmed without requiring specific additional actions for the purpose of authentication. It is also behave as blind detection. In this technique there is no prior information related to Image.Assessing the originality and authenticity we used passivedetection technique on images, without any using of active technique like watermarking and digital Signature. These are based on the assumptionswhich tell there are no clues of forged region on digital image andthis may disturb the underlying imageregularity of our surrounding sightimage thatinitiates new artifacts manufacturing in numerous types of anomalies.Forged region of image is also referred as anomaly of the image. The techniques of passive image authentication chiefly classified into 5 types [1]

in the objects and light interaction with 3D. For capturing aimage light s very important.

Think about the twinkling of stars in the night, walking down in the garden to see the stars. Both types of images created by cloning together to make one image. This comes under Physical based forgery.
(5) Geometric based technique- In this technique,detection ofthe forgeries involvedby measurements of objects at geometry level.

(A.) Pixel-based detection: These are grouped in fourtypes:

(i.) Copy move: Thisimage tampering technique is the most prevalent technique. In copy move techniques involves copy a particular area from one picture and pasteit to another picture. After all the duplicated area belongs to the realpicturethus dynamic range and color remain suitable with the remainsof the picture[5].

Following steps are possessed by CMFD. This is general approach for CMFD:

Pass 1. Put the input image into the system.
Pass 2. Division of overlapping blocks.
Pass 3. Features Extraction using any algorithm like DWT(Discrete wavelet transform),DCT(Discrete Cosine Transform),PCA(Principal Component Analysis), etc.

Pass 4. Block Matching using algorithm like Radix sort, K-D Tree, Quick-Sort, Bucket -Sort, etc.

Pass 5. Explore duplicate vectors.
Pass 6. Block matching Performed.
Pass6. Locate the forged Region.

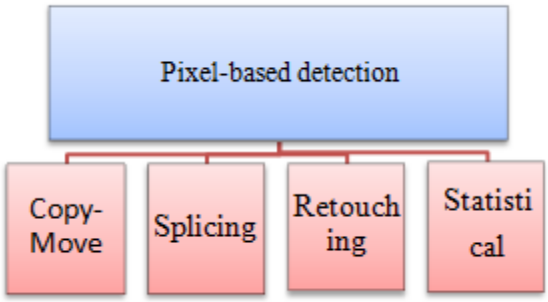


Fig: Pixel-Based Forgery Detection

Few parameters such as scaling, blurring, noise, color from the tempered imagemay be impossible to distinguish. From the pastsurveyCMFDis classified into[6]: way. These are as follows:
A) Block-based algorithms: In this method takenpicture is separate among overlapping blocks of picture.Forged area isreceived after comparison ofblocks pixels.This technique involves:

Discrete Cosine Transform is mathematical function it express a finite sequence of data points interms of a sum of cosine function used for feature extraction in images. This observes the forgedareas of the image.
· Principal Component Analysis: It is statistical procedure to detract the block feature dimensions of the image. Except from the above-stated method in tempering, the feature ofimagecomputation is verysignificant to acquire thescaling, rotation, compressions and time complexity improvements.So for the scaling and rotationwe apply feature key-pointdependedmethod.
B) Feature key-point based:
some possess that come underFeature key-point are mentioned below:

· SIFT- In computer vision,Scale-invariant feature transform isa feature detection algorithm appliedfor detecting and describing the local features ofpictures.Host imagesare extracted for duplicate detection or tempering.

· SURF-This Speed up Robust Featuremethodhave beenapplied for feature extraction and alsoapplied to locate and distinguish objects, to designed 3D scenes, to detect objects. This is a patented local feature detector and descriptor.

Fast and robust CMFDtechniques are createdbymerging of the block-based and feature-based algorithms. However the abovemethodsmayenhance computational complexity and show
tempered regionof the image with high accuracy but some ofissuesthatdecrease the recall rate due to regularity in blocking techniques. Recent techniques minimizing these problems and depend on[6]flexible over-segmentation along with feature dotmatched up. In this proposed model, the partitions of blocks areirregular blocks and not overlapped.By using feature point matching and adaptive over-segmentation technique recall rate was raiseddue toirregularity in the blocks.

ii. Image splicing: It is also known as copy paste forgery. In Image Splicing we add more than singleimages to make one. It changes the overall meaning of realimage and generates a forged image. Spliced images shows,blur, edges, lines, particular forged area, and color. The developments of the software processing tools have made tempering like color, texture, to addin imagewhich is visually hardlynoticeable for human. So Splicing is big issues for researchers.

ImageSplicing and Steganography are two different techniques in forgery detection. However, these two techniques used for temperedimages. Hence, statistical approaches such as SIFT; SURF etc. are used to find outthis trace[7]. The image-splicing method possesses dimensional feature vectors. There are mainly fourwaysthat is used for steganalysis which was applied on images. Researcher acquire 80% accuracy in this model of image splicing detection[7].
The applications of this technique are:

· 2-Dimensional Markov chain-By using these three directions (the main diagonal, horizontal, vertical) feature is extracted. In this model researcher acquired 76.25%.accuracy for forgery detection.

Singular Value Decomposition– It isdependingon 50-Dimensional characteristicsvector combined by DCT. The researcher obtains 78.82% of detection accuracy.

Addition of One-Dimension and Two-Dimension - statistical moments of One-Dimension and Two-Dimension characteristic features arederive through local domain along withMB-DCT are merged.In this model researcher acquired 87.07%accuracy for forgery detection.
iii.Image retouching: The retouching means enhanced or reduces lighting, blurring, Texture of the image.Image retouching usedin fashion photography and many commercial applications. In retouching only single image used for tempering. Available of original make the retouching to detect easily. Image retouching is usedfor showing the redness, blurring, enhancements, color changes and brightness or lighting effect in the temperedimages. There are Global or local modifications done in retouching[8]

In copy-move only local modification can be applied whilein retouching global modification can be applied. Global modification containsbrightness,Texture and blurring.

In [9]to detect between tempered and original image a model is proposed. It possess some process such that a change in texture, lightness, color, blurring etc.

In [10], an algorithm explainsa procedure which gives indication about histogram equalization along with find the global enhancement.

As the same method which depends on the probabilistic method of picture-element was elaborated in[11].Itapproximatesto show thepercentage of contrast modification. It provides morecorrect results in terms of enhancement which wasNonstandard. Some enhancement algorithms are discussed which easily detect the tempering and what the processing or modification is applied on image in either globally or locally and in both way [10][12]. Thismay befeasible that the part of the picture is untouched at all in false captioning.However,the inscription of the picture thatgivesthe background isaltered through the realconditionand the intent to misguide the viewers and readers.

Authors in [8]purpose amethod whichshows contrast.The binary equality assessesfunctions andgives the variations. Theactual and efficacious outcomes are created in circumstance of the images which is deeplyconverted.

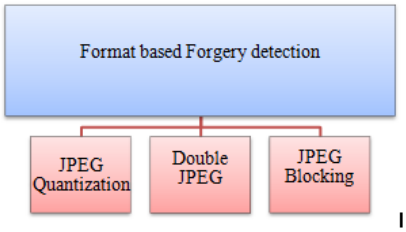
In[13]proposed a model for finding thegamma correction for detecting tempered images. This method has depended on the evaluation of histogram features which are estimatedthroughpeak gap characteristics. These characteristics are distinguishedthrough pre-processing histogramsin order to gamma improvement for detectingin pictures. The outcomesof themethod showincredibly helpful for allglobal along with local gamma improvement alteration.

In [14] the researchers proposea wayto detectthe retouching whichis based on bi-Laplacian filtering. Themethod applies on matching blocks based on a K-D tree sorting method for everyblock of images. Since image is two dimensional arrays so K-D Tree works well in low dimension. This method also works well for both either compressed or uncompressed images. Accuracy as wellrelies on the region of the tampered partsof the compressed images. There areTwo methodsproposed in [15]for showing the results of increasing the contrast in pictures. Thisshows the percentage of contrast increaseused for JPEG-compressed pictures. Primary method of this model ishistogram peak/gap which artifacttransactedfrom JPEG compression along with picture-element amount mappingisexplored in theory and differentiatethroughrecognizeby zero-height gap fingerprint.One more method in the similar paper developedan algorithm to recognize the compoundpicturemadethroughapplying the contrast adjustment eitheron one side or both side of origin area. These pick/gap bins are grouped together to recognize the percentage of contrast improvement. This algorithmused for completelydissimilarsource areas. The above two methods are very successful for detection of forgery images.

Authors in [16] proposed a method which is depend on photo-response non-uniformity (PRNU).By applying sensor pattern noise, it finds out the forged images. This methodexhibitsbetter results and broadutilization. There are manyalgorithms and techniques have beenintroducedwhichtalk over the retouching image forgery. The extent of the most of the methods performsnicely if the image is too much tampered incompare to the realimages.

iv.Statistical based: Statistical analysis of input image, $I_i(x, y)$: In this step statistical analysis of input image is done using various measures like mean, mode, median, variance, standard deviation, covariance, skewness, kurtosis etc. Selection of statistical measure: Depending upon the requirements in output optimized image, the statistical parameter is chosen.

B)Format-based technique: Thisone is common images formats used current time is the JPEG lossy compression format.[17]Images alteration does not validate malicious manipulation of color adjustment for imagesimprovement, image format modification and image compression.Quantization table determine the property of apicture and the size. This table tends to distinguish among camera maker. Thesetempering do not change the fundamental parts of realimages, however,malicious manipulationmaychange the value of images, likemodifying aimages in a scene.Clearly, this method doesn't perform well in order to non-JPEG imagesand thesedependoverartifacts proposed through JPEG procedure.These malicious tampering in collaborate with consequent manipulation likecolor adjustment, contrast adjustment, JPEG compression, Texture effect, etc., would difficult to detect such retouching easily. Therefore picture-tempering detection determined whether the picturesare real, authenticate and it also helpingfor furthermore study.



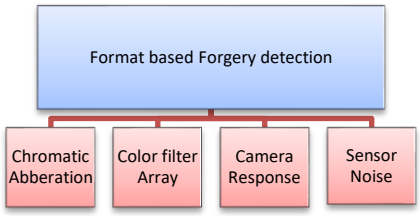
In [17], [18], researcher hasexplain a way to recognize bitmap compression history.This method shows the origin of the lossy compression. The prime motive of this paper is not for forgery detection. This will give us indirect proofof forged area. Due to block artifacts Jpeg images may be different. There is other challenge concerning JPEG forgeries are that detecting the double JPEG compression.Similar compression rise to fixed artifacts thatutilized to disclose forgery.Detectionof double

compression may optional implies formalicious intent. For instance, over a communication network,this is fully achievable to turn back aimages with a low quality factor in order to faster transfer.

In [19], Researcher has introduced a way to recover the first quantization coefficients of the first jpg compression in a double compressed jpg images. He estimates the first quantization matrix through a double-compressed JPEG picture.In this model, if the second quantization factor is lower than the first one then the first quantization coefficient s can be determined.

In [20], Researcher hasproposed a model to estimate JPEG images compressed or not. It used discrete cosine transform coefficients for feature extraction which is initiated by dual JPEG compression. It depends on DCT coefficients of histogram.

C.) Camera-based techniques:In this technique,pictures or images are captured by digital camera after that a sequence of processing including JPEG compression, white balancing, colour correlation, texture, quantization, filtering, gamma correction, blurring, and cropping steps applying on images. Some artifacts exist in cameras that may be applied forimages withstandard cameras. Many Differentmethods exist to facilitate this form of images forensics.Low priceand more cameras is being replaced by typical cameras. In daily lifeimages are achieved throughdifferent companies of cameras, likeLeica, Sony, Fujifilm, Pentax, Panasonic, Canon, Nikon, etc.



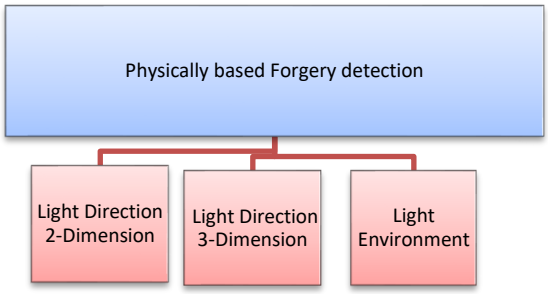
Theprimary issuesof thisresource identification are the categorization of camerasfor thetakenimages.

The bad impact of these methods does not mean that picture may not be made through a camera by a specific lens, due to the lens can have been cleaned of the dust.For the resolve of this issue,we shouldexamine the interchangeable images file format (EXIF) header of the outcomeimages for camera identification.EXIFheader possess these settingslike the manufacturing of camera, Flash control, color balance the model of the camera, Filter Effects, Monochrome, location info, size of images, time of exposure, pocket mode, and the quantization matrix [21]apply in JPEG compression, Whentaken picture is exceed the given range of the taken camera settings then it may be examine that images did not come from the camera or it may be tempered or forged one at least.

In[22],there are few limits in this proposed technique.If the region of image hascommon intensity of lightingdefects in pixel,that isapparent only in darker regions or in lighter regions.Due to different wavelengths of the light, this bent on different extents by the lens. Due to temperature the defects causes in pixels.In addition, few post-processing manipulationlikeimage, contrast, compression, blurring, etc., can exclude faulty pixels.Because of high cost,many manufacturers used aonly onesensor rather than multiple sensors for clicking a natural colour scene.Hence, colour filter array (CFA) often used in sensor for regulate the band of wavelengths whichreaching into CCD array. Reconstructingfor full-resolution colour sight, fewprojection algorithms have beenproposed. Thesecalculation are generallycarry throughdetached thevicinal pixel-element applying a matrix contain values through thelostpicture-elementthat is referred asdemosaicking methods [23].The authors in [24] explain pattern noise whichcontain two primaryconstituent: first one is the fixed pattern noise which is abbreviated as FPN and the second one is Picture-response non-uniformity noise which is abbreviated as PRNU. On a CCD chip, FPN is especially generatesfromdusky current. The dusky current occurs because of thermal operation in the image. That was depending on the shutter which is either opened or locked. Obviously, the quantities of dusky current on a CCD are continuously with identicallyand it is completely different pixels that could bediscontinuousgenerationspeed of dark current.Also in [24], to spot the video camera by videotape pictures authors applied FPN. One hundred black pictures are recorded by themand after that graphsof the images werecollected to depress the impact of the arbitrary noise. The evaluated output exhibitsfewlight dots are ascertained within the collected pictures.Thelightpointsare at variouslocations for every camera.After all, FPN is detectable solely in the dusky structure. Other first origin of pattern noise of the picturesensor is PRNU. PRNU is the picture-elementtransformation under brightness while light is not reached then FPN iscreated thermally in the sensor.Fixed pattern noise is an offset, whereasimages-response non-uniformity is a benefit. Hence, the main origin of pattern noise carried in natural picturemay be picture-response non-uniformity.

D.) Physically-based techniques:In this technique, it involve in the objects and light interaction with 3D. For capturing a image light is very important.Another major issue in makingsubstantial spliced imageswhich haspairs the light-source side of the pictures being merged.Thisvariation of light applies for theproof of tampering in apicture. In this technique,Images are mergedat the time ofmodificationwhich isacquired in various lighting circumstances. It happenstroublesome to matchup the lighting statebyadding theseimages. The lighting inconsistency in the mixedimagesmay apply forshowing the tempered portions of imageforgery. First timeJohnson and Farid [24] initiated a method for these issues.They discover a way for assessing the side of a lighting source in the first degree of

freedom for showing the results of tampering.



By assessing the direction andmagnitude of light source Johnson and Farid again in[25] build a classifierto detect forgery which is depend on lighting anomaly. This technique is inspiredby an earlier technique[26]even if this generalize classifier by assessingextra complex illuminating and may be adapted to one illuminatingresource.It assesses parameter of model from one image.

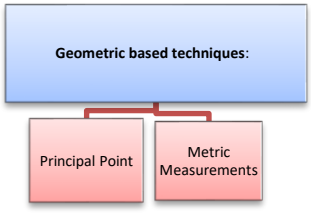
In[27] authors explain a model to assess the 3-D lighting environment with a low dimensional model. It assesses parameter of model from one image.

In[28], Researcherproposes a method for showing the results of forged part of image thatdepend on anomaly in light direction. The above method applied to estimate the plane normal matrix of the pictureby using blind identification methods.In this model researcher acquired 87.33%.accuracy for forgery detection.

In [29] researchersdeveloped a method whichdepend on tempering part of image detection applying a 2D lighting system. It does not estimate the 3-D shape of the object.

In[30] researchersexplain a model for detect the tempered images which isdepends on anomalies in the colour of lighting. Knowledgethrough physicalor statistical-based illuminate assessor on imagesarea of identical material isapplied. SVM meta-fusion model is applied. In this method researcher acquired 86% accuracy for forgery detection. The benefits of this approach are that it creates the lighting anomalies within the forged picture which is easy to show. In this model, the researcher acquired 87.33%.accuracy for forgery detection.

E.) Geometric based techniques: A geometric method is obtained by transforming the image into geometric primitives like angle movement curves and points.TheVariationsof thecalculated principal point throughout the picturemay be applied for the proof of the originality of the picture.



In [31], the researcher proposed a unique method for PIM and PRCG classification for detecting the tempered images. Theyexploredthe physical variations in the generation among CG and imagegraphic.In this model researchers acquired with a classification accuracy of 83.5%for forgery detection.

REFERENCING

[1] H. Farid, “Image forgery detection,” IEEE Signal Process. Mag., vol. 26, no. 2, pp. 16–25, 2009, doi: 10.1109/MSP.2008.931079.
[2] S. . P. Doke, Kanchan K, “Digital Signature Scheme for Image,” vol. 49, no. 16, pp. 1–6, 2012, doi: 10.5120/7708-1012.
[3] J. Fridrich, “Robust Bit Extraction from Images,” pp. 536–540, 1999.
[4] X. Zhao, J. Li, S. Li, and S. Wang, “Detecting Digital Image Splicing in Chroma Spaces,” pp. 12–13, 2011, doi: 10.1007/978-3-642-18405-5_2.
[5] S. B. Ã and A. K. Nandi, “Automated detection and localisation of duplicated regions affected by reflection , rotation and scaling in image forensics,” Signal Processing, vol. 91, no. 8, pp. 1759–1770, 2011, doi: 10.1016/j.sigpro.2011.01.022.
[6] C. Pun, S. Member, X. Yuan, and X. Bi, “Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching,” vol. 6013, no. c, pp. 1–12, 2015, doi: 10.1109/TIFS.2015.2423261.
[7] Z. Moghaddasi, H. A. Jalab, and R. Noor, “SVD-based Image Splicing Detection,” 2014, pp. 27–30, doi: 10.1109/ICIMU.2014.7066598.
[8] S. Khan, K. Khan, F. Ali, and K. Kwak, “SS symmetry Forgery Detection and Localization of Modifications at the Pixel Level,” pp. 1–10, 2020, doi: 10.3390/sym12010137.
[9] S. Bayram, N. Memon, M. Ramkumar, and B. Sankur, “A Classifier Design For Detecting Image Manipulations,” 2004, pp. 1–4, doi: 10.1109/ICIP.2004.1421647.
[10] M. S. and K. J. R. Liu, “BLIND FORENSICS OF CONTRAST ENHANCEMENT IN DIGITAL IMAGES,” 2008, pp. 3112–3115, doi: 10.1109/ICIP.2008.4712454.
[11] M. C. S. and K. J. R. Liu and Dept., “FORENSIC ESTIMATION AND RECONSTRUCTION OF A CONTRAST ENHANCEMENT MAPPING,” 2010, pp. 1698–1701, doi: 10.1109/ICASSP.2010.5495488.
[12] M. C. Stamm, S. Member, and K. J. R. Liu, “Forensic Detection of Image Manipulation UsingnStatistical Intrinsic Fingerprints,” vol. 5, no. 3, pp. 492–506, 2010, doi: 10.1109/TIFS.2010.2053202.
[13] H. Kong, “FORENSIC ESTIMATION OF GAMMA CORRECTION IN DIGITAL IMAGES Gang,” 2010, pp. 2097–2100, doi: 10.1109/ICIP.2010.5652701.
[14] Y. Lv, X. Shen, and H. Chen, “An improved image blind identification based on inconsistency in light source direction,” pp. 50–67, 2011, doi: 10.1007/s11227-010-0531-y.
[15] G. Cao, Y. Zhao, S. Member, R. Ni, and X. Li, “Contrast Enhancement-Based Forensics in Digital Images,” vol. 9, no. 3, pp. 515–525, 2014, doi: 10.1109/TIFS.2014.2300937.
[16] G. Chierchia, S. Member, G. Poggi, C. Sansone, and L. Verdoliva, “A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection,” 2014, vol. 9, no. 4, pp. 554–567, doi: 10.1109/TIFS.2014.2302078.
[17] M. A. Qureshi and M. Deriche, “A Review on Copy Move Image Forgery Detection Techniques,” pp. 1–5, 2014, doi: 10.1109/SSD.2014.6808907.
[18] Z. Fan, R. L. De Queiroz, and S. Member, “Identification of Bitmap Compression History : JPEG Detection and Quantizer Estimation,” vol. 12, no. 2, pp. 230–235, 2003, doi: 10.1109/TIP.2002.807361.
[19] J. Lukáš and J. Fridrich, “Estimation of Primary Quantization Matrix in Double Compressed JPEG Images,” Researchgate, pp. 1–17, 2003.
[20] B. R. Donald, “Statistical Tools for Digital Image Forensics,” pp. 1–137, 2004.
[21] H. Farid, “Digital Image Ballistics from JPEG Quantization,” pp. 1–6, 2006.
[22] Z. J. Geradts, J. Bijhold, M. Kieft, K. Kurosawa, and K. Kuroki, “Methods for identification of images acquired with Digital cameras,” vol. 4232, pp. 505–512, 2001, doi: 10.1117/12.417569.
[23] A. C. Popescu and H. Farid, “Exposing Digital Forgeries in Color Filter Array Interpolated Images,” vol. 53, no. 10, pp. 3948–3959, 2005, doi: 10.1109/TSP.2005.855406.

[24] M. K. Johnson, “Exposing Digital Forgeries by Detecting Inconsistencies in Lighting,” pp. 1–9, 2005, doi: 10.1145/1073170.1073171.
[25] M. K. Johnson, S. Member, and H. Farid, “Exposing Digital Forgeries in Complex Lighting Environments,” vol. 2, no. 3, pp. 1–17, 2007, doi: 10.1109/TIFS.2007.903848.
[26] M. K. Johnson and H. Farid, “Exposing Digital Forgeries Through Specular Highlights on the Eye,” Springer, pp. 1–15, 2007, doi: 10.1007/978-3-540-77370-2_21.
[27] 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.
[28] Y. Lv, X. Shen, and H. Chen, “An improved image blind identification based on inconsistency in light source direction,” pp. 50–67, 2011, doi: 10.1007/s11227-010-0531-y.
[29] 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.
[30] 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.
[31] T. Ng, S. Chang, J. Hsu, and L. Xie, “Physics-Motivated Features for Distinguishing Photographic Images and Computer Graphics,” 2005, pp. 1–10, doi: 10.1145/1101149.1101192.