A review paper on digital image forgery detection techniques

Conference Paper · July 2017

DOI: 10.1109/ICCCNT.2017.8203904

3 authors, including:

Navpreet Gill
National Institute of Technical Teachers Training and research,chandigarh,india
1 PUBLICATION **52** CITATIONS
SEE PROFILE

Amit Doegar
National Institute of Technical Teachers Training and Research
21 PUBLICATIONS **367** CITATIONS
SEE PROFILE

A Review Paper on Digital Image Forgery Detection Techniques

Navpreet Kaur Gill
Research Scholar
CSE,NITTTR
Chandigarh, India
Navpreet.cse@nitttrchd.ac.in

Ruhi Garg
Research Scholar
CSE,NITTTR
Chandigarh, India
Gargruhi2011@gmail.com

Er.Amit Doegar
Assistant Professor
CSE,NITTTR
Chandigarh, India
Amit@nitttrchd.ac.in

***Abstract*— These days digital image forgery has turned out to be unsophisticated because of capable PCs, propelled image editing softwares and high resolution capturing gadgets. Checking the respectability of pictures and identifying hints of altering without requiring additional pre-embedded information of the picture or pre-installed watermarks are essential examine field. An endeavor is prepared to review the current improvements in the research area of advanced picture fraud detection and comprehensive reference index has been exhibited on passive methods for forgery identification. Passive techniques donot require pre-embedded information in the image. Several image forgery detection techniques are arranged first and after that their summed up organization is produced. Author will review the various image forgery detection techniques along with their results and also compare the various different techniques based on their accuracy.**

Keywords-*Image Forensics, Copy-move forgery detection, JPEG artifacts, Image splicing*

I. INTRODUCTION

Advancement in image forensics has given upliftment to various methods for the detection of tampered images. Digital forgery detection techniques include many techniques for detecting artifacts produced during Resampling [1][2],aberrations due to color filter array[3],Cloning[4][5],Splicing[6],lighting inconsistencies[7][8][9] and noise pattern due to disturbances in camera's sensor[10] [11].Now-a-days images can be tampered without any impressions left-behind with the help of sophisticated computer graphics algorithms and image editing softwares like Photoscape and Acorn etc.[12][13]

Digital image forgery detection field has grown fundamentally to battle the issue of image falsification in numerous areas like legitimate administrations, medical sciences, legal sciences [14,15].The Scientific Working Group on Imaging Technology (SWGIT) gives proposals and rules to authorization offices for criminal equity framework in regards to the accepted procedures for images and video examination [www.swgit.org]. SWGIT gives data for proper utilization of different forgery detection techniques by staff in the criminal equity framework via upcoming records like the SWGIT latest archives.


INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

1 2 3

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

Fig. 1: Example of Digital Image Forgery

II. TAXONOMY OF IMAGE FORGERY DETECTION TECHNIQUES

Forgery identification determines the genuineness of pictures [16]. For confirmation of authenticated images different techniques have been created. In this paper we extensively order different strategies into two categories:

- Active techniques
- Passive techniques

This taxonomy depends on the fact whether the original picture is accessible or not. Each strategy can be further sub partitioned. The chain of division is shown in figure 1.

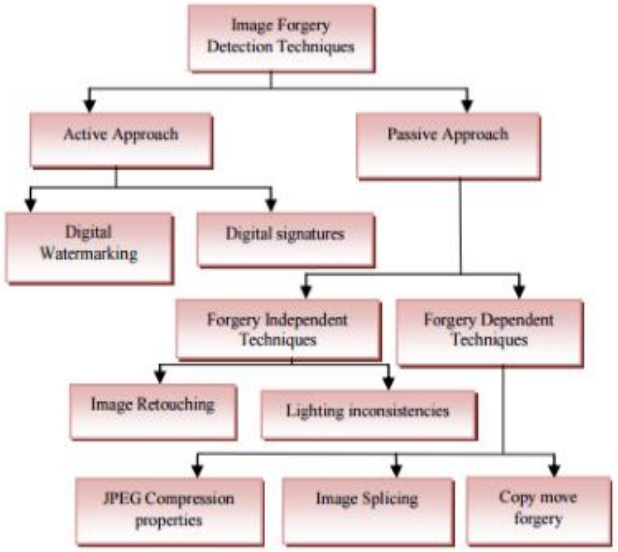


Fig. 2 : Categorization of Image Forgery Detection Techniques

2.1 Active Forgery identification Techniques

An active forgery detection technique requires pre-extracted or pre-embedded information. Digital Watermarking [17-21] or digital signatures [22-26] are popularly known methods used in Active approach[27-29].

2.2 Passive Forgery detection Techniques

Passive methods, popularly known as blind methods, merely uses the image itself for its authentication and integrity[30-32].This method assumes that although there may be no visual clues of tampering in the image, but tampering may disturbs the underlying statistics property due to the Noise inconsistency[33],Blurring of image [34],Image sharpening[35],Forgery through copy-move [36] and Image inpainting[37] etc.

Forgery dependent techniques are intended to distinguish just certain kind of forgeries, like splicing those are reliant on the sort of forgery carried out on the picture[38-39].

Forgery independent techniques recognize forgeries that are independent from fraud but in view of artifact traces left behind due to the procedure of sharpening, blurring and because of inconsistencies due to shading and light effects [40].

III. GENERALIZED SCHEMA FOR IMAGE FORGERY IDENTIFICATION

Forgery identification in pictures is two step issue. The principle target of blind forgery detection technique stays to categorize a given picture as real or altered. We will depict a widely used schema of image forgery identification procedure,that comprises of the following steps:

1. Image Preprocessing: Image preprocessing is the initial pace. Some preprocessing is performed on the picture under deliberation like image filtering, image enrichment, trimming, change in DCT coefficients, RGB to grayscale transformation before handling the image to feature extraction procedures. Algorithms examined at this juncture might possibly include this step depending upon the calculation[41].

2. Feature Extraction: Selection of features for every class separates the image-set from different classes however in the meantime stays constant intended for a specific class chosen. The attractive element of the chosen set of features is to have a tiny measurement so that computational complexity can be diminished and have an extensive distinction with other classes[42].

3. Selection of Classifier: Depending upon the feature-set that is extracted in above step, suitable classifier is either chosen or composed. The large training sets will yield the improved performance of classifier [43][44].

4. Classification:-The only motive behind classification is to determine if the image is original or not. Neural systems [45], LDA[46] and SVM[47,48,49] are classifiers used for this purpose.

5. Postprocessing:-Some forgeries will possibly require post processing that include manipulations like localization of copy locales [50,51,52,53].

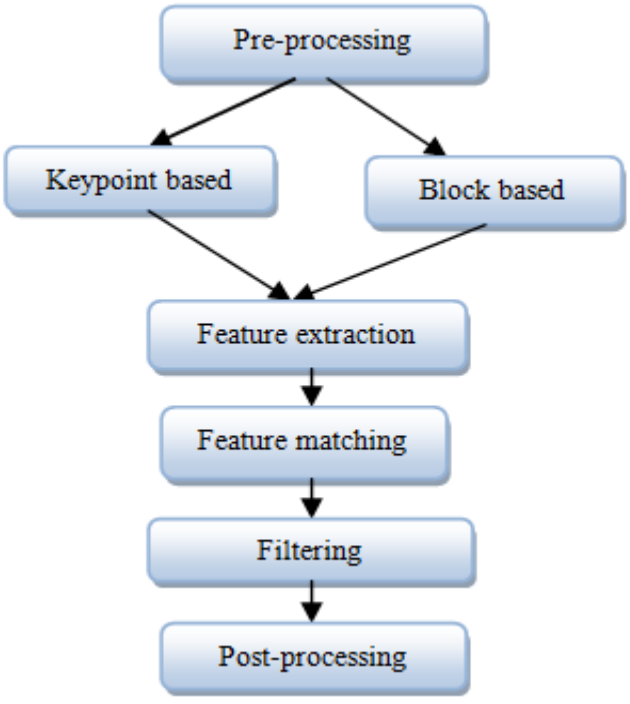


Fig. 3: Generalized schema for image forgery detection

IV . COPY-MOVE FORGERY DETECTION

A block of the picture is replicated and stuck to another block of a similar picture in copy-move forgery. It is exceptionally hard to recognize this sort of fabrication as the replicated picture is taken from a similar picture[54,55]. Copy-move forgery detection techniques are of following three types :-

- Brute Force
- Block Based Techniques
- Keypoint Based Techniques

Brute force method is based on exhaustive search and auto correlation technique. In exhaustive search, image is used to examine matching segment with circularly shifted versions. As it makes such large number of comparisons, its computational unpredictability is high. Autocorrelation determine location change. Keypoint based method uses scale and rotation invariant feature detector and descriptor algorithms which are Speeded-up Robust features (SURF) and Scale Invariant feature Transform (SIFT) whereas block based approach use the algorithms such as Discrete Wavelet Transform (DWT), Principle Component Analysis[54] (PCA), Singular Value Decomposition (SVD)and Discrete Cosine Transform (DCT) [55].

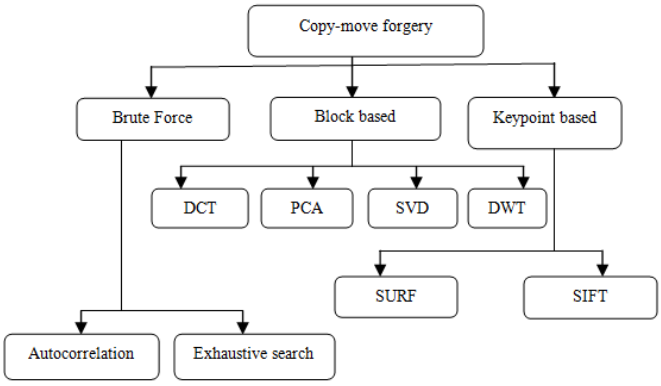


Fig. 4: Copy-Move Forgery Detection Methods

Popescu and Farid [2] recommended a technique in which principal component analysis (PCA) has been performed on the overlapping square blocks.

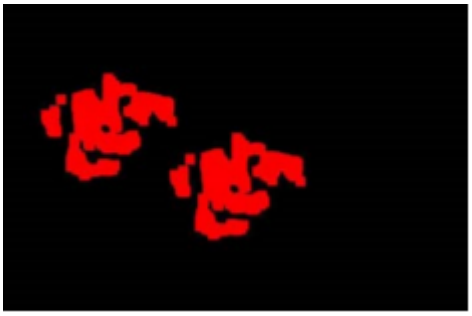
Lin et al. [56] proposes a detection technique in which picture is separated into the squares of equivalent size, and after that element of each square is extracted and sorted. The difference of the positions of each pair neighboring elements is processed. The aggregated number of each of this distinction is computed, more gathered number means conceivable occurrence of copy area.

Jing and Shao [57] proposes Scale Invariant Feature Transform (SIFT) calculation for recognizing neighborhood invariant components of image.When specified threshold value is compared with similar points and the value of similar points is greater,then image is manipulated.

Kohale et al. [58] propose a strategy which consolidates block based approach and feature based approach for falsification identification. Maind et al. [59] propose an enhanced block based technique which compares both the methodologies viz PCA and DCT for distinguishing forgery.

As indicated by Kulkarni and Chavan [60] block based techniques give appropriate result for identification of forgery in any jpeg image but takes additional time than keypoint based strategies.

(a) **(b)**



(c)

Fig. 5: (a) Original Image (b) Forged Image (c)Copy-Move Forgery Detection using PCA

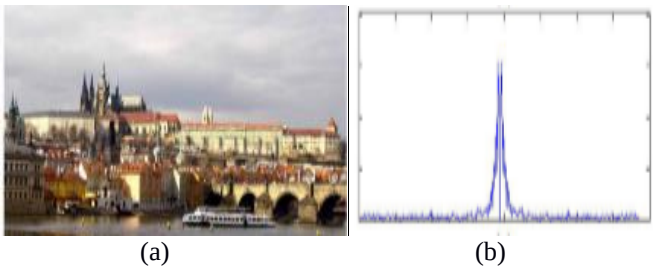
Table 1. Evaluation of Most efficient Copy-Move Forgery Identification Techniques

Technique proposed by	Features Extracted	Classifier used	Precision of detection method
Langille and Gong[61]	Zero normalized cross correlation in the sorted block array	K-dimensional tree	-
Luo[62]	Intensity based	-	96.31%

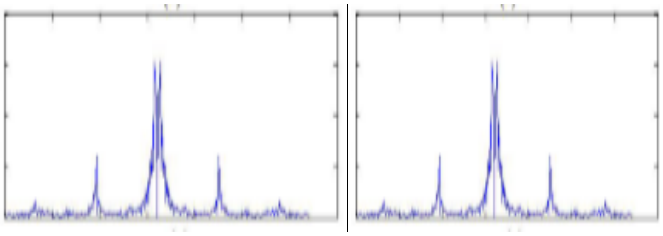
	characteristic features		
Mahdian and Saic[63]	Blur moment invariants	KD-tree	98%
Muhammad[64]	Dyadic Wavelet Transform	Thresholding classification	95.9%with false positive of 4.54%
Xunyu and siwei[65]	SIFT Keypoints	K-means clustering	99.08%
Kakar and Sudha[66]	Transform Invariant Features	Image MPEG-7 signature tools	90%
Suthiwan[67]	Multi-size Block DCT markov process	Support Vector Machine	99%
Gopi[68]	Auto Regressive coefficients	Artificial Neural Network	77.67% in experiment 1 94.83% in experiment 2
Zhao and Guo[69]	DCT of overlapping Blocks	Lexicographical Sorting	96.1%

V. Image Forgery Detection using JPEG Artifacts

Most of digital cameras export JPEG document format. Manipulation of image content and cropping are the attacks which can be performed on JPEG images. Since single compressed and double compressed JPEG images contain blocking artifacts, therefore these images can be detected by assessment of these artifacts. The image which undergoes manipulation will distort the alignment of the JPEG artifacts. To distinguish if a picture is previously JPEG compressed or not is an imperative matter.



(a) (b)



(c) (d)

Fig. 6: (a) Original Image under test (b) Result of single compressed version of image (a) (c) Result of (a) after double compression with quality factor 80 followed by 75 (d) Result of (a) after double compression with quality factor 80 followed by 85

Popescu[70] built up a procedure for identifying whether the given JPEG picture is double compressed or not by inspecting the DCT coefficients histograms as double JPEG compression adds up the double quantization of square DCT coefficients that presents particular artifacts noticeable in the DCT coefficient histograms.

Huang[71]introduced a technique will make use of quantization matrix to recognize double JPEG compression.

Kee and Jhonson[72]prescribed a method that will make use of camera signature of a JPEG image to figure out whether an image has been altered or not.

Bianchi and Piva[73] proposed a strategy for the detection of non-aligned double JPEG compression in the light of perception that when the blockwise DCT is processed in accordance with th primary JPEG compression grid,its coefficients will display an integer periodicity.

Table 2. Evaluation of Most Robust Image Forgery Techniques using JPEG Artifacts

Technique proposed by	Features extracted	Classifier Used	Precision of detection method
Fridrich and Lukas[74]	Estimation of Primary Quantization Method	Neural Network Classifier	99%
Tjao[75]	Estimation of Block size	-	95%
Luo[76]	Maximum Likelihood Estimation	Morphgological Operation	70%
Fridrich and Penvy[77]	DCT modes of low frequency DCT coefficients	Support Vector Machine	90%
Qu[78]	13 features are extracted	SVM classifier	90%

Chunhun[79]	Transition Probability Matrix	Machine Learning based schemes	95%
Luo[80]	Rounding and Truncation Errors	-	94.52%

VI .Image splicing forgery detection

Image Splicing includes convergence of at least two pictures to create a fake image. If the pictures with contrasting foundation are combined then it turns out to be extremely hard to make the borders and boundaries incoherent.[81,82]

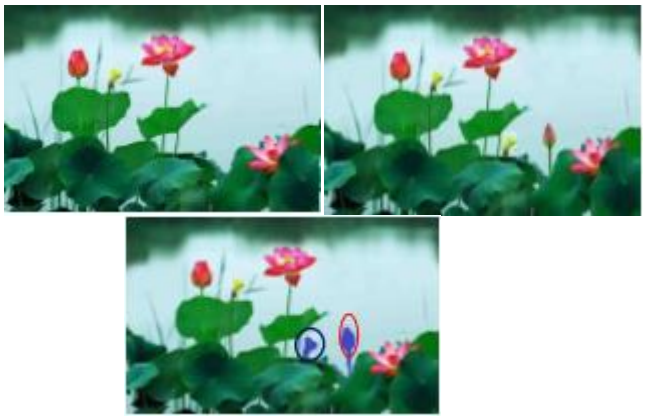


Fig. 7: (a) Original Image (b) Forged Image (c) Copy-Move Forgery Detection using PCA

Ke[83] proposes an approach which depends on the assumption that the shadow will not change the surface texture of an object. So the shadow and body both are duplicated and pasted from another picture during fabrication In this way, the surface in the texture consistency of shadow range is not consistent with that of the original area in the tampered image.

Su [84] introduced an improved version of Markov state selection procedure. Statistical boundaries get destroyed by strong edges produced by image splicing in the wavelet domain. Statistical moments are calculated from co-occurrence probability matrix of parent and child subbands in the wavelet domain. SVM classifier uses these extracted features as input. The benefit of this method is that it shows good performance even with the small number of features.

Burvin and Esther [85] introduced a machine-learning based procedure and requires minimal user interaction. This technique needs no expert intervention to take forgery decision and it is applicable to images containing two or more people. To achieve this, statistical-based illuminant estimators and physics-based are used to incorporate information on the image regions. Edge-based as well as texture based features are extracted from these illuminant estimates and are used to take automatic decisions based on machine-learning based mechanisms.

Table 3. Comparison of most famous Image Splicing Detection Methods

Technique proposed by	Feature extracted	Classifier used	Precision of detection method
Lint[86]	Inverse camera response functions by analyzing edges	Support Vector Machine	100%
Chen[87]	Wavelet Characteristics function and 2D phase congruency	Support Vector Machine	82.32%
Dong[88]	Statistical moments of run-length and edge detection	Support vector machine	76.52%
Wang[89]	Chroma components from grey level cooccurence matrix	Support vector machine	90.5%
Fang[90]	Color sharpness and difference of single value between different channels	LDA	90%

VII Conclusion

Forgery detection using passive forgery detection techniques is one of the most growing field of research. We have presented some of the passive techniques and also compare them in terms of accuracy of their results. The prime drawback of the existing methods is Automation that is the answers can be interpreted with the intervention of human only. Second drawback is that if we talk about copy-move forgery, then the use of these methods is computationally expensive. Thirdly as these techniques are applied to images only, we can extend the research on audios and videos. Fourthly at present there is no technique which can identify between the malicious forgery and just the retouching like artistic manipulation. The most challenging tasks is to develop a unified algorithm having capacity to detect any type of forgery.

REFERENCES

[1]J.Fridrich,D.Soukal and J.Luka,"Detection of copy-move forgery in digital images", *in Digital Forensic Research Workshop*,pp.6-8,2003.

[2]A.C.Popescu and H.Farid,"Exposing digital forgeries by detecting duplicated regions",*Dept. of Computer Science,Dartmouth college Technical Representation*,pp.2004-515,2004.

[3]T.Ngand and S.F.Chang,"A model for image splicing*",in IEEE International Conferemce on image processing,Singapore*,pp.1169-1172,2004.

[4]S.Bayram,I.Avcibas,B.Sarkar,N.Memin,"A classifier design for detecting image manipulations",*in International conference on image processing*,pp.2645-2648,2004.

[5]H.Farid and A.C.Popescu,"Exposing digital forgeries by detecting traces of re-sampling",*IEEE Transactions Signal Processing*,pp.758-767,2005.

[6]H.Farid and A.C.Popescu,"Exposing digital forgeries in color filter array interpolated images",*IEEE Transactions Signal Processing*,pp.3948-3959,2005.

[7]H.Farid and M.K.Johnson,"Detecting photographic compsites of people",*Workshop on Digital watermarking,China*,2007.

[8]M.K.Johnson and H.Farid," Exposing digital forgeries through chromatic aberration,"*ACM Multimedia and Security Workshop,Geneva,Switzerland*,pp.48-55,2006.

[9] M.K.Johnson and H.Farid," Exposing digital forgeries by detecting inconsistencies in lightning",*ACM Multimedia and Security Workshop*,pp.1-10,2005.

[10] M.K.Johnson and H.Farid," Exposing digital forgeries through specular highlights on the eye",*International Workshop on information hiding,Saint Malo,France*,pp.311-325,2007.

[11] M.K.Johnson and H.Farid," Exposing digital forgeries in complex lightning environment,"*IEEE Transition on Information Forensics Security*,pp.450-461,2007.

[12]G.Liu,J.Wng,S.Lian and Z.Wang,"A passive image authentication scheme for detecting region-duplication forgery with rotation",*Journal of Network and Computer Applications*,pp.1557-1565,2010.

[13]N.Sebe,Y.Liu,Y.Zhuang,T.Huanag and S.F.Chang,"Blind passive media forensics:motivation and opportunity".*Multimedia Content Analysis and Mining,Springer,Berlin*,pp.57-59,2007.

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

[15]B.L.Shivakumar and S.S.Baboo,"Detecting copy-move forgery in digital images:a survey and analysis of current methods",*Global Journal of Computer Science*.,pp.61-65,2010.

[16]G.K.Birajdar and V.H.Mankar,"Digital image forgery detection using passive techniques:A survey",*Digital investigations*,pp.226-245,2013.

[17]C.Y.Lin and S.F.Chang,"Generating Robust Digital Signature for image/video Authentication",*Multimedia and Security Workshop at ACM Multimedia*,1998.

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

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

[20]X.Wang,J.Xue,Z.Zheng,Z.Liu and N.Li,"Image forensic signature for content authenticity analysis",*Journal ofComputers and Electrical Engineering*,(2012).

[21]M.Sengupta and J.K.Mandal,"Authentication through Hough transformation generated signature on G-Let D3 Domain(AHSG)",*International conference on computational intelligence:Modeling Techniques and Applications*,2013.

[22]J.M.Shieh,D.C.Lou and T.Ming Chang Chang,"A semi-blind digital watermarking scheme based on singular value decomposition",*Computer standards and interfaces,pp.428-440,2006.*

[23]R.Chamlawi,A.Khan and I.Usman,"Authentication and Recovery of images using multiple watermarks",Computers and Electrical Engineering,pp.578-584,2010.

[24]Y.S.Chen and R.Z.Wang,"Reversible authentication and crossrecovery of images using threshold and modified-RCM watermarking",*Optics Communications*,pp.2711-2719,2011.

[25]G.Schirripa and M.Desantis,"Holographic watermarking for authentication of cut images",*Optics and Lasers in Engineering*,pp.1447-1455,2011.

[26]L.Rosales,M.Cedillo,M.Nakano,H.Perez,"Watermarking based image authentication with recovery capability using halftoning technique,"*Signal Processing:Image communication*,pp.69-83,2013.

[27]S.Katzenbeisser and F.A.Petitcols,"Information techniques for stenography and digital watermarking",2000.

[28]I.J.Cox,M.L.Miller and J.A.Bloom,"Digital waterking",2002.

[29]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 andcybernatics*,pp.3463-3467,2008.

[30]T.T.Ng,S.F.Chang,C.Y.Lin and Q.Sun,"Passive-blind image forensics",*Multimedia security technology for digital rights*,2006.

[31]W.Luo,Z.Qu,F.Pan,J.Huang,"A survey of passive technology for digitl image forensics",*Front computer science China*,pp.166-79,2007.

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

[33]B.Mahdian and S.Saic,"Using noise inconsistencies for blind image forensics,"*Image and vision computing*,pp.1497-1503,2009.

[34]G.Cao,Y.Zhao and R.Ni,"Edge-based blur metric for tamper detection",pp.20-27,2007.

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

[36]F.Peng,Y.Nie and M.Long,"A complete passive blind image copy-move forensics scheme based on compound statistics features",Internation journal of *Fornsic science*,pp.21-5,2011.

[37]Y.Q.Zhao,M.Liao,F.Y.Shih and Y.Q.Shi,"Tampered region detection of impainting JPEG images",*International Jounal on light electron optics*,pp.2487-2492,2013.

[38]T.T.Ng,S.F.Chang,C.Y.Lin and Q.Sun,"Passive-blind image forensics",*Multimedia security technologies for digital rights management*",pp.383-412,2006.

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

[40]J.A.Redi,W.Taktak and J.L.Dugelay,"Digital image forensics:a booklet for beginners",*Multimedia Tools Applications*,pp.133-162,2011.

[41] A. Makandar, B. Halalli, "A review on preprocessing techniques for digital mammography images" ,I*nternational Journal ofcomputerapplications*,pp.0975-887,2015.

[42]A.Phkan,M.Borah,"A survey paper on the feature extraction module of offline handwriting character recognition",*International Journl of computer Engineering and Applications*,pp.51-60,2014.

[43]M.Y.Munirah,N.M.Nawi,N.Wahid and M.Shukra,"A comparative analysis of feature selection techniques for classification problems",*ARPN Journal of Engineering and Appliedsciences*,pp.13176-13187,2016.

[44]P.Sutthiwan,Y.Q.Shi,S.Wei and N.Tian,"Rake transform and edge statistics for image forgery detection",I*EEE international conference on munltimedia*,pp.1463-8,2010.

[45]W.Lu,W.Sun and J.W.Huang,"Digital image forensics using statistical features and neural network classifiers",*International conference on machine learning and cybernetics*,pp.12-15,2008.

[46]Z.Fang,S.Wang and X.Zhang,"Image splicing detection using camera inconsistency",*International Conference on multimedia information networking and security*,pp.20-4,2009.

[47]D.Fu,Y.Shi and W.Su,"Detection of image splicing basedon Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition",*International workshop on digital watermarking*,pp.177-87,2006.

[48]W.CHEN,Y.Shi and W.Su,"Image splicing detection using 2D Phase congruency and statistical moments of characteristic function,"*SPIE electronic imaging:security,steganography and watermarking of multimedia contents*,2007.

[49]W.Luo,J.Huang and G.Qiu,"Robust detection of region-duplication forgery in digital images,"*International conference on Pattern recognition*,pp.746-749,2006.

[50]E.Gopi,N.Lakshmanan,T.Gokul,S.Ganesh and P.Shah,"Digital image forgery detection using artificial neural network and auto regressive coefficients",*Canadian conference on electrical and computer engineering,pp.194-7,2006.*

[51]V.Christlein,C.Riess,J.Jordan and E.Angelopoulou,"An evaluation of popular copy-move forgery detection Approaches",*IEEE Transactions on*

information forensics and security,pp.1841-1854,2012.
[52]M.Ghorbani,M.Firouzmand and A.Faraahi,"DWT-DCT(QCD) based capy-move image forgery detection",*International conference on systems,signals and image processing*,pp.1-4,2011.
[53]G.Muhammad,M.Hussain,K.Khwaji and G.Bebis,"Blind copy-move image forgery detection using dyadic uncedimated wavelet transform",*International Conferemce on digital image processing*,2011.
[54]E.Ardizzone,A.Bruno and G.Mazzola,"Copy-move forgery detection via texture description",*ACM Workshop on multimedia in forensics,security and intelligence*,pp.59-64,2010.
[55]B.Soloria and A.K.Nandi,"Automated detection and localization of duplicated regions affected by reflection,rotation and scaling in image forensics",*International Journal of signal Processing*,pp.1759-1770,2011.
[56]H.Lin,C.Wang and Y.Kao,'An efficient method for copy-move forgery detection",*International conference on applied computer and applied computational science*,pp.250-253,2009.
[57]L.Jing and C.Shao,"Image copy-move forgery detection based on local invariant feature",*Journal of multimedia*,pp.90-97,2012.
[58]T.A.Kohale,S.D.Chede and P.R.Lakhe,"Forgery detection technique based on block and feature based method",*International Journal of advanced research in computer and communication Engineering.*,pp.7334-7335,2014.
[59]R.A.Maind,A.Khade and D.K.Chitre,"Image copy-move forgery detection using block representing method",*International Journal of soft computing and Engineering(IJSCE)*,pp.49-53,2014.
[60]V.S.Kulkarni and Y.V.Chavan,"Comparison of methods for detection of copy-move forgery in digital images",*InternationalJournal of Engineering science and Tech.*,2014.
[61]A.Langille,M.Gog,"An efficient match-based duplication detection algorithm",*Canadian conference on computer and rabot vision*,pp.64-66,2006.
[62]W.Luo,F.Pan,J.Huang,"A survey of passive technology for digital image forensics",*Front computer science China*,,pp.166-79,2007.
[63]B.Mahdian,S.Saic,"Blind methods for detecting image fakery",*IEEE Int. Carnahan conference on security technology*,pp.280-6,2008.
[64]G.Muhammad,M.Hussain and G.Bebis,"Passive copy-move forgery detection using undecimated dyadic wavelet transform",*Digital investigation*,pp.49-57,2012.
[65]P.Xunyu and L.Siwei,"Region duplication detection using image feature matching",*IEEE Transactions on Information Forensics security*,pp.857-67,2011
66]P.Kakar,N.Sudha,"Exposing postprocessed copy-paste forgeries through transform-invariant features",*IEEE Transactions on Information forensics security*,pp.1018-28,2012.
[67]P.Sutthiwan,Y.Q.Shi,S.Wei and N.Tian,"Rake transform and edge statistics for image forgery detection",*IEEE Internation conference on multimedia*,pp.1463-8,2010.
[68]T.Gokul and S.Ganesh,"Forgery detection using artificial neural network and auto regressive coefficients",*Conference on electrical and computer engineering*,pp.186-93,2007.
[69]J.Zhao and J.Guo,"Passive forensics for copy-move image forgery using a method based on DCT and SVD",*International Conference on forensic science*,pp.158-166,2013.
[70]A.C.Popescu and H.Farid,"Exposing digital forgeries by detecting traces of resampling",*IEEE Trans signal processing*,pp.758-67,2005.
[71]F.Huang,W.Guo and Y.Zhang,"Detecting double JPEG compression with the same quantization matrix",I*EEE Transactions Information Forensics security*,pp.848-56,2010.
[72]E.Kee and M.Jhonson,"Digital image authentication from JPEG headers",*IEEE Transactions Information forensics security*,pp.1066-75,2011.
[73]T.Bianchi and P.Piva,"Detection of non-aligned double JPEG compression based on integer periodicity maps",*IEEE Transactions Information Forensics security*,pp.842-8,2012.
[74]J.Fridrich and J.Lukas,"Estimation of primary quantization matrix in double compressed JPEG images",*Digital forensic research workshop*,2003.
[75]W.Luo,Z.Qu and J.Huang,"A novel method for detecting cropped and recompressed image block"*IEEE International conference on acoustics,speech and signal processing*,pp.633-6,2007.
[76]S.Tjao,W.Lin and H.Zhao,"Block size forensic analysis in digital images",*IEEE International conference on acoustics,speech and signal processing*,pp.217-20,2007.
[77]J.Fridrich and T.Penvy,"Detection of double-compression for applications in steganography",*IEEE Transactions of forensics security*,pp.247-58,2008.
[78]Z.Qu,W.Luo and J.Huang,"A convolutive mixing model for shifted double JPEG compression with application to passive image authentication",*IEEE International conference on acoustics,speech and signal processing*,pp.1661-4,2008.
[79]C.Chunhua,Y.Q.Shi amd S.Wei,"A machine learning based scheme for double JPEG compression detection",*Internatioal Conference on pattern recognition*,pp. 1-4,2008.
[80]W.Luo,J.Huang and G.Qiu,"JPEG error analysis and its applications to digital image forensics",*IEEE Transactions on Forensics Security*,pp.480-91,2010.
[81]Z.Moghaddasi,H.A.Jalab,R.Noor and S.Aghabozorgi,"Improving RLRN image splicing detection with the use of PCA and Kernel PCA",*The scientific World Journal*,2014.
[82]R.W.Ibrahim,Z.Moghaddasi,H.A.Jalab and R.M.Noor,"Fractional differential texture descriptors base onthe machado entropy for image splicing detection", *International Journal of Computer Science issues*,pp.4775-4786,2015.
[83]Y.ke,W.Min,X.Du and D.Li,"Image splicing detection based on texture consistency of shadow",*Journal of convergence information tevhnology*,2013.
[84]B.Su,Q.Yuan,S.Wang,C.Zhao and S.Li,"Enhanced state selection markov model for image splicing detection",*EURASIP Journal on wireless communications and networking*,pp.1-10,2014.
[85]P.Sabeena and J.Esther,"Detection of digital image splicing using luminance",*International Journal of Engineering Research and Applications*,pp.29-33,2014.
[86]Z.Lint,R.Wang,X.Tang and H.Shum,"Detecting doctored images using camera reponse normality and consistency",*IEEE Computer society conference on computer vision and pattern recognition*,pp.1087-92,2005.
[87]W.Chen,Y.Shi and W.Su,"Image splicing detection using 2D phase congruency and statistical moments of characteristic function",*SPIE electronic imaging:security,steganographyand watermarking of multimedia contents*,2007.
[88]J.Dong,W.Wang,T.Tan and Y.Shi,"Run-length and edge statistics based approach for image splicing detection",*International workshop on digital watermarking*,pp.76-87,2008.
[89]W.Wang,J.Dong and T.Tan,"Effective image splicing detection based on image chroma",*IEEE International Conference on image processing*,pp.1257-60,2009.
[90]Z.Fang,S.Wang and X.Zhang,"Image splicing detection using camera characteristic inconsistency",International Conference on multimedia information networking and security,pp.20-4,2009.