Volume 5, Issue 4, 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Brief Survey of Different Techniques for Detecting Copy-Move Forgery

Harpreet Kaur
Student master of technology
Sri Guru Granth Sahib World University
Fatehgarh Sahib Punjab India

Kamaljit Kaur
Assistant Professor
Sri Guru Granth Sahib World University
Fatehgarh Sahib Punjab India

Abstract: The use of digital images has increased over the past few years to spread a message. This increase the need of image authentication.But Preserving image authenticity is very complexbecause easily availability of image editing software. The pixel-based image forgery detection aims to verify the authenticity of digital images without any prior knowledge of the original image. There are many ways for tampering an image such as splicing or copy-move, re-sampling an image (resize, rotate, stretch),addition and removal of any object from the image. Copy-move forgery is one of the most popular tampering artifacts in digital images. In this paperwe presents different technique to detect copy move forgery using block based method.

Keywords: Image processing,Digital Image Forensic, Tampering,Copy-Move forgery(cloning),Block based methods

I. INTRODUCTION

Digital Image Forensics is an emerging branch of image processing . Digital Image Forensics is that field which deals with the authentications of the images. Digital image Forensics checks the integrity of the images by detecting various forgeries[1]. One of the principal tasks of image Forensics is image tampering detection. Tampering means to interfere with something in order to cause damage or make unauthorized alterations[2]. The availability of low-cost hardware and software tools, makes it easy to create, alter, and manipulated digital images with no obvious clues[6].Such software can do an alteration in digital image by changing blocks of an image without showing the effect of the modification in the forged image. These modifications cannot be noticed by human eyes[8]. It may no longer be possible to distinguish whether a given digital images is original or a modified version . Digital image Forgery is a growing problem in criminal cases and in public course. Detecting Forgery in digital images is a rising research field for ensuring the credibility of digital images .In the recent past digital image manipulation could be seen in tabloid magazine, fashion Industry, Scientific Journals, Court rooms, main media outlet and photo hoaxes we receive in our email[3].

1.1 Applications of Digital Image Forensic

- Digital forensics is commonly used in both criminal law and private investigation.
- Forensic analysis the images on online social networks.
- Used for detecting tampered or Forged image.
- Image Forgery detection system is needed in many fields for protecting copyright and preventing Forgery or alteration of images. It is applied in areas such as journalism, scientific publications, digital forensic science, multimedia security, surveillance systems etc.

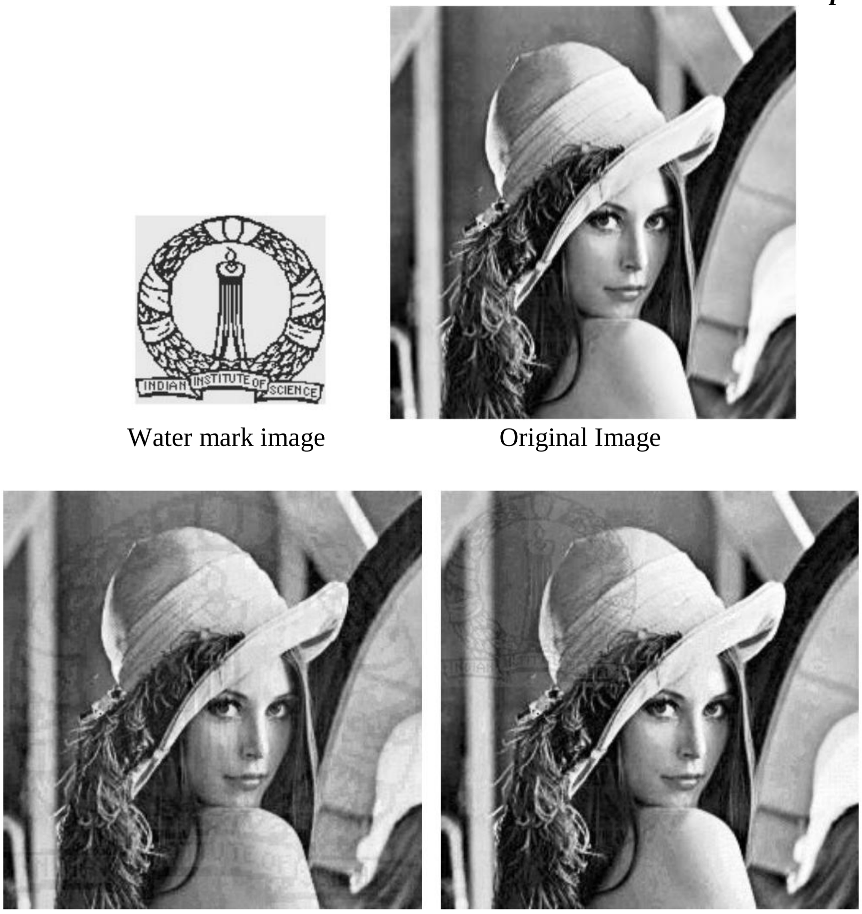
1.2 Classifications of Approaches

Digital image Forgery detection techniques are classified into active and passive approach.

a. Active Approaches: An active detection method which consists of adding image details in order to describe digital tampering such as name, date, signature, etc[22]. It require a special hardware implementation to mark the authentication of the digital image

Techniques of Active Approach:

a.1**Watermarking**:Watermarking is used for image forgery detection .Watermark must be inserted at the time of creating the image. Embedding a watermark in the image/video is equivalent to signing a specific digital producer identification (signature) on the content of images/videos. Once the image/video is manipulated, this watermark will be destroyed such that the authenticator can examine it to verify the originality of contents.The watermarking consists of hiding a mark or a message in a picture in order to protect its copyright at the time of image acquisition and to check the authenticity this message is extracted from the image and verified with the original watermarks. If image is not manipulated these watermarks will remain same else they will not match the original watermarks. Hence this method relies on the source information before hand. Some camera sources do not embed watermarks into image therefore this method is not that useful and usually does not work well with lossy compression[32].



Water mark image Original Image

Watermarked original image (Watermark over the whole image)

Watermarked original image (Watermark at the corner)

Fig1 Example of Watermarking[33]

a2.**Digital Signatures**: Digital signature is some sort of cryptographic is a mathematical scheme for demonstrating the authenticity of digital document[6].It generates a content-based digital signature which includes the important information of contents and the exclusive producer identification .The signature is generated by a producer-specific private key such that it can not be forged. Therefore, the authenticator can verify a received image/video by examining whether its contents match the information conveyed in the signature .

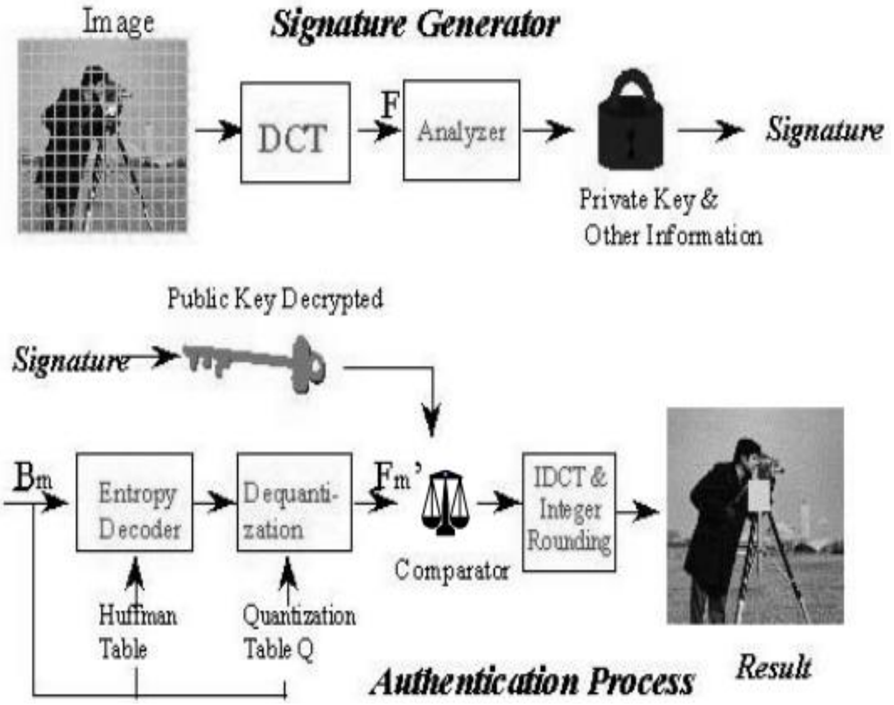


Fig2 Signature Generator and Image Authentication Process[31]

A signature and an image are generated at the same time. The signature is an encrypted form of the feature codes orhashes of this image, and it is stored separately. Once a user needs to authenticate the image he receives, he shoulddecrypt this signature and compare the feature codes (or hash values) of this image to their corresponding values in the original signature. If they match, this image can be claimed to be "authentic"[31] .

Advantage of Active Approach:

- Computational cost less ,simpleif knowledge about original image is available.

Disadvantage of Active Approach:

- These techniques require prior knowledge about original image thus they are not automatic.They required some human intervention or specially equipped cameras.
- There are more than millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authenticity of the image[7].
- In Digital Signature scheme, Extra Bandwidth is needed for transmission of Signature

b.Passive Approach:Passive method detects the duplicated objects in forged images withoutneed of original image watermarkand depends on traces left on the image by different processing steps during image manipulation. Passive approach also determines the amount and the location of forgery in the image. There are two methods of passive approach.

Image source identification- It identifies the device used for the acquisition of the digital image. It tells that the image is computer generated or digital camera image. In this method the location of forgery in image cannot be determined.

Tampering detection- It detects the intentional manipulation of images for malicious purposes. Image manipulation is denoted as tampering when it aims at modifying the content of the visual message[32].

Techniques of Passive Approach:

b1.. Pixel-based techniques that detect statistical anomalies introduced at the pixel level.

b2. Format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme.

b3. Camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing.

b4. Physically based techniques that explicitly model and detect anomalies in the three-dimensional interaction between physical objects, light, and the camera.

b5. Geometric-based techniques that make measurements of objects in the world and their positions relative to the camera [5].

Advantage of passive approach:

- Pre existing digital images and data cannot gain any profit using Active approach. Passive approach overcomes this disadvantage; the pre-existing images can also be catered using this approach.

Disadvantage of passive approach:

- These techniques based on the assumption that digital forgeries may leave no visual clues that indicate tampering,so they require different statistics of an image. Thus it is complex.

1.3 Types of Digital Image Forgery

The forgeries are classified into five major categories

- Image Retouching
- Image Splicing
- Copy-Move (cloning)
- Morphing
- Enhanced

Image Retouching: where the method is used for enhances an image or reduces some feature of an image and enhances the image quality for capturing the reader's attention. In this method, the professional image editors change the background, fill some attractive colors, and work with hue saturation for toning and balancing.

Image Splicing: where the different elements from multiple images are combined in a single. Such splicing can usually be detected by searching the splicing boundary (or the effect of the splicing on image statistics)

Copy-Move:In the copy move a part of the image is copied and pasted somewhere else within the same image. This method usually for hide definite particulars or to matching convinced features of an image. The blur tool is use for retouching borders and decrease the effect between original and pasted area [23].

Morphing: In this type the image and video can be exposed into unique influence ,where the one object on image is turned into another object in the other image. The morphing is used to transfer the one-person image from another person image by using seamless transition between two images.

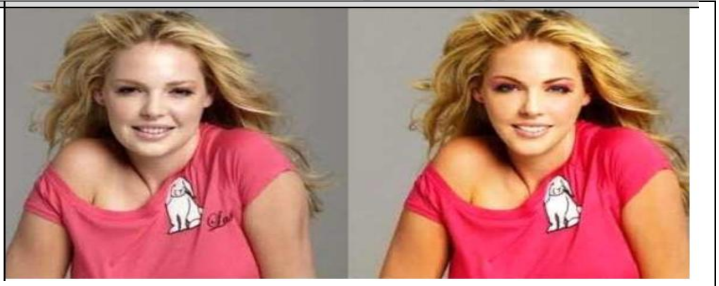
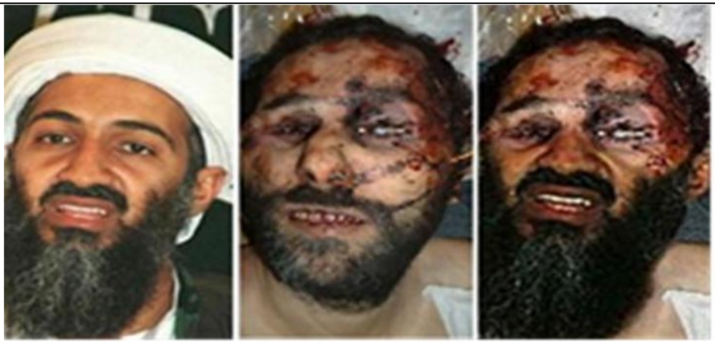
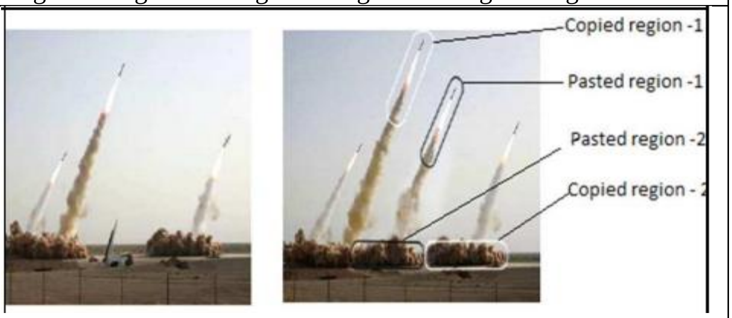
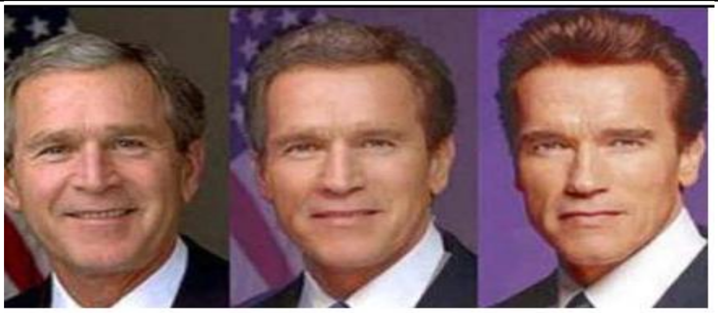
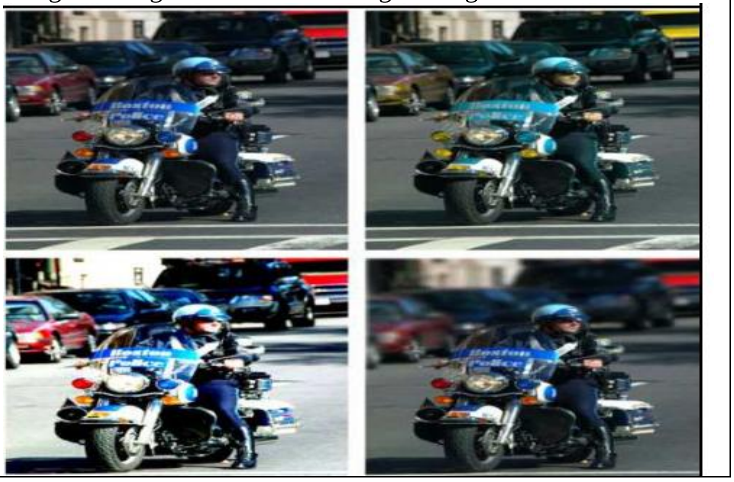
Image Retouching	In this method, the image editors change the background, fill some attractive colors, and work with hue saturation for toning and balancing[23].	 Original Image Forged Image
Image Splicing	where the different elements from multiple images are combined in a single.[25]	 Original Image Original Image Forged Image
CopyMove (cloning)	In the copy move a part of the image is copied and pasted somewhere else within the same image.[24]	 Copied region -1 Pasted region -1 Pasted region -2 Copied region - 2 Original Image Forged Image
Morphing	The morphing is used to transfer the one-person image from another person image by using seamless transition between two images[23].	 Original Image Forged Image Original Image
Enhanced	The original image is forged by enhanced image with color change, perform blur on background[22]	Original Image Forged Image 

Fig3:Types of Digital Image Forgery

II. COPY-MOVE FORGERY DETECTION

Copy-Move image forgery is the widely used technique to edit the digital image.Copy-Move forgery is performed with the intention to make an object "disappear" from the image by covering it with a small block copied from another part of the same image. Since the copied segments come from the same image, the color palette, noise components, color and the other properties will be same with the rest of the image, thus it is very difficult for a human eye to detect[3].A copy move forgery is easy to create. The copied content of image which is used to perform forgery is called snippet. As the source and the target regions are from the same image, the image features like noise, color, illumination condition etc. will be same for the forged region and the rest of the image. A clever forger may also do some post-processing on the copied region like rotation, scaling, blurring, noise addition before the region is pasted. These factors make the forgery detection more complex. So the crucial point in such a forgery detection technique would be extraction of features.[2]

Generally, Copy-Move forgery detection techniques can be classified into two: Block based approaches and Key-point based approaches [7]. In both the approaches some form of pre-processing will be there.Unlike block-based methods, Keypoint based methods compute their features only on image regions with high entropy, without any image subdivision for do not divide the image into blocks to extract the features instead, the features are extracted from the whole image.There are two types of keypoint based methods such as Scale Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF). Block-based methods subdivide the image into overlapping blocks of specified size for feature extraction. Similar feature vectors are subsequently matched. There are 13 block-based features and it can be grouped into four categories: Moment-based (Blur[13], Hu, Zernike[12]), Dimensionality reduction-based (PCA [5], SVD[11], KPCA), Intensity-based (Luo[10],Lin,Bravo, Circle[14]), Frequency -based (DCT [8] [9], DWT, FMT [12]).

III. PREVIOUS WORK DONE

In the last decade, many passive detection schemes for copy-move forgery have been proposed. Fridrich [8] first proposed a method of detecting copy-move forgery using discrete cosine transform (DCT) of overlapping blocks . Popescu [9] presented a method using principal component analysis (PCA) for the representation of image segments i.e. overlapping square blocks DCT. Luo [10] introduced a copy-move forgery detection and localization method based on dividing an image into small overlapped blocks, then comparing the similarity of these blocks and finally identifying possible duplicated regions using intensity based characteristics features.The algorithm has lower computational complexity and is more robust against stronger attacks and various types of after-copying manipulations, such as lossy compression, noise. A different approach was presented by Kang [11] in which the features were represented by the singular value decomposition (SVD). In this method the correlation is used for copied and pasted areas and for searching equal regions.Bayram [12] applied Fourier-Mellin transform (FMT) to each block and FMT values were finally projected to one dimension to form the feature vector. Mahdian [13] used a method based on blur moment invariants to locate the forgery regions. Li [14] extracted the features of the circular blocks using rotation invariant uniform local binary patterns.Reference [16] the image is subdivided into circular blocks . Polar sine transform is used to extract features and feature matrix is sorted.In 2012, [28] proposed a method using dyadic wavelets. Undecimated dyadic wavelets were chosen because of their property of shift invariance .The work in [29] forward a method using DCT and circular blocks in 2012. After block subdivision DCT is applied to each block. As in DCT, the energy concentrates on low frequency coefficients; a circle block representation is adopted for each block. A circle block is divided into four quadrants and features extracted from each quadrant.Another work [30] in 2013 presented a method that takes only low frequency part of the image by performing a Gaussian pyramids decomposition. Low frequency part will be half the size of the image. Mixed moments are computed for the overlapping b x b sub-blocks whose total count will be Y= ([M/2]-b+1) x ([N/2]-b+1).In another method [24] the Guassian pyramid are used for image dimensions for circle block and analyzed four features.The image separated into many fixed sized blocks that and further coinciding and calculate the reign values through Hu moments. A recent method based of expanding blocks was proposed in [31] in 2013. In their approach they used the direct block comparison instead of comparison based on block features.Blocks are compared against blocks in the same bucket only. A block is eliminated from the bucket if it does not match with any other block in the bucket. Blocks with no matches are eliminated, the search region is expanded and the comparison is continued. As the region expands the number blocks in the bucket reduces and remaining blocks are considered as part of the copied region.

IV. COMPARISON BETWEEN EXISTING TECHNIQUES

Sr no.	Author/year	Methodology	Advantage	Disadvantage
1	J. Fridrich 2003[8]	DCT	Copy-move region is Detected	Will not work in noisy Image
2	Popescu,2004[9]	PCA	Efficient method, low false positives	Low efficiency for low quality of image, low SNR and small blocks.
3	W. Q. Luo 2006[10]	Similarity matching	Copy-move region detected in noisy conditions	Time complexity isReduced

4	G. H. Li 2007	DWT-SVD	Efficiently detects forged region	Time complexity isless compared to other algorithms
5	Mahdian,2007[13]	BLUR	Duplicated regions detect with changed contrast values and blurred regions can also be detected	High computation time of the algorithm
6	J. Zhang 2008	DWT	Exact copy-move region is detected	Works well in noisyand compressed Image
7	H. Huang 2008	SIFT	Copy-move region is detected Copy-Move region isdetected	Detects false result also Will not work in
8	X. Kang 2008[11]	SVD	accurately	highly noised & compressed image
9	Wang, 2009,	CIRCLE	Working for post-processinglike blurring, rotating, noise adding etc.	Scaling and geometric transformations cannot be detected.
10	H.-J. Lin 2009	Improved PCA	Exact Copy-Moveregion is detectedWorks well in noisy, compressed image	
11	Z. Lin 2009	Double Quantization DCT	Tampered region isdetected accurately	Works only in JPEG Format
12	Ting, 2009, .	SVD	Can detect duplication even postprocessing is done, robust and computationally less complex	Cannot detect copy paste Regions
13	Bayram, 2009[12]	FMT	Efficient and robust to blurring, noise, scaling, lossy JPEG compression and translational effects.	Cannot detect forgeries, which have rotation of above 10 degrees and scaling of 10%.
14	Wang,2009,	HU	Robust and efficient method, detects post-processing effects like noise addition, blurring, lossy compression etc.	Many False positives
15	Qiao, 2011,	CURVELET	Multi-dimensional and multidirectional gives precise results.	Cannot be applied on compressed images.
16	M. Ghorbani 2011	DCT-DWT	Forged region is Detected accurately	Will not work in highly compressed image
17	S. D. Lin 2011	DCT-SURF	Copy-Move and spliced both region detected	
18	Muhammad , 2012[28]	Dy DWT	Reduced false positives. Advantageous than previous methods using DWT	Tested only for small rotation angle and good quality images
19	Cao Y 2012[29]	Circular Block with DCT	Perfect detection for uniform background images, non regular duplicate regions, high resolution images. Detect multiple copies -move	Poor performance with poor image quality. Not robust to geometrical operations

20	LGavin, 2013[31]	Expanding Blocks	Detection with irregularly shaped regions and for forged regions slightly darkened or lightened.	Slow in execution. Number of false positives more when compared to other methods.
21	Mohamadian,2013 [28]	ZERNIKE	Flat regions of forgeries are detected	Calculating Zernike moment coefficients is complex
22	Zhong L 2013[30]	Mixed Moments	Tested for rotation, scaling, brightness enhancement, contrast changes. Reduced number of Blocks	Qualitative evaluation not specified Rotation angle and scaling factor not specified.
23	Zhu H, 2013[16]	Polar harmonic transform	Addressed affine transforms like shearing and perspective projections that were rarely considered before	Simulation results only available

V. CONCLUSION

Copy-Move forgery detection in digital images is more prevalent problem during the past two or three decades. Many techniques have been proposed to address this problem. This paper providebrief survey to detect copy move forgery detection method. This also covers limitations of different techniques used for passive method to detect copy move forgery. The comparative work can be extended by proposing a novel technique with which the existing limitations can be overcomed.

REFERENCES

[1] MohdDilshad Ansari, S. P. Ghrera&VipinTyagi :"Pixel-Based Image Forgery Detection: A Review" IETE Journal of Education, 40-46(Aug 2014)

[2] ResmiSekhar,Chithra AS:" Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images" International Journal of Computer Applications (0975 – 8887),Volume 89 , no. 8, March 2014.

[3] Rohini.A.Maind, AlkaKhade, D.K.Chitre:" Image Copy Move Forgery Detection using Block Representing Method" International Journal of Soft Computing and Engineering (IJSCE)ISSN: 2231-2307, Volume-4, Issue-2, May 2014.

[4] Ms. P. G.Gomase, Ms. N. R. Wankhade:" ADVANCED DIGITAL IMAGE FORGERY DETECTION: A REVIEW"Journal of Computer Science (IOSR-JCE) e-ISSN: 2278-0661, PP 80-83.

[5] HanyFarid, ”Image Forgery Detection”, IEEE SIGNAL PROCESSING MAGAZINE, pp. 16-25, MARCH 2009.

[6] Nikhilkumar P. Joglekar, Dr. P. N. Chatur"A Compressive Survey on Active and Passive Methods for Image Forgery Detection"International Journal Of Engineering And Computer Science ISSN:2319-7242 ,Volume 4 , Page No. 10187-10190, 1 January 2015. Tushant A. Kohale

[7] Dr. S.D. Chede, Prof. P.R.Lakhe" Forgery of Copy Move Image Detection Technique by Integrating Block and Feature Based Method" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2015

[8] J. Fridrich, D. Soukalm and J. Lukas, “Detection of Copy-Move Forgery in Digital Images, Digital Forensic Research Workshop, Cleveland, (2003), pp. 19–23.

[9] A. C. Popescu and H. Farid, “Exposing Digital Forgeries by Detecting Duplicated Image Regions”, Tech. Rep. TR2004-515, Dartmouth College, (2004).

[10] W. Luo, J. Huang and G. Qiu, “Robust detection of region-duplication forgery in digital images”, in: International Conference on Pattern Recognition, vol. 4, (2006), 746–749.

[11] X. Kang and S. Wei, “Identifying tampered regions using singular value decomposition in digital image forensics”, in: Proceedings of International Conference on Com-puter Science and Software Engineering, (2008), pp. 926–930.

[12] S. Bayram, H. T. Sencar and N. Memon, “An efficient and robust method for detecting copy-move forgery”, in: IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, New York,(2009).

[13] B. Mahdian and S. Saic, “Detection of copy-move forgery using a method based on blur moment invariants”, Forensic Sci. Int., vol. 171, (2007) pp. 180–189.

[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, no. 1, (2013) January, pp. 46-56.

[15] G. Lynch, F. Y. Shih and H. M. Liao, “An efficient expanding block algorithm for image copy-move forgery detection”, Inf. Sci., vol. 239, (2013), pp. 253–265.

[16] Li L, Li S, Zhu H, Wu X. “Detecting copy-move forgery under affine transforms for image forensics”, Computer Electric Eng (2013)

[17] Cheng Yan ”Research on Forged Identification of Forged Images”, *International Conference on Mehatronic Sciences,Electric Engineering and Computer*,20 dec 2013

[18] Ashima Gupta, NisheethSaxena, S.K Vasisth,”Detecting Copy Move Forgery Using DCT*”, International Journal of Scientific and Research Pulication*,Vol.3,Issue5,May 2013

[19] Amanpreet Kaur ,Richa Sharma ,” Optimization of Copy-Move Forgery Detection Technique”, *International Journal of Advanced Research in Computer Science and Software Engineering* , Vol 3, Issue 4, April 2013

[20] Wei Hou, ZheJi, Xin Jin, Xing Li, "Double JPEG Compression Detection Based on Extended First Digit Features of DCT Coefficients",*International Journal of Information and Education Technology*, Vol. 3, No. 5, October 2013

[21] Abhitha.E, V.J Arul Karthick, "Forensic Technique for Detecting Tamper in Digital Image Compression", *International Journal of Advanced Research in Computer and Communication Engineering* Vol.2, Issue3,March 2013

[22] Salam A.Thajeel and Ghazali Bin Sulong,"STATE OF THE ART OF COPY-MOVE FORGERY DETECTION TECHNIQUES: A REVIEW",*International Journal of Computer Science Issues*, Vol. 10, Issue 6, No 2, November 2013

[23] H. SHAH, P. SHINDE, AND J. KUKREJA,"RETOUCHING DETECTION AND STEGANALYSIS," IJEIR, VOL. 2, PP. 487-490, 2013

[24] SALAM A.THAJEEL,GHAZALI SULONG,"A SURVEY OF COPY-MOVE FORGERY DETECTION TECHNIQUES",Journal of Theoretical and Applied Information Technology. Vol.70 , 10thDecember 2014

[25] Mariam Saleem,"A Key-Point Based Robust Algorithm for Detecting Cloning Forgery",International Journal of Current Engineering and Technology,Vol.4, No.4 (Aug 2014).

[26] M. Sridevi, C. Mala, AND S. Sandeep ,"COPY–MOVE IMAGE FORGERY DETECTION IN A PARALLEL ENVIRONMENT," 2012.

[27] J. Fridrich, D. Soukal, and J. Lukas,“Detection of copy move forgery in digital images,”in Proceedings of the Digital Forensic Research Workshop, Aug. 2003, pp. 5-8.

[28] Muhammad, G., Hussain, M., Bebis, G., “Passive copy move image forgery detection using undecimated dyadic wavelet transform”, Digital Investigation (9), 2012.

[29] Cao Y, Gao T, Fan L, Yang Q., “A robust detection algorithm for copy-move forgery in digital images”, Forensic Sci Int. 2012 Jan.

[30] Zhong L, Xu W, “A robust image copy-move forgery detection based on mixed moments”, IEEE International Conference on Software Engineering and Service Sciences (ICSESS), 2013 May.

[31] L Gavin, S Frank, L Hong-Yuan Markl, “An efficient expanding block algorithm for image copy-move forgery detection”, Information Sciences 239, 2013.

[32] Amanpreet Kaur,RichaSharma"Copy-Move Forgery Detection using DCT and SIFT",International Journal of Computer Applications (0975 – 8887) Volume 70– No.7, May 2013

[33] A Project Report on Watermarking of Digital Images by Saraju Prasad Mohanty