INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

REVIEW ON COPY-MOVE FORGERY DETECTION IN DIGITAL IMAGE FORENSICS

PALLAVI P PURI

Student of Master of Engineering (Computer Science & Engineering), Raisoni College of Engineering and Management, Amravati, India.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Forensic Science is a scientific field that works with the field of law. Forensic Investigation helps in solving many criminal cases using DNA Analysis, Finger Printing, Forgery Detection. Digital forensics is a branch of forensic science which includes scientific method and techniques to recover and investigate data found in digital or electronic devices. One of the main objectives of image forensics techniques is to understand what kind of tampering has been applied. Copy–move forgery is one of the most common types of tampering for digital images. Block matching methods are good in pure translation, as they reach pixel-wise precision, they give information about the copied pixels, also work in case of homogeneous areas , but are extremely slow, and do not work well in case of geometric transformations. Point based methods achieve very good results, in case of geometrical transformations. But gives only information about single (or groups of) points that are part of the copy pasted area and not about the pixels inside the copied areas. Proposed method can be used for geometric transformations as well as for copy-move recognition and detection, as they are able to find the presence of copy-moved areas and to expose parts of them.

Keywords: Copy-move forgery, Block based method, Point based method, Delaunay triangulation, OFDM

Corresponding Author: MS. PALLAVI P PURI

Access Online On:

www.ijpret.com

How to Cite This Article:

Pallavi P. Puri, IJPRET, 2016; Volume 4 (9): 1174-1186

PAPER-QR CODE

INTRODUCTION

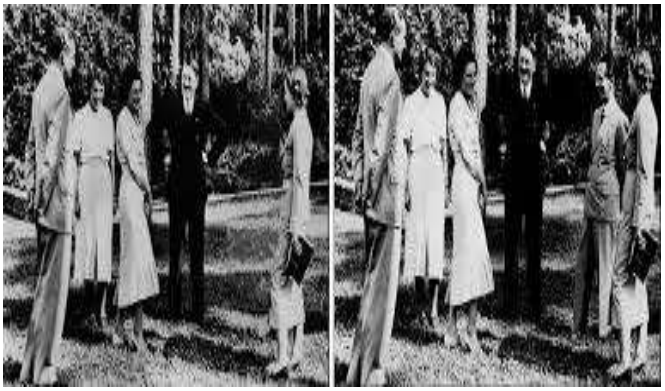
Digital Image Forensics deals with the problem of certifying the authenticity of a picture, or its origin [1]. An image has generally been accepted as a proof of occurrence of the depicted event. The availability of powerful digital image processing programs, such as Photo Shop, makes it easy to create digital forgeries from one or multiple images. The availability of low cost hardware and software tools, makes it easy to create, alter, and manipulated digital images with no obvious traces of having been subjected to any of these operations [2]. Therefore, it is important to verify the authenticity of digital images. Digital image forgery detection techniques are classified into active and passive approaches. In active approach, the digital image requires some pre-processing such as watermark image [5].

In passive technology does not need any digital signature generated or watermark embedded in advance. There are three techniques widely used to manipulate digital images. 1) Image Retouching 2) Image Splicing 3) Copy-Move [6].

(a) **(b)**

Figure.1. Example of image retouching. Original image (a), Tampered image (b).

Image Retouching is a process to transform a photograph into a desired image by cropping an image, eliminate “red-eye” or simply improve an image [19]. It is often much more explicit than subtle alterations to color balance or contrast and may involve changing a sign's text, for examples. Image editing software can be used to apply effects and warp an image until the desired result is achieved. The resulting image may have little or no resemblance to the photo from which it originated [20]. It involve enhancement i.e. adjusting colors , contrast, white balance, sharpness, noise, removing elements or visible flaws on skin or materials. In above example year is edited and sharpness is added in tampered image than original one.



(a) (b)

Figure. 2. Example of image splicing. Original image (a), Tampered image (b).

Image Splicing is a process in which an image editing method is used to copy a part of an image and paste it onto another image, and it is commonly followed by post processing such as local/global blurring, compression, and resizing [9]. The splicing tampered image could be used in news reports, photography contest, key proof in the academic papers, and so on, which could bring certain negative influences [15]. In above example one person is copied from external source and pasted in the original image to show his presence in the meeting. The tampered image shows the proof of occurrence of that person in meeting.

(a) (b)

Figure. 3. Example of copy-move forgery. Original image (a), Tampered image (b).

A copy-move forgery denotes an image where part of its content has been copied and pasted within the same image. Typical motivations are either to hide an element in the image, or to

emphasize particular objects, e.g., a crowd of demonstrators [25]. A copy-move forgery is straightforward to create. Additionally, both the source and the target regions stem from the same image, thus properties like the color temperature, illumination conditions and noise are expected to be well-matched between the tampered region and the image. In this paper we have discussed the copy-move forgery detection technique [26].

I. LITERATURE SURVEY

Edoardo Ardizzone, Alessandro Bruno, and Giuseppe Mazzola [1] This paper shows advantages of triangle of keypoints method over block based and point based method. With respect to block based methods, proposed methods can find, with a very high precision, the tampered areas of the images, also in case of geometric transformations at fast speed. In comparison with point based ones, proposed methods have a lower number of false positives at the image level. Davide Cozzolino, Giovanni Poggi, And Luisa Verdoliva [2] This paper states the accurate detection & localization of Copy Move Forgery in Dense field images. Patch Match is a suited for the computation of dense fields over images. This algorithm can efficiently reduce overall complexity and is a fast post-processing procedure based on dense linear fitting. Chi-Man Pun, Xiao-Chen Yuan, And Xiu-Li Bi [3] This paper states a new approach of copy–move forgery detection scheme by using 2 methods adaptive over segmentation and feature point matching which combines block-based and keypoint-based forgery detection methods. Jian Li, Xiaolong Li, Bin Yang, And Xingming Sun [4] In this paper the copy-move forgery is detected by extracting the keypoints for comparison. The proposed scheme first segments the test image into semantically independent patches prior to keypoint extraction.

Vishakha B. Pawar, Prof. Pritish A. Tijare, Prof. Swapnil N. Sawalkar [5] In this paper Cryptography is studied to secure the data in the field of network security. Various audio encryption algorithms are studied. Rohini.A.Maind, Alka Khade, D.K.Chitre [6] This paper states that the block based method. It can work without any digital watermarks or signatures information. It is strong to handle attacks such as multiple copy move forgery, noise adding and blurring. Sunil Joshi, Neha Kothari, Rashmi Suthar [7]. This paper states OFDM method & its application in wireless communication system. OFDM based wireless Communication system works by transmitting and receiving a compressed image.

Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, L. D. Tongo, and G. Serra [8] This paper states a new technique based on SIFT features to detect and localize copy-move forgery. It introduces a clustering procedure which operates in the domain of the geometric transformation. Tanzeela Qazi, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Joanna Kołodziej,

Hongxiang Li, Weiyao Lin, Kin Choong Yow, Cheng-Zhong Xu [9] This paper cover the blind techniques that have been proposed for exposing forgeries. The detection techniques for three of the most common forgery types copy/move, splicing and retouching are surveyed.

Beena R. Ballal, Ankit Chadha, Neha Satam [10] This paper gives an overview of OFDM, its applications in various systems such as IEEE 802.11a, Digital Audio Broadcasting (DAB) and Digital Broadcast Services to Handheld Devices (DVB-H) along with its advantages and disadvantages. V. Christlein, J. Jordan, C. Riess, and E. Angelopoulou [11] This paper shows that a key point-based method, based on SIFT features, can be very efficiently executed compared to other methods. It gives low computational load, combined with good performance. In block-based methods Zernike gives improved detection results among block-based feature sets. Pravin Kakar, N. Sudha [12] This paper states a novel technique based on transform-invariant features. These are obtained by using the features from the MPEG-7 image signature tools. The results display high true positive rates and extremely low false positives.

Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra [13] This paper shows a novel methodology to support image forensics investigation based on SIFT features. It can reliably detect if a certain region has been duplicated and, determine the geometric transformation applied to perform such tampering. Tie Liu, Zejian Yuan, Jian Sun, Jingdong Wang, Nanning Zeng [14] This paper shows a supervised approach for salient object detection which is formulated as a binary labeling problem using a set of local, regional, and global salient object features. Condition Random Field (CRF) model is used for detection of salient object. B.L.Shivakumar, Lt. Dr.S.Santhosh Baboo [15] This paper shows the effect of region duplication detection: without and with Scaling and Rotation for block based method. The conclusion of this paper is that the block based method fails to detect region duplication when scaling and rotation is applied on the copied image. Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee [16] In this paper, copy rotate- move (CRM) detection scheme is used for identifying and detecting suspicious image. The magnitude of Zernike moments is used to identify and localize the CRM region even though the region had been manipulated intentionally. E. Ardizzone, A. Bruno, and G. Mazzola [17] This paper describes the ability of some standard texture descriptors to detect copies in tampered images. A common framework is used to test descriptors: a block matching approach and a post-processing step, to filter out false positives. Block matching methods are not applicable when copies are processed by geometrical transformations.

Ramsay Dyer, Hao Zhang, And Torsten Moller [18] This paper shows that the delaunay triangulation characterizes a natural neighbor relation amongst points distributed in a

Euclidean space. In this survey to define triangle meshes for representing smooth surfaces embedded in 3D Euclidean space extensions of the delaunay paradigm that have been used. Hany Farid [19] This magazine states two technique for detecting image forgery. Digital watermarking has been proposed as a means by which an image can be authenticated. Passive techniques for image forensics operate in the absence of any watermark or signature. H. T. Sencar and N. Memon [20] this paper describes growing need for digital image forensics techniques. Ultimately, these techniques have to be incorporated together to obtain reliable decisions. Two major challenges to be met by image forensics research. Performance Evaluation and Benchmarking, Robustness Issue. H. Bay, T. Tuytelaars, And L. Van Gool [21] This paper introduce a novel scale- and rotation-invariant interest point detector and descriptor, coined SURF. Using this method there is increase in speed and accuracy. D. G. Lowe [22] This paper presents a keypoint method which extracts distinctive invariant features from images which can be used to perform reliable matching between different views of an object or scene. A.C. Popescu And H. Farid [23] This paper describes an efficient technique that automatically detects duplicated regions in a digital image. This technique efficiently works on credible forgeries, and quantify its robustness and sensitivity to additive noise and lossy JPEG compression.

III. COPY-MOVE FORGERY DETECTION METHODS

Image has been used as a proof of occurrence in the court of the law, business, fashion industry, scientific journals, military affairs, tabloid magazine, or at academic research. Due to advancement in technology, many tools have been developed to crop an image, to modify some features of an image, to enhance image can be done [6]. Due to which tampering of an image is done. Copy-Move forgery is tampering of an image by copying some portion of the image & pasting that portion in the same image in order to conceal some information, to misguide the court if it is used as a proof, or to divert the investigation [25]. Example of image tampering that appeared in press in July, 2008. The forged image shows four Iranian missiles but only three of them were real. In order to overcome copy-move forgery we first need to detect copy move forgery. The existing copy-move forgery detection methods are as follow.

1. Block Based Method.
2. Point Based Method.
3. Triangular Based Method.

A. *Block Based Method*

The first method which is used to detect copy-move forgery is block based method suggested by Fridrich. In this method the forged image is divided into the block & then some features from each block are compared with another block & if there is any similarity between the features of two blocks [6]. Then we found that the image is forged. This method is robust to noise, filtration & compression. But it can't be efficiently used for geometric transformation i.e. they cannot detect forgery if the rotation is done i.e. if the image is rotated by an angle of 60º & then it is pasted on the same image block based method is inefficient to find the forgery [20]. If the image is scaled i.e. if its size is increased or decreased & then pasted on same image block based method can't find the forged region.

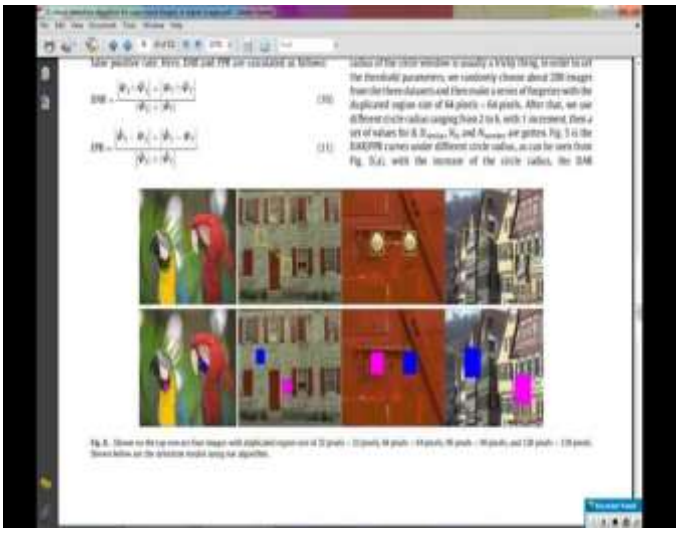


Figure. 4. Example of Block Based Method.

B. Point Based Method

The second method is point based method. In this method the interest points are extracted by using SIFT. Local descriptors are used to find the matching points in the image [3]. We use feature extraction and key point matching method in point based method [11]. This method is robust to geometric transformations. This method is not robust to homogenous areas. They give information only about points that are part of the copy pasted area of a single point, but not about the pixels that are inside the copied areas. Therefore they cannot be used to detect the copy-pasted areas, until a proper post-processing technique is used [1].

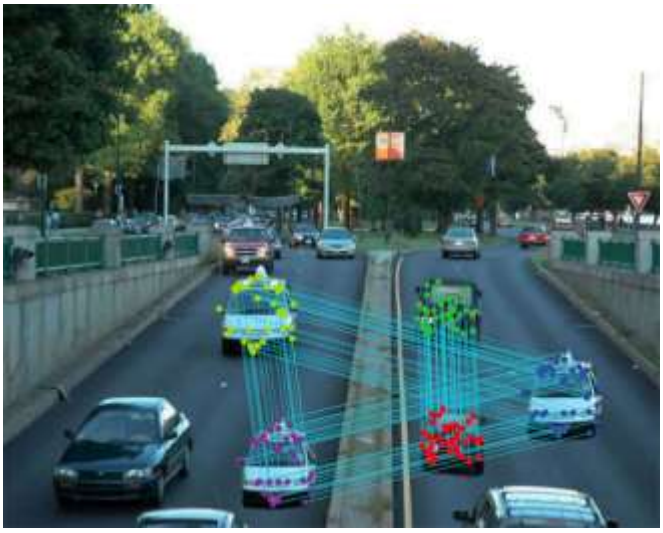


Figure. 5. Example of Point Based Method.

C. *Triangular Based Method*

The third method is Delaunay triangulation method suggested by Christlein [1] [18]. This method is hybrid of block based method & point based method. The point of interests are extracted first then based on that points delaunay triangles are built. As like block based method the image is divided into the triangles. This method is robust to geometric transformation & also to noise, filtration & compression. But in case of complex scenes, there are high numbers of detected triangles which influences the matching process, resulting in worse performances. We cannot use triangular method if no interest points are detected [1].

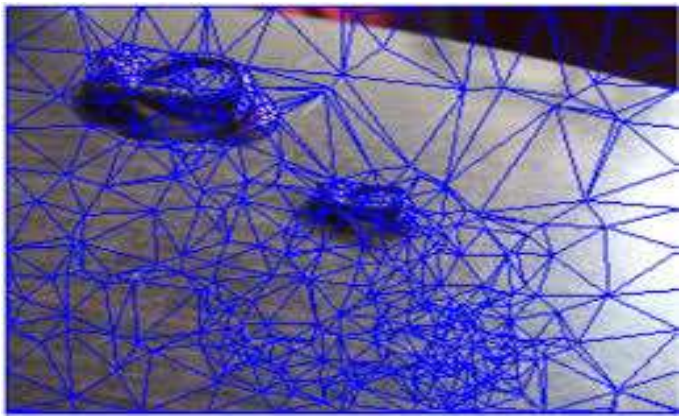


Figure. 6. Example of Triangular Method [1].

IV COPY-MOVE FORGERY DETECTION USING OFDM

OFDM was first projected by Chang [5]. OFDM is a method of digital modulation in which a signal is split into several narrowband channels at different frequencies. A frequency selective channel is converted into a parallel collection of frequency flat sub-channel by using OFDM. OFDM selects the subcarrier frequencies in such manner that the signals are mathematically orthogonal over one OFDM symbol period. Inverse fast fourier transform is used to attain modulation & multiplexing & also the required orthogonal signals are generated accurately by it [10].

OFDM is a technique which allows digital data to be reliably & efficiently transmitted over a radio channel even in heavy multipath environment. When we use OFDM in wireless communication system, the receiver does not need to adjust an equalizer as a single carrier system would. OFDM system has properties like high spectral efficiency, robustness to channel fading, immunity to impulse interference, capability of handling very strong echoes [7].

We are using OFDM Method for Detection of Copy-Move Forgery. It detects forgery in the following way.

Algorithm

1. Select Image.

2. Convert Image to Binary Format.

3. Enter Height. Calculate the Width using Formula.

   Width= Height *2 - 1.

4. Create Blank Orthogonal Matrix using above height & width.

5. For i=1 to Height

   Select binary image sample

   L (Binary Image) =Width

   Insert Binary Sample at i=0 Row.

   Set Width= Width-2.

Repeat Step 5 upto i= = Height.

End.

6. Save OFDM Segment.

7. For i=0 to cont (OFDM Segment)

Convert OFDM Segment to OFDM Image.

End.

8. Stop.

Select an image to find whether it is forged or not. Then convert it into binary format i.e. in the format of 1and 0. Now enter the height and width to form the orthogonal matrix. Height can be user define to calculate width we use formula Height * 2 – 1 to create orthogonal matrix. Then insert binary value into orthogonal matrix formed by height and width. In each step the width is decreased by 2 each 1 from both end to form orthogonal matrix Until i= = height. Then we will obtain orthogonal segment which are further converted into orthogonal images.

V. CONCLUSION

Image Forgery Detection is done to find out the authenticity of an image. So it is necessary to find out the type of forgery done on an image. Copy Move Forgery is an image forgery in which image is copy from same image and pasted at different place on same image so as to conceal some information. To detect copy move forgery litrture had used block based method, point based method and Delaunay triangle method. Block based method is robust to noise, filtration & compression. But it can't be efficiently used for geometric transformation. Point based method is robust to geometric transformations. This method is not robust to homogenous areas. Delaunay method is robust to geometric transformation & also to noise, filtration & compression. But in case of complex scenes it gives worst performance. In this paper a new approach i.e. an OFDM method will be used to detect the copy-move forgery area or region. This method can be robust to geometric transformation i.e. it can be efficiently used to determine forgery even if rotation of image is done or if the image is resize. The proposed method may be fast compare to all the existing ones.

REFERENCES

1. Edoardo Ardizzone, Alessandro Bruno, And Giuseppe Mazzola, "Copy–Move Forgery Detection By Matching Triangles Of Keypoints," IEEE Transactions On Information Forensics And Security, Vol. 10, No. 10, October 2015.
2. Davide Cozzolino, Giovanni Poggi, And Luisa Verdoliva, "Efficient Dense-Field Copy–Move Forgery Detection," IEEE Transactions On Information Forensics And Security, Vol. 10, No. 11, 2015.
3. Chi-Man Pun, Xiao-Chen Yuan, And Xiu-Li Bi, "Image Forgery Detection Using Adaptive Over Segmentation And Feature Point Matching," IEEE Transactions On Information 3.Forensics And Security, Vol. 10, No. 8, August 2015.
4. Jian Li, Xiaolong Li, Bin Yang, And Xingming Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015.
5. Ms. Vishakha B. Pawar, Prof. Pritish A. Tijare, Prof. Swapnil N. Sawalkar, "A Review Paper On Audio Encryption," International Journal Of Research In Advent Technology, Vol.2, No.12, December 2014.
6. Rohini.A.Maind, Alka Khade, 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.
7. Sunil Joshi, Neha Kothari, Rashmi Suthar, "Orthogonal Frequency Division Multiplexing Based Wireless Communication System For Digital Broadcast Applications," IP Multimedia Communications A Special Issue From IJCA.
8. I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, L. D. Tongo, And G. Serra, "Copy-Move Forgery Detection And Localization By Means Of Robust Clustering With J-Linkage," Signal Image Communication, Vol. 28, No. 6, Pp. 659–669, Jul. 2013.
9. Tanzeela Qazi, Khizar Hayat, Samee U. Khan, Sajjad A. Madani, Imran A. Khan, Joanna Kołodziej, Hongxiang Li, Weiyao Lin, Kin Choong Yow, Cheng-Zhong Xu, "Survey On Blind Image Forgery Detection," The Institution Of Engineering And Technology 2013 IET Image Process., 2013, Vol. 7, Iss. 7, Pp. 660–670.
10. Beena R. Ballal, Ankit Chadha, Neha Satam, "Orthogonal Frequency Division Multiplexing And Its Applications," International Journal Of Science And Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 1, January 2013.

11. V. Christlein, C. Riess, J. Jordan, C. Riess, And E. Angelopoulou, "An Evaluation Of Popular Copy-Move Forgery Detection Approaches," IEEE Trans. Inf. Forensics Security, Vol. 7, No. 6, Pp. 1841–1854, Dec. 2012.
12. Pravin Kakar, N. Sudha, "Exposing Postprocessed Copy-Paste Forgeries Through Transform-Invariant Features," IEEE 2012.
13. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, And G. Serra,"A SIFT-Based Forensic Method For Copy–Move Attack Detection And Transformation Recovery," IEEE Trans. Inf. Forensics Security, Vol. 6,No. 3, Pp. 1099–1110, Sep.2011.
14. T. Liu Et Al., "Learning To Detect A Salient Object," IEEE Trans. Pattern Anal. Mach. Intell.,Vol.33,No.2.Pp.353–367,Feb.2011.
15. B. L. Shivakumar And S. S. Baboo, "Detecting Copy-Move Forgery In Digital Images: A Survey And Analysis Of Current Methods," Global J. Computer. Sci. Technol., Vol. 10, No.7,Pp.61–65,2010.
16. S. J. Ryu, M.J. Lee, And H.K. Lee, "Detection Of Copy-Rotate-Move Forgery Using Zernike Moments," In Proc. Inf. Hiding Conf., Jun. 2010 , Pp. 51–65.
17. E. Ardizzone, A. Bruno, And G. Mazzola , "Copy-Move Forgery Detection Via Texture Description," In Proc. 2nd ACM Workshop Multimedia Forensics, Security Intell. (Mifor), 2010, Pp. 59–64.
18. Ramsay Dyer , Hao Zhang, And Torsten Moller, "A Survey Of Delaunay Structures For Surface Representation," Gruvi Lab, School Of Computing Science, Simon Fraser University, Canada January 16, 2009.
19. H. Farid, "Image Forgery Detection," IEEE Signal Process. Mag., Vol. 26, No.2 , Pp.16–25,Mar.2009.
20. H. T. Sencar And N. Memon, "Overview Of State-Of-The-Art In Digital Image Forensics," Algorithms, Archit. Inf. Syst. Security, Vol. 3 ,Pp. 325–348, Dec. 2008.
21. H. Bay, T. Tuytelaars, And L. Van Gool, "SURF: Speeded Up Robust Features," In Proc. Eur. Conf. Comput. Vis. (ECCV), 2006
22. D. G. Lowe, "Distinctive Image Features From Scale-Invariant Keypoints," Int. J. Computer Vis., Vol. 60, No. 2, Pp. 91–110, Nov. 2004.
23. A.C. Popescu And H. Farid, "Exposing Digital Forgeries By Detecting Duplicated Image Regions," Dept. Computer Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.
24. G. Li, Q. Wu, D. Tu, And S. Sun, "A Sorted Neighborhood Approach For Detecting Duplicated Regions In Image Forgeries Based On DWT And SVD," In Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2007, Pp. 1750–1753

25. J. Fridrich, D. Soukal, And A. J. Lukáš , "Detection Of Copy-Move Forgery In Digital Images," In Proc. Digit. Forensic Res. Workshop, Cleveland, OH, USA, Aug. 2003, Pp. 342–358.
26. W. Luo, J. Huang, And G. Qiu, "Robust Detection Of Region-Duplication Forgery In Digital Image," In Proc. 18th Int. Conf. Pattern Recognit., 2006, Pp. 746–749.
27. W. Li And N. Yu, "Rotation Robust Detection Of Copy-Move Forgery," In Proc. 17th IEEE Int. Conf. Image Process. (ICIP), Sep. 2010, Pp. 2113–2116.
28. X. Pan And S. Lyu, "Region Duplication Detection Using Image Feature Matching," IEEE Trans. Inf. Forensics Security, Vol. 5, No. 4, Pp. 857–867, Dec. 2010.
29. E. Ardizzone, A. Bruno, And G. Mazzola, "Detecting Multiple Copies In Tampered Images," In Proc. 17th IEEE Int. Conf. Image Process. (ICIP), Sep. 2010, Pp. 2117–2120.
30. B.L Shivakumar, S.S Baboo, "Detection Of Region Duplication Forgery In Digital Images Using SURF," Int. J. Computer Science Issues, Vol. 8, No. 4, Pp. 199–205, 2011.