International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137

Volume – 01, Issue – 09, December – 2016, PP – 01-10

Detection of Cloning Forgery Images using SURF + DWT and PCA

Manpreet Singh, Er. Harpal Singh[2]

[1]Research Scholar M-Tech, Computer Science and Engineering, Guru Kashi University, India

[2]Assiatant Professor, UCCA, Guru Kashi University, India

Abstract: Over the last few years, there has been a growing body of work on tools for digital image forensics. These tools are capable of detecting tampering in images from any camera, without relying on watermarks or specialized hardware. Instead of watermarks, these tools assume that images possess certain regularities that are disturbed by tampering. So to evaluate the algorithms for image manipulation and to group they based upon their degree of manipulation. It is also important to consider image compression of image files in the area of work. An evaluation and comparison of the existing forgery detection techniques, and carry out the evaluation along with defining a new grouping structure for forgery detection techniques. There are cases when it is difficult to identify the edited region from the original image. Detection of forgery part of an image drives a need of an authenticity and to maintain integrity of an image. Here in work two techniques such DWT and PCA with SURF as detector is implemented to detect the forged part of an image from tampered image. Both algorithms have their own validation but PCA with Surf improves to be better in all respective. As in PCA SURF we can detect as well remove the forged object and it also takes less time to solve the detection problem than DWT SURF.

Keywords: SURF, PCA, DWT, tampering, Forged.

I. INTRODUCTION

A digital image is a numeric representation of a two-dimensional image. Depending on whether the image resolution is fixed, it may be of vector or raster type. Without qualifications, the term "digital image" usually refers to raster images also called bitmap images. When we see a picture on our monitor or use our digital camera (or scanner), the image we are viewing or dealing with is not continuous like a pencil drawing – it is made up of many small elements next to each other. When we have enough elements, we get the illusion of a picture or image. Early digital images (before color) appeared in black and white. The tiny elements that comprised digital images were either black or white. These two 'colors' corresponded to 1 and 0 (called BITS or BI-nary digits). Digits 1 and 0 are used in the binary (base 2) system. Thus, a map (pattern) made up of these 1's and 0's was referred to as a bit-map. All digital images are a rectangle or square. Today, the elements are called pixels.

Forensics means the use of science and technology in the investigation and establishment of facts. So the photographs or other pictures can be transmitted to and reconverted into pictures by another computer. Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices. Digital image forensics aims at validating the authenticity of images by recovering information about their history. Two main problems are addressed: the identification of the imaging device that captured the image, and the detection of traces of forgeries. Nowadays, thanks to the promising results attained by early studies and to the always growing number of applications, digital image forensics represents an appealing investigation domain for many researchers. With the widespread availability of image editing software, digital images have been becoming easy to manipulate and edit even for non-professional users. Image manipulation has become commonplace with growing easy access to powerful computing abilities. Some common image manipulation with the intension of deceiving a viewer includes:-

Copy and paste

Composition or Splicing

Retouching, healing, cloning

Content embedding or Steganography

Nowadays, due to rapid advances and availabilities of powerful image processing software, modifying the content of digital images becomes much easier with the help of sophisticated software such as Adobe Photoshop. Digital watermarking is the process of embedding information into a digital signal which may be

used to verify its authenticity or the identity of its owners. There are several characteristic of watermarked image:

1. Robustness
2. Perceptibility
3. Capacity
4. Embedding method

There are many ways to categorize the image tampering, and generally, we can tell that some usually performed operations in image tampering are:

1. Deleting or hiding a region in the image.
2. Adding a new object into the image
3. Misrepresenting the image information;

to insert and splicing image part of the original image is the one of the most typical method. Watermarking is the popular way to counterfeit the forgery image. The digital watermark, unlike the printed visible stamp watermark, is designed to be invisible to viewers. The bits embedded into an image are scattered all around to avoid identification or modification. Therefore, a digital watermark must be robust enough to survive the detection, compression, and operations that are applied on.

II. LITERATURE SURVEY

Rutuja Tendulkar (2015), here authors refer to authentication of an image received from communication network as a challenging as well as a necessary task. Copy-move forgery is common type of digital image forgery where a region from the image is copied and pasted in the same image at different location. Here he proposed an algorithm to find copy-move forgery using transform domain. It applies Discrete Wavelet Transform (DWT) and Fast Fourier Transform (FFT) on a forged image to find matching blocks. With the help of border pixel variation technique, it finds the original and forged block from the detected matching blocks. Here algorithm increases the accuracy of forged region detection and reduces computational complexity of detection process. [6]. Sushama Kishor Bhandare (2015), here author said that photo editing tools and software are easily available to modify the images but such modified images become problematic in some areas where the geniuses of image has a prime important and in such fields it become extremely difficult to verify the authenticity and integrity of digital images. Modern software has made the manipulation of photos easier to carry out and harder to uncover than ever before. Therefore there feel a need to find out a forensic technique which will be capable to detect the tampering in modified digital images and to verify images authenticity. Here reviews the forensic methods for detecting globally and locally applied contrast enhancement, cut-and-paste forgery, histogram equalization, and noise in the digital image. [7] Mohammad Farukh Hashmi (2014), here author describes that the storing of the information is no more a problem and the information can be easily passed on from one place to another in digital format. The big benefit however comes with the hidden loss and in this case it is the tampering of images and videos which has become a matter of serious concern in recent days because of the readily available software tools in the market like Photoshop etc. which can be used by a common person to tamper the image or video for hiding or changing the original contents. Thus for the aforementioned problem, proposed a series of algorithms which are combination of speeded-up robust feature transforms and Wavelet Transforms. The results obtained conclude the proposed algorithms are better than their counterparts both in terms of computational complexity and invariance to scale and rotation and also for the combination of attacks. [1] Jessica Fridrich, images can be easily modify by many software application as to add and remove important features from an image without leaving any obvious traces of tampering. Detection of malicious manipulation with digital images (digital forgeries) are worked out. Here of digital forgery – the copy-move attack in which a part of the image is copied and pasted somewhere else in the image with the intent to cover an important image feature. Here the problem of detecting the copy-move forgery and describe an efficient and reliable detection method such as DCT is worked which has successfully detect the forged part even when the copied area is enhanced/retouched to merge it with the background and when the forged image is saved in a lossy format, such as JPEG [3]. Takwa Chihaoui (2014), data are created in digital form allowing easy control over storage and manipulation due to the technology which dragged a lot of risks, especially the ones related to the security as it is easier to create fake images without leaving any obvious perceptual traces of tampering. Here , a method that automatically detects duplicated regions in the same image is worked out by using the Scale Invariant Feature Transform (SIFT) and Singular Value Decomposition (SVD) method. Results of hybrid method is robust to geometrical transformations and is able to detect with high performance duplicated regions [8]. Ramesh Chand Pandey, As sophisticated image editing softwares, it has become easy to forge digital images which can be forged using copy-move technique to duplicate or hide undesirable objects. While

object whened copy-moved with the help of geometrical and illumination transform, it becomes difficult to detect that object. Speed up Robust Feature (SURF) and Scale Invariant Feature Transform (SIFT) are invariant with respect to geometrical and illumination transform. Here, method SURF and SIFT, both are used to make it very fast and robust in detecting copy-moved regions[5]. I. Amerini (2014), several image application domains, including Image Forensics (e.g. detection of copy-move forgery or near duplicates) uses SIFT method. SIFT techniques are quite effective in producing an attacked image with very few (or no) keypoints, but at the expense of an image distortion. Here effectiveness of the attacking methods is evaluated also from the side of perceptual image quality; a new version of a SIFT keypoint removal method, based on a perceptual metric, has worked with series of perceptive experiments[2]. Tushant A. Kohale (2014) have studied Digital images are the most important source of information transfer. The availability of powerful digital image processing software's, makes it relatively easy to create digital forgeries from one or multiple images. In today's world it is easy to manipulate the image by adding or removing some elements from the image which result in a high number of image forgeries. A copy-move forgery is created by copying and pasting content within the same image, and potentially post-operating it. The detection of copy-move forgeries has become one of the most actively researched topics in blind image forensics. The key objectives of the proposed approach is to study the effect of different types of tampering on the digital image, detect image forgery by copy-move under many types of attacks by combining block-based and feature based method and accurately locating the duplicated region[10]. Salma Amtullah (2014) studied Tampering in digital images has become very easy due to the availability of advanced image editing software's to the users. Images are being tampered in a very efficient manner without leaving any visual clue. As a consequence, the content of digital images cannot be taken as for granted. There are various types of image tampering techniques. One of the most common tampering techniques is copy-move forgery. In copy-move forgery one part of an image is copied and pasted in another part of the same image. In this paper, the passive image forensic method is presented to detect copy move forgery in digital images. The proposed method is based on SURF (Speed Up Robust Features) algorithm. In this method the features are extracted and their descriptors are obtained by SURF algorithm and the Nearest Neighbor approach is used for feature matching to identify the copy move forgery in digital images. This detection method is found to be rotation and scale invariant and is robust enough to noise, jpeg compression and blurring. Multiple copy move forgery is also detected by this method [11]. P.Kakar (2011) Image manipulation has become commonplace with growing easy access to powerful computing abilities. In this paper, the author propose a novel technique based on transform-invariant features. These are obtained by using the features from the MPEG-7 image signature tools. Results are provided which show the efficacy of this technique in detecting copy-paste forgeries, with translation, scaling, rotation, flipping, lossy compression, noise addition and blurring. We obtain a feature matching accuracy in excess of 90% across post processing operations, and are able to detect the cloned regions with a high true positive rate and lower false positive rate than the state of the art [12].

III. METHDOLOGY

The Proposed method of copy-move forgery detection has following main parts.

1. Discrete Wavelet Transform
2. Lexicographic Sorting
3. Shift Vector Calculation
4. Neighbor block matching

This method will work as follows:-

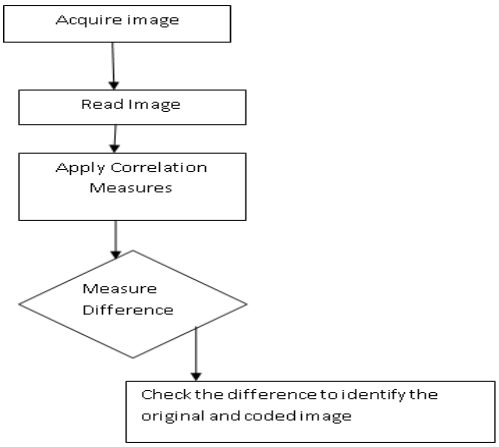


Figure 1.1: Flow chart to define the methodology

IV. RESULTS

The result and analysis explain is implemented that shows of the copy paste part of the images. In this chapter database is used to detect the forensics images.

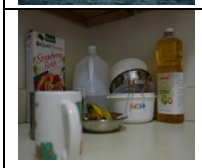
Original image	Detected by DWTSURF	Detected by PCASURF
		
		
		

Figure 1.2: Original image with detected and removed part of forged image

4.1. Result with DWT technique

In Matlab, all implementation is done to perform the outcome as to detect the copy pasted part.
Figure 1.3 to 1.7 shows the DWT results. Figure 1.3, shows the original image.

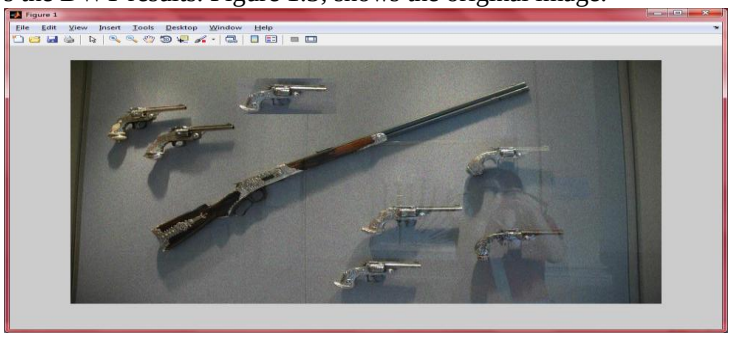


Figure 1.3: Original image for DWT

Figure 1.4 below shows the processed input image, after decomposed and output image after all processing.

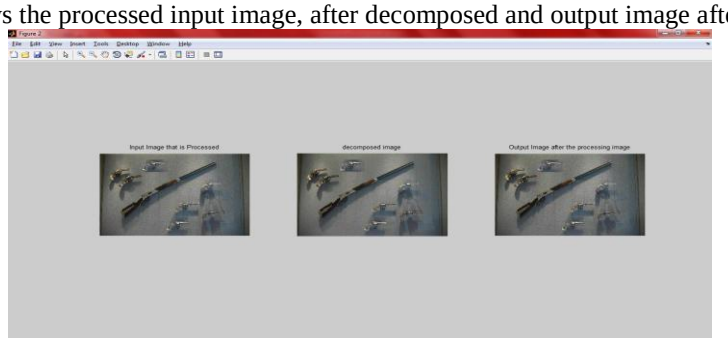


Figure 1.4: Input image after processing and decomposed firstly by DWT

Below Figure 1.5, shows the image with different color intensity as red, green , blue colors are also decomposed further in Lower part of level.

Figure 1.5: Input image in LL part with color intensity by DWT

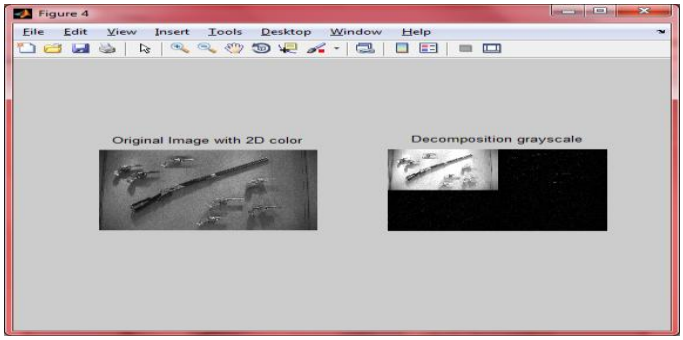


Figure 1.6: Image with 2D color and decomposed Garyscale Image by DWT

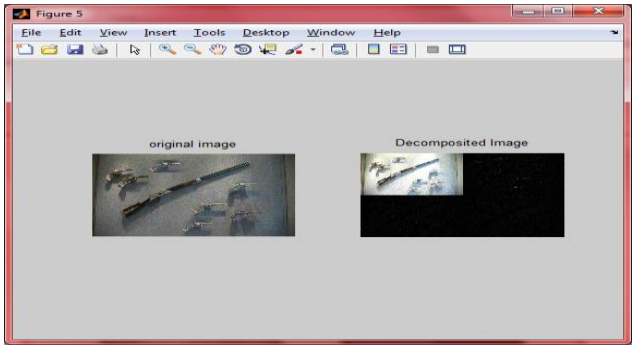


Figure 1.7: Original Image and decomposed Image by DWT

Figure 1.6. above shows the original image with 2 d coloir and that image after decomposition in gray scsle image. Figure 1.7, shows the original image with the Decompositon level which have been given as for compression. Or compressesd decomposited image is shown.

4.2. Result with SURF technique

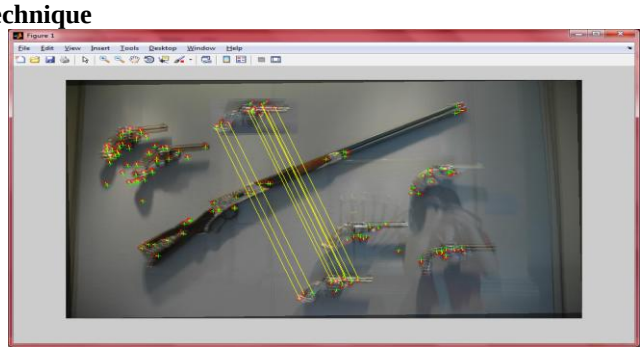


Figure 1.8: Forged Image with detection of copied part by SURF

Figure 1.8, shows the surf techniques in which copied part of images is detected from forged image.

4.3. Result with DWT SURF technique

In Matlab, all implementation is done to perform the outcome as to detect the copy pasted part.

Figure 1.9 to 1.10 shows the DWT SURF results. Figure 1.9, shows the original image.

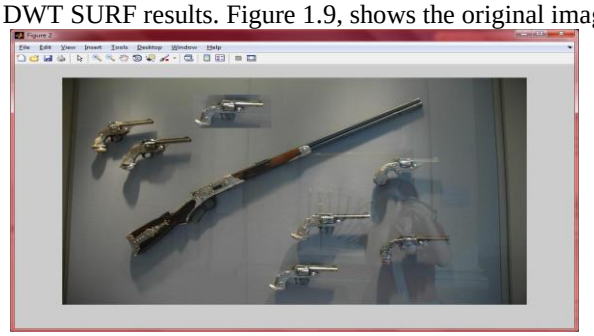


Figure 1.9: Original Forged Image for DWTSURF

Below Figure 1.10, shows the detection of copied part from forged image by using DWTSURF techniques

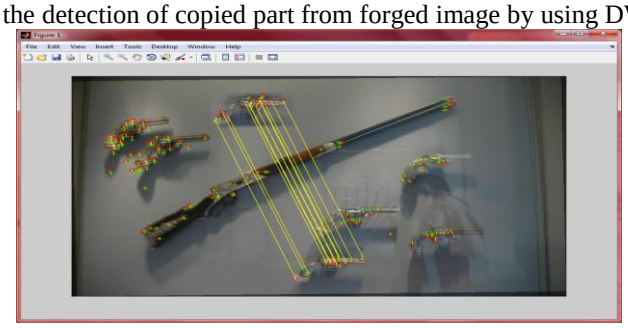


Figure 1.10: Detection of Forged Image by DWTSURF

4.4. Result with PCA technique

Figure 1.11, below shows the detection on by performs parameters by using PCA technique.

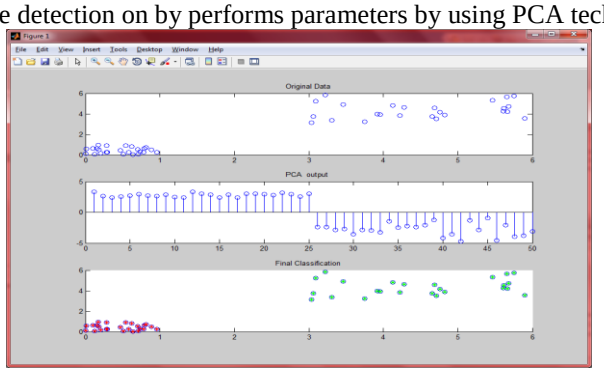


Figure 1.11: Detection of parameter for Forged Image by PCA

4. 5. Result with PCASURF technique

Figure 1.12, below shows the detection on by performs parameters by using PCA SURF technique.

Figure 1.12: Detecting Original Part of Forged Image by PCASURF

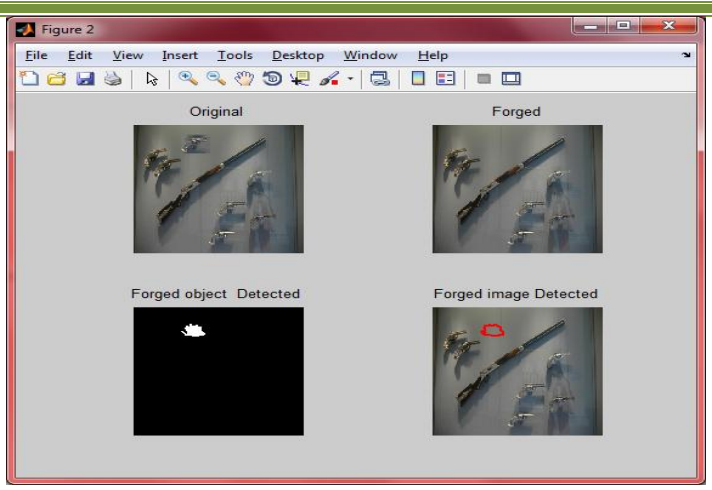


Figure 1.13: Detecting Copied Part of Forged Image by PCASURF

Figure 1.13, above shows the detection part of copied in forged image using PCA SURF technique. In above window four parts are shown, first part is the original image, second shows the Forged image. Third image is the image where actually detected part from black and white image means 2D color. Then at last, forged means copied part is shown in the forged image.

V. DISCUSSION

The above images show the different copy paste parts of the images according to the true and false detection. In this all the above images having red part using PCA SURF technique is the copy and paste part that is detected from the original images. Same way DWT Surf technique is used from above images it shows through lines what from where which part has been copied. Both the techniques use their own way for detection but as comparing we can say that PCA SURF is bests detection technique as it detect the object and also remove that part where as DWT SURF does not remove the detected part what only tells that from where the part has been copied. From table 5.1, it is clarified that PCA SURF is best as it take half or less time compared to DWT SURF and results in more clarity of detecting of copied object.

Table: 1.1 Comparisons through Elapsed Time of PCA SURF and DWT SURF

Images/ Techniques	**PCA SURF**	**DWT SURF**
	**7.0930**	**15.0693**
	**4.6027**	**14.3953**
	**4.0719**	**14.1402**
	**7.0746**	**15.9955**

VI. CONCLUSION

Digital image forensics aims at validating the authenticity of images by recovering information about their history. Copy-paste forgery, where in a region from an image is replaced with another region from the same image (with possible transformations). Because the copied part come from the same image, its important properties, such as noise, color palette and texture, will be compatible with the rest of the image and thus will be more difficult to distinguish and detect these parts. Digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history. The fundamental problems which research found in the literature can be categorized into the natural, forgery detection, flow mapping, and source identification. Therefore, the originality and authenticity of images or data in many cases become challenging problem. Researchers have related the natural issues to the advance in computer graphics, animation, multimedia in the association of high computing machines, algorithms, increases the complexity of the issue.In response to this, researchers have begun developing digital forensic techniques capable of identifying digital forgeries. These forensic techniques operate by detecting imperceptible traces left by editing operations in digital multimedia content. In this dissertation, we propose several new digital forensic techniques to detect evidence of editing in digital multimedia content. We use DWT and PCA with SURF for forensic tasks such as identifying cut-and-paste forgeries from compressed images. Additionally, we consider the problem of multimedia security from the forger's point of view. PCA SURF is best compared to DWT SURF in tme and Clarity of detecting objects.

VII. FUTURE SCOPE

In the future we can use real time images to detect the copy and paste part with the help of frames and masking. To detect these different techniques applied by DCT, correlation and filters.

REFERENCES

[1]. Andrea Costanzo, Irene Amerini, Roberto Caldelli, "Forensic Analysis of SIFT Key point Removal and Injection," in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 9, SEPTEMBER 2014.

[2]. I. Amerini et al., "EXPLOITING PERCEPTUAL QUALITY ISSUES IN COUNTERING SIFT-BASED FORENSIC METHODS," in 2014 IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP).

[3]. Jessica Fridrich, David Soukal, and aJan Lukáš, "Detection of Copy-Move Forgery in Digital Images".

[4]. Mohammad Farukh Hashmi, Vijay Anand, Avinash G. Keskar "A Copy-move Image Forgery Detection Based on Speeded Up Robust Feature Transform and Wavelet Transforms" 2014 5th International Conference on Computer and Communication Technology, 978-1-4799-6758-2/14/$31.00 ©2014 IEEE.

[5]. Ramesh Chand Pandey et al., "Fast and Robust Passive Copy-Move Forgery Detection Using SURF and SIFT Image Features., vol. 15, no. 4, p. 041102, 2006.

[6]. Rutuja Tendulkar, Associate Prof. Manoj Sabnis, "Copy-Move Image Forgery Detection Using Transform Domain", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.

[7]. Sushama Kishor Bhandare, Nitin Krishnarao Bhil, "Digital Image Forensic", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 7, July 2015.

[8]. Takwa Chihaoui, Sami Bourouis, and Kamel Hamrouni, "COPY-MOVE IMAGE FORGERY DETECTION BASED ON SIFT DESCRIPTORS AND SVD-MATCHING," in 1st International Conference on Advanced Technologies for Signal and Image Processing - ATSIP'2014, March 17-19, 2014, Sousse, Tunisia.

[9]. Harpreet Kaur, Kamaljeet kaur, "A Brief Survey of Different Techniques for Detecting Copy Move Forgery", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, 2015.

[10]. Tushant A. Kohale*, Prof. P. R. Lakhe " Detection of Post operated Copy Move Image Forgery by Integrating Block Based and Feature Based Method" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014 ISSN: 2277 128X.

[11]. Salma Amtullah, Dr. Ajay Koul "Passive Image Forensic Method to detect Copy Move Forgery in Digital Images" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 96-104.

[12]. P. Kakar and N. Sudha "Exposing Post processed Copy-Paste Forgeries through Transform-Invariant Features", vol. 206, no. 1-3, pp. 178–184, 2011.

[13]. S. Bayram, H. T. Sencar and N. Menon "A Survey of Copy-Move Forgery Detection Techniques", submitted to ICASSP 2009, 2009.

[14]. Dhara Anandpara" A Joint Forensic System to Detect Image Forgery using Copy Move Forgery Detection and Double JPEG Compression Approaches" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

[15]. M. C. Stamnn, "Forensics Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Transactions on information Forensics And Security, vol. 5 No 3, 2010.

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

[17]. M. K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," in Proc. ACM Multimedia and Security Workshop, New York, NY, 2005, pp. 1–10.

[18]. T.-T. Ng, S.-F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," in Proc. IEEE Int. Symp. Circuits Systems, Vancouver, BC, Canada, May 2004, vol. 5, pp. V-688–V-691.

[19]. S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Image, vol. 15, no. 4, p. 041102, 2006.

[20]. Pan, X. Z., & Wang, H. M. "The Detection Method of Image Regional Forgery Based DWT and 2DIMPCA", Advanced Materials Research, 532, 692-696, 2012.

[21]. Shiva kumar, B., & Baboo, S. S., "Automated Forensic Method for Copy-Move Forgery Detection based on Harris Interest Points and SIFT Descriptors", International Journal of Computer Applications, 27(3), 2011.

[22]. Yao, H., Qiao, T., Tang, Z., Zhao, Y., & Mao, H., "Detecting Copy-Move Forgery Using Non-negative Matrix Factorization", Paper presented at the Third International Conference on Multimedia Information Networking and Security (MINES), 2011.

[23]. Pujari, V. S., & Sohani, M, "A Comparative Analysis On Copy Move Forgery Detection Using Frequency Domain Techniques", International Journal of Global Technology Initiatives, 1(1), E104-E111, 2012.

[24]. Chen, L., Lu, W., Ni, J., Sun, W., & Huang, J, "Region duplication detection based on Harris corner points and step sector statistics", Journal of Visual Communication and Image Representation, 24(3), 244-254, 2013.

[25]. Liu, M.-H., & Xu, W.-H., "Detection of copy-move forgery image based on fractal and statistics", Journal of Computer Applications, 8, 061, 2011.

[26]. Yadav, P., Rathore, Y., & Yadu, A., "DWT Based Copy-Move Image Forgery Detection", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 1(5), 56-58, 2012.

[27]. Pujari, V. S., & Sohani, M., "A Comparative Analysison Copy Move Forgery Detection in Spatial Domain Method Using Lexicographic and Non Lexicographic techniques", IJECCE, 3(1), 136-139, 2012.

[28]. Shiva kumar, B., & Santhosh Baboo, L. D. S., "Detecting copy-move forgery in digital images: a survey and analysis of current methods", Global Journal of Computer Science and Technology, 10(7), 2010.

[29]. Chen, L., Lu, W., & Ni, J. (2012). An Image Region Description Method Based on Step Sector Statistics and its Application in Image Copy-Rotate/Flip-Move Forgery Detection. International Journal of Digital Crime and Forensics (IJDCF), 4(1), 49-62, 2012.

[30]. Liu, G., Wang, J., Lian, S., & Wang, Z., "A passive image authentication scheme for detecting region duplication forgery with rotation", Journal of Network and Computer Applications, 34(5), 1557-1565, 2011.

[31]. Sridevi, M., Mala, C., & Sanyam, S., "Comparative Study of Image Forgery and Copy-Move Techniques", Advances in Computer Science, Engineering & Applications (pp. 715-723): Springer, 2012.

[32]. A merini, I., Barni, M., Caldelli, R., & Costanzo, A, "Counter-forensics of SIFT-based copy-move detection by means of key point classification", EURASIP Journal on Image and Video Processing, 2013(1), 18.

[33]. Muhammad, G., Hussain, M., Khawaji, K., & Bebis,G., "Blind copy move image forgery detection using dyadic undecimated wavelet transform", Paper presented at the Digital Signal Processing (DSP, 2011.

[34]. Piva, A., "An Overview on Image Forensics", ISRN Signal Processing, 2013.

[35]. Wang, J.-W., Liu, G.-J., Zhang, Z., Dai, Y., & Wang. Z., "Fast and robust forensics for image region duplication forgery", Acta Automatica Sinica, 35(12), 1488-1495, 2009.

[36]. Mahdian, B., & Saic, S., "Bibliography on blind methods for identifying image forgery", Signal Processing: Image Communication, 25(6), 389-399, 2010.

[37]. Math, S., & Tripathi, R., "Digital Forgeries: Problems and Challenges", International Journal of Computer Applications, 5(12), 2010

[38]. M. Chen, J. Fridrich, M. Goljan, and J. Luká˘s, "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[39]. T.-T. Ng, S.-F. Chang, J. Hsu, L. Xie, and M. P. Tsui, "Physics-motivated features for distinguishing photographic images and computer graphics," in Proc. ACM Multimedia, Singapore, 2005, pp. 239–248.

[40]. A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," IEEE Transactions on Signal Processing, vol. 53(2), pp. 758–767, 2005.

[41]. M.K. Johnson and H. Farid, "Exposing digital forgeries by detecting inconsistencies in lighting," Proc. ACM Multimedia and Security Workshop, New York, pp. 1–9, 2005.

[42]. M.Wu A. Swaminathan and K. J. Ray Liu, "Image tampering identification using blind deconvolution," Proc. IEEE ICIP, 2006.

[43]. S.Khan and A.Kulkarni ,"Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform" International Journal of Computer Applications (0975 – 8887) Volume 6– No.7, September 2010.

