ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Review And Analysis of Image Forgery Detection Technique for Digital Images

Navneet Kaur[#1], Navdeep Kanwal[*2]

[#]Department of Computer Engineering, Punjabi University, Patiala
Patiala, Punjab,India
*Assistant Professor, Department of Computer Engineering, Punjabi University, Patiala
Patiala, Punjab,India

***Abstract*--**Digital visual media have turned into the principle data bearers in the computerized time. Recently the quality of advanced visual data has been questioned because of straightforwardness in duplicating both its source and content. Digital image forensics is a shiny new research field which goes for approving the genuineness of pictures by recouping data about their history. Two fundamental issues tended to are: the recognizable proof of the imaging gadget that caught the image, and the detection of hints of forgeries. In the fields for example crime scene investigation, medical imaging, e-commerce and mechanical image validness and integrity of advanced pictures are the key. Further image forgery can be active or passive. In active approach the digital image requires some kind of pre-processing such as watermark or signatures generated at the time of creating the image. Passive approach includes the concept of copy move forgery, image splicing and retouching which is a great challenge in image processing techniques.

Keywords*--Digital image tempering, copy move forgery, image splicing, DCT, SIFT.*

1. INTRODUCTION

Images and videos have turned into the fundamental data transporters in the advanced period. The least difficult video in TV news is regularly acknowledged as a confirmation of the honesty of the reported news. Correspondingly, video observation, recordings can constitute principal trial material in an official court room. Together with undoubted advantages, the availability of advanced visual media brings a major drawback. Image processing specialists can undoubtedly get to and alter picture content in this way its significance without leaving outwardly noticeable follows is lost. Besides, with the easy availability of editing tools, the craft of altering and forging visual substance is not any more limited to specialists. As a result, the alteration of image for malicious purposes has become common. Digital forensics is the way toward revealing and translating electronic information. The objective of procedure is to detect any proof in its most beginning structure while carrying out an organized examination by gathering, distinguishing and approving the computerized data for reason for reproducing past confirmations. An image can experience diverse types of assaults amid the tempering process. Among these assaults, the least complex one is the copy move, in which the part of the picture is copied inside the same picture. The picture parts can likewise be replicated from different pictures (image splicing) and the picture itself or the altered locales can other distinctive sorts of changes to make the tempering undetectable. Likewise selected to assemble the distinctive visually impaired image forgery detection approaches under five noteworthy categories i.e., pixel-based, compression based, camera-based, physics based, and geometric based method[1].

A. Pixel based method:

This method depends on distinguishing the measurable inconsistencies happened in picture pixels amid the tempering process. These systems additionally break down relationships among pixels acquainted due with the particular type of altering in a spatial area or a changed space. These methods pixel based visually impaired forgery detection location systems have been the most generally utilized methods particularly when we realize that the easiest and most generally utilized ways to deal with falsification are additionally pixel based. Such strategies depend on the investigation of between pixel relationships that emerge from altering, either straightforwardly or indirectly. As said in the Introduction, the most regular pixel-based falsification discovery methodologies are copy move, Image splicing, Re sampling, lastly retouching detection.

B. Compression based method:

The change of a forged image with the end goal of compression and different applications can make forgery detection an exceptionally difficult errand. JPEG picture pressure, for instance, is appeared to make falsification recognition extremely troublesome. In any case, in crime scene investigation examination, a few properties of JPEG compression are abused recognize the follows left by altering. These procedures can themselves be assembled into JPEG quantization based [2], double JPEG compression based [3].

C. Camera based method:

The image acquisition process in an advanced camera framework includes distinctive handling stages. In the first place, the light enters the camera lens then goes to the sensors through Color Filter Array (CFA). The sensor contains a cluster of photo detectors that catch occurrence light and change over it into voltages took after by the Analog-to-Digital (A/D) change stage. Today advanced cameras depend for the most part on Integral Metal-Oxide Semiconductor (CMOS) innovation with couple of producers as yet utilizing the conventional Charged Coupled Device (CCD) innovation. To catch color images from these sensors, CFA is utilized. The sensors catch one only color and the rest of the hues are assessed utilizing additions (demosaicing). The connections presented in the addition step can be utilized as a part of altering discovery. Before the final stockpiling, the picture quality is enhanced utilizing different upgrade procedures like Gamma revision and white parity. The curios presented in the distinctive phases of the picture creation procedure are abused to recognize hints of altering. Chromatic abnormality[4],camera source recognizable as clue, shading channel cluster, demosaicing relics , furthermore, sensor noise imperfections can help in estimation of various camera artifacts.

D. Physics based method:

Neutral photos are typically taken under various lighting conditions. In this way, the lighting of a produced locale may not coordinate the first in joining operations (where two or more pictures are utilized to make a fashioned picture). In material science based procedures, the irregularities in light source between particular items in the scene are utilized to uncover the clues related to tampering [5]. Johnson et al. [5] proposed an altering discovery strategy that uses the course of occurrence light and figured a low-dimensional descriptor of the lighting environment in the picture plane. The algorithm estimates the brightening heading from the force circulation along physically clarified object limits of homogeneous shading. Kee et al. [6] extended this way to deal with misusing known 3-D surface geometry

2. IMAGE TEMPERING DETECTION TECHNIQUES

Image tampering is a computerized craftsmanship which needs comprehension of image properties and great visual inventiveness. One tempers pictures for different reasons either to appreciate fun of advanced works making unimaginable photographs or to deliver false proof. Regardless of whatever the reason for act may be, the counterfeiter ought to utilize a solitary or a blend arrangement of picture preparing operations. Many techniques are developed for the verification of authenticity of images. These techniques can be described as intrusive (active) and nonintrusive (blind or passive).

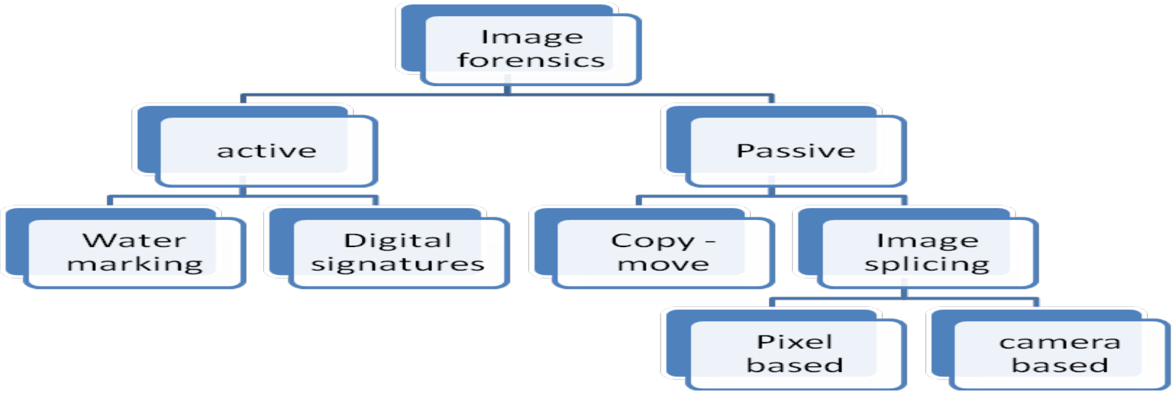


Figure1: Tempering detection techniques

2.1 Active approach:

In active approach some kind of pre processing is required on digital image at the time of creation of image such as watermarking, digital signatures [7]. In recent time various schemes are proposed for providing the security to image which is similar to the concept of watermarking such as hash function on image, message authentication code and image checksum.

2.1.1Watermarking:

In watermarking the digital information is hidden for security purpose by embedding security structure into the image. It is typically used to verify the authenticity and integrity of the digital information or to verify the identity of its owners. Watermarking uses the steganographic techniques to hide the digital information.

2.1.2 Digital signatures:

Digital signature is another method of active approach which employ embedding of signature onto the digital image for the security purposes. We can detect the Image is tampered, if special information cannot be extracted from that obtained image. Recently biometric acceptance is much into demand for verification of signatures.

2.2 Passive approach:

Passive approach is a great challenging task in the image processing techniques. In passive approach the image undergoes through various steps of digital image processing such as preprocessing, feature extraction, feature selection, feature matching, verification and finally localization of tempered region as there is not any particular method which can treat all the cases of image forgery[7].

2.2.1 Copy move forgery detection techniques:

The diverse parts are copied and moved to the same image in duplicate move fraud as shown in figure 2, thus solid connection exists between these which can be utilized as a proof for forgery identification. Be that as it may, the primary test is to find proficient elements and matching algorithms for finding related portions. In these techniques, to start with, trademark elements are computed either by isolating the picture into covering pieces or computing neighborhood key focuses for the entire picture. The positions of every piece (or key point) are additionally put away in the element vector. At that point, the element coordinating is performed to discover comparable components inside the same picture. The imitation confinement is finished by showing the coordinated pieces (or key focuses) in colors comparing.

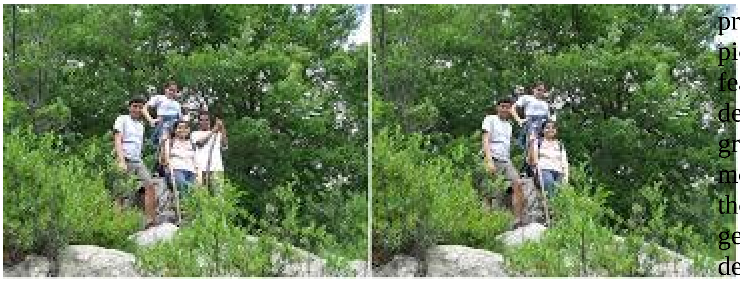
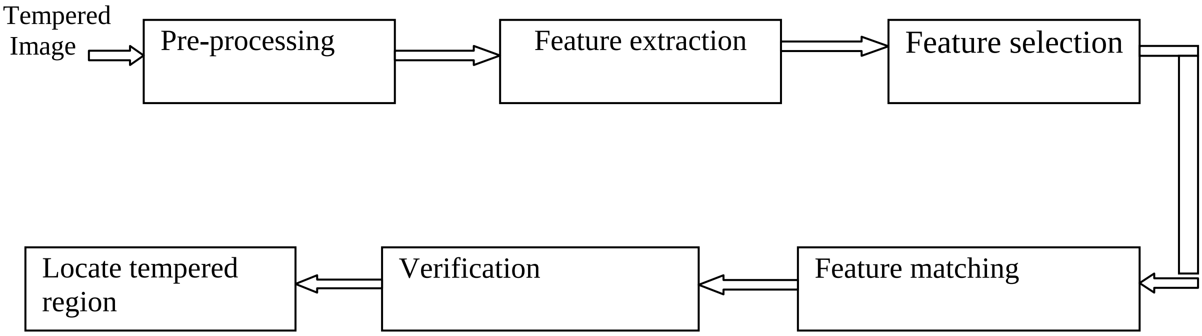


Figure 2- example of copy move tempering

One of the most copy move forgery detection algorithms is proposed by Rajeev Rajkumar et al. [8], in light of isolating the picture into settled size covering squares and put away as 1-D feature vector. An imperative was made in connection to the decision of square size, as it ought to be not exactly the span of greatest copy move block section. Next, a movement vector methodology was utilized for feature vector and hinders with the same movement were announced as tempered regions. This general system is regular among most copy move temper detection strategies and the primary steps are portrayed as takes after:



Block diagram for copy move tempering detection algorithm

2.2.2 Image splicing detection techniques:

Image splicing is a glue up created by staying together photographic images as shown in figure 3. While the term photomontage was initially used to allude a work of art or demonstration of making composite photo can be followed back to the season of camera invention[9]. The errand of image splicing detection among bona fide and tempered image is a case of binary classification .It begins with the preprocessing stage which is generally color to grey-scale transformation took after by the element extraction stage. Diverse sorts of elements are separated from credible and altered pictures for a Amerini et al. [10] proposed an image splicing detection technique in view of irregularity in the movement blur.

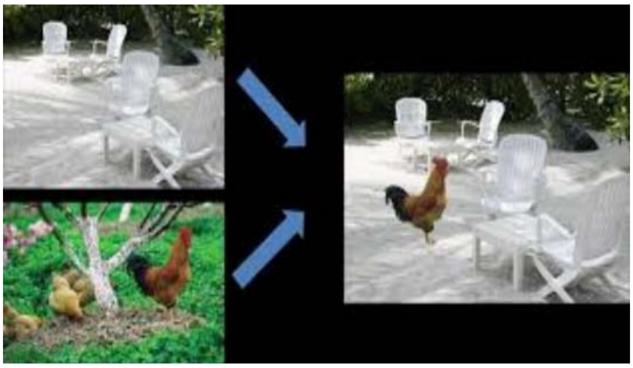


Figure 3-An example of image splicing tempering technique

2.2.3 Image retouching technique:

Image retouching is a typical strategy utilized as a part of the media industry. It is seen as an adequate and at times an attractive strategy for changing images. It doesn't result in any critical change in a picture rather it accentuates (or decreases) given dataset. The component extraction stage is basic and the characterization execution relies on upon the choice of best components for the issue under investigation. The removed components are used to prepare a classifier and the prepared model is utilized to characterize the genuine and altered pictures. At last, in the post-preparing stage, the altered areas are localized.

Amid the image splicing process, for the instance of out of focus blurred images, the altered regions are falsely blurred to coordinate the blur of the actual image. The irregularity is left in the blur and can be utilized as a proof of altering. Kakar some attractive (or undesirable) components of the picture (see Fig. 4). It is a well known procedure utilized with magazine photographs and as a part of motion pictures. The picture is upgraded to make it more appealing and here and there a few areas are changed, (for example, evacuating wrinkles) to acquire the last photograph, while such sort of control is not seen as producing, we incorporate it here as it includes altering the first image[11].

Since the most recent decade, electronic and print media as very much utilized picture correcting devices like Adobe Photoshop, and many other editing tools, to make the photographs more regular and alluring. Retouched photographs are utilized to make a honorable representation of genuine excellence. While the writing has diverse methodologies in identifying the inventiveness of a picture what's more, are sorted by location of upgrade operation.

Table 1: Image tempering techniques and detection techniques

Image temper technique	Tools used	Temper detection techniques
Copy-move (exhaustive search ,block matching)	Copy , move (using DCT or PCA)	Spatial domain method ,transform based methods and feature matching methods
Image splicing	Copy ,resize ,move ,analysis, feature extraction, feature mapping and verification	Pixel based splicing algorithms
Image retouching	Image correcting ,blurring image editing	Image inpainting detection algorithms

3. RELATED WORK

Detection of forgery in digital image can be divided into two categories: active (intrusive) and passive (non-intrusive or blind).Judith A. Redi et al.[12] in their booklet "Digital image forensics: a booklet for beginners" presented that Digital images using image editing tools the digital images can be easily Modified .Tampering Detection Operation is an important field in modern multimedia environment. Passive digital image tampering detection aims at proving the authenticity of digital images without having any prior knowledge on original image. In this paper various methods are explained in three levels, that is low level, middle level, and high level in semantic sense.

In a copy-move forgery which is an passive approach, a part of the digital image is copied and pasted to another part of the same digital image which is done with the intension to hide an object. The copied areas are easily blend with background and cannot be detected easily with human eye. There are many methods developed for detection of copy move forgery. Swapnil et al[13]**,** in their paper " Copy –Move Attack Forgery Detection by using SIFT" explains the various SIFT based Image Forgery detection techniques . In this author uses advance algorithms which are based on SIFT to detect such forgery. In this paper, to input image SIFT transform is applied to reduce dimensional representation. Irene Amerini et al.[14] In their paper **"**A SIFT-based forensics method for copy-move attack detection and transformation recovery**"** main attention is paid on geometric transfor
mations are used to adjust the image patch to the new content. For this type of tempering the scale invariant feature transformation SIFT is proposed .This technique is useful to detect copy-move attack and also to recover the geometric transformation applied to perform forgery .This method is suitable for multiple cloning too. Chieng-shien lin et al.[15] proposed a scheme which improves previous cluster expanding block scheme to clustering by mean and variance for reducing the computation time. The over head of pre- processing is extra load which takes more time than previous cluster expanding block scheme but still the computation time is still improved by 10%. Another method is proposed by Fredrich et al[16] extracted the DCT coefficients then sorted them lexicographically scheme to reduce the complexity of comparisons. Finally the copied regions are detected based on approximate block matching. Panali Mukherjee et al[17] explains some techniques of copy move based on discrete cosine transformation(DCT) and Discrete wavelet transformation(DWT).There are various techniques to counter the copy move attack based on exhaustive search and block matching approach .In this paper they have analyzed the both techniques have their pros and cons .

In image splicing one part of an image is copied and pasted on the part of another image. The copied part is blurred or other techniques such as rotation, scaling etc are applied on it so that forgery cannot be recognized by human eye. There are many methods that are developed to detect this forgery. Manu VT and BM Mehtre[18] in their paper "Visual artifacts based image splicing detection in uncompressed images**"** proposed a method of image splicing based on visual artifacts in uncompressed images. Then results were produced and the accuracy of this proposed method is 88.15%. This is new method to detect tempering on images based on non reference image quality metrices. This was done by quantifying the artifacts in the images that might have occurred during the tempering of original. Khosro Bahrami and Alex C. Kot in their method[19] first the colored image is converted into gray scale image then it is divided into blocks. After the block-based partitioning is done a local blur type detection feature is extracted from the estimated local blur kernels. These local features are incorporated for classification of image blocks into out of focus blur or motion blur. Finally a fine splicing localization is applied to increase the precision of regions boundary. The experimental results in the partial blur type detection show that the proposed method classifies the out of focus blur and motion blur types successfully.

Another method is proposed by E- Sayed M.EI-Alfy, Muhammad Ali Qureshi[20] in their paper "combining spatial and DCT based Markov features for enhanced blind detection of image splicing" proposed the new method for blind detection of image splicing. It extracts and combines Markov features in spatial and Discrete Cosine Transform domains to detect the artifacts introduced by the tampering operation. To reduce the computational complexity due to high dimensionality, Principal Component Analysis is used to select the most relevant features. Then, an optimized support vector machine with radial-basis function kernel is built to classify the image as being tampered or authentic. M. H. Fahime Hakimi [21]proposed another method for detection of image splicing. Firstly the algorithm converts input RGB image into YCbCr color channel, afterwards chrominance component is divided into non-overlapping blocks. Secondly Local Binary Pattern (LBP) operator is performed, and wavelet transform is applied in all blocks. Finally, Principal Component Analysis (PCA) is used for all blocks and the output is fed to Support Vector Machine (SVM) classifier as features. Parvin kakar and N.Sudha[22] in their paper **"**Exposing digital image forgeries by detecting discrepancies in motion blur" present a novel method of detecting splicing in images, using discrepancies in motion blur. They use motion blur estimation through image gradients in order to detect inconsistencies between the spliced region and the rest of the image. They also develop a new measure to assist in inconsistent region segmentation in images that contain small amounts of motion blur. Experimental results show that their technique provides good segmentation of regions with inconsistent motion blur.

Table 2: Comparison of methods forgery detection techniques

Sr. no	Title	Author contribution/ year of publication	Tempering detection type and Method used	Accuracy /Research gap
1.	An efficiency enhanced cluster expanding block algorithm for copy-move forgery detection	Chieng-shien lin et al.[15](2015)	Copy-move forgery detection(improves cluster expanding scheme by using mean and variance to reduce computation time)	87% accurate(Computation time is still required more further schemes can be applied to reduce the computation time)
2.	Copy –Move Attack Forgery Detection by using SIFT	.Swapnil et al[13]**(**2004)	SIFT(scale invariant feature transformation) is used to recover the geometric transformation applied to perform forgery	88% Accurate(method work for the single cloning only further this method can be extended to work for multiple cloning too)
3.	Visual artifacts based image splicing detection in uncompressed images	Manu VT and BM Mehtre[18](2015)	Image splicing(based on visual artifacts in uncompressed images by quantifying the artifacts in images)	88.15% Accurate(proposed scheme can be applied on images with copy move forgery and also the method can be improved by using better classification techniques).
4.	Splicing localization based on blur type inconsistency	Khosro Bahrami and Alex C. Kot [19](2015)	Image splicing (partial blur type inconsistent method that classifies the out of focus blur and motion blur types	94.6% Accurate (method detects forgery in different blur types in image but not able to detect forgery in single blur type)
5.	Combining spatial and DCT based Markov features for enhanced blind detection of image splicing	E- Sayed M.EI-Alfy, Muhammad Ali Qureshi[20]**(**2015)	Image splicing(spatial domain and DCT based Markov features)	98.82% Accurate(More accuracy can be achieved by using less number of features as compared with the state-of the-art splicing detection

				methods tested on the same dataset).
6.	Image Splicing Forgery detection using local binary pattern and discrete transformation	M. H. Fahime Hakimi [21](2015)	Image splicing is detected by using LBP operator, PCA for feature extraction, SVM as classifier features)	95.13% Accurate (Computation time of this proposed scheme is large and can further be decreased by using more classification methods).
7.	Exposing digital image forgeries by detecting discrepancies in motion blur	Parvin kakar and N.Sudha[22](2015)	Image splicing (discrepancies in motion blur are used)	96.15% Accurate (This method is suitable to detect the discrepancies in motion blur but not suitable for out of focus blur and accuracy can also be increased by using more schemes).

3.1 Algorithm analysis for table and its discussion:

A lot of work has been carried out to detect the image forgery. Many algorithms have been developed to detect the various forgeries. Chieng-shien lin et al.[15] proposed a scheme for copy move forgery which improves previous cluster expanding block scheme to clustering by mean and variance for reducing the computation time. This method is 87% accurate and Computation time is still required more further schemes can be applied to reduce the computation time. Swapnil et al[13]**,** in their paper " Copy –Move Attack Forgery Detection by using SIFT" explains the various SIFT based Image Forgery detection techniques . In this author uses advance algorithms which are based on SIFT to detect such forgery. In this paper, to input image SIFT transform is applied to reduce dimensional representation. This method is 88% Accurate and this method work for the single cloning only further this method can be extended to work for multiple cloning too. Khosro Bahrami and Alex C. Kot

Proposed an method for Image splicing (partial blur type inconsistent method that classifies the out of focus blur and motion blur types). Further method can be improved by making it applicable for blur consistency. E- Sayed M.EI-Alfy, Muhammad Ali Qureshi proposed the new method for blind detection of image splicing. It extracts and combines Markov features in spatial and Discrete Cosine Transform domains to detect the artifacts introduced by the tampering operation. This method is 98.82% Accurate. More accuracy can be achieved by using less number of features as compared with the state-of the-art splicing detection methods tested on the same dataset. M. H. Fahime Hakimi [21]proposed another method for detection of image splicing. This method is 95.13% Accurate and Computation time of this proposed scheme is large and can further be decreased by using more classification methods. Parvin kakar and N.Sudha present a novel method of detecting splicing in images, using discrepancies in motion blur. Accuracy of this method is 96.15% This method is suitable to detect the discrepancies in motion blur but not suitable for out of focus blur and accuracy can also be increased by using more schemes.

IV. CONCLUSION

The techniques that we reviewed in this survey represent important results for multimedia security, especially considering that the problems they tackle were previously (almost) unexplored. In this paper the various forgery detection techniques are discussed, their detection methods and algorithms are also discussed. In this paper comparison of various detection techniques such as copy move and image splicing and their further methods is also given. Our extended overview of image forgery detection techniques shows that this area of research is still in its flourishing stage, and holds a huge potential for future R&D applications.

Despite these achievements still there are challenges for digital image forensics. Algorithms explained in this paper still have some anomalies. Further research can be done to remove these various anomalies. As we are working on splicing localization based on blur type inconsistency. Future works will deal with the drawbacks presented in proposition when the background regions and the spliced regions have consistent blurring kernels. Computation time can also be decreased and accuracy can also be improved

REFERENCES

[1] M. Ali and M. Deriche, “Signal : Processing Image Communication A bibliography of pixel-based blind image forgery detection techniques,” *Signal Process. Image Com. mun.*, vol. 39, pp. 46–74, 2015.

[2] C. Alex and HBlurred, “Blurred Image Splicing Localization by Exposing Blur Type Inconsistency,”.IEEE transactions on information forensics and security10(5):999-1009.may 2015.

[3] T. B. Member, A. Piva, and S. Member, “Politecnico di Torino Porto Institutional Repository Detection of Non-Aligned Double JPEG Compression Based on Integer Periodicity Maps,” 2013.

[4] “IMAGE TAMPER DETECTION BASED ON DEMOSAICING ARTIFACTS Ahmet Emir Dirik Polytechnic Institute of NYU Electrical & Computer Engineering Dept . Nasir Memon Polytechnic Institute of NYU Computer Science & Engineering Dept .”Image processing(ICIP).2009 16th IEEE International conference.

[5] M. K. Johnson, S. Member, and H. Farid, “Exposing Digital Forgeries in Complex Lighting Environments,”IEEE transations on information forensics and security,2007, pp. 1–17.

[6] J. Fridrich, D. Soukal, and J. Lukáš, “Detection of Copy-Move Forgery in Digital Images.” Proc. ACM Workshop on Multimedia and Security, Orlando volume 139 feb.2011.

[7] C. S. Gupta, M. T. Scholar, F. Detection, and C. Forgery, “‘ A Review on Splicing Image Forgery Detection Techniques ,’” vol. 6, no. 2, pp. 262–271, 2016.

[8] R. Rajkumar, “Digital Image forgery detection using SIFT feature,” no. c, 2015.IEEE

[9] W. Wang, F. Zeng, and H. Yuan, “Identifying Image Composites by Detecting Discrepancies in Defocus and Motion Blur,” vol. 8, no. 11, pp. 2789–2794, 2013.

[10] I. Amerini, R. Becarelli, R. Caldelli, and A. Del Mastio, “Splicing Forgeries Localization through the Use of First Digit Features,” pp. 143–148, 2014.

[11] K. Shortcuts, O. Files, N. Color, T. C. Tools, I. Healing, R. Reduction, and C. K. Shortcuts, “Photoshop CS for Restoration and Retouching,” pp. 1–44, 2003.

[12] J. A. Redi, “Digital Image Forensics a booklet for beginners,” vol. 33, no. 0, pp. 1–40.

[13] Mohasin N.shaikh R. Article, “Review Article A SIFT FOR COPY-MOVE ATTACK DETECTION & Transformation recovery.”International journal of advanced engineering research and studies E-ISSN2249- 8974

[14] I. Amerini, M. Barni, R. Caldelli, and A. Costanzo, “Counter-forensics of SIFT-based copy-move detection by means of keypoint classification,” pp. 1–17, 2013.

[15] C. Lin, C. Chen, and Y. Chang, “An Efficiency Enhanced Cluster Expanding Block Algorithm for Copy-Move Forgery Detection,” pp. 13–16

[16] N. D. Wandji, S. Xingming, and M. F. Kue, “Detection of copy-move forgery in digital images based on DCT.”International journal of computer science issues 10,1-8(2013).

[17] P. Mukherjee and S. Mitra, “A Review on Copy-Move Forgery Detection Techniques Based on DCT and DWT,” vol. 4, no. 3, pp. 702–708, 2015.

[18] I. I. Confe, C. Graphics, C. Security, B. Technology, and C. Science, “Image Splicing Detection in Un ncompressed Images,” no. June 1971, pp. 145–150, 2015.

[19] K. Bahrami and A. C. Kot, “Image Splicing Localization Based on Blur Type Inconsistency,” pp. 1042–1045, 2015.

[20] E. M. E. M. A. Qureshi, “Combining spatial and DCT based Markov features for enhanced blind detection of image splicing,” Springer-verlag london 2014.

[21] F. Hakimi, “Image splicing forgery detection using local binary pattern and discrete wavelet transform Image Splicing Forgery Detection using Local Binary Pattern and Discrete Wavelet Transform,” no. November 2015, 2016.

[22] W. Exposing, P. Kakar, S. Member, N. Sudha, S. Member, W. Ser, and S. Member, “Exposing Digital Image Forgeries by Detecting Discrepancies in Motion Blur,”IEEE Transactions on multimedia,13(3),443-452 2011.