International Journal on Emerging Technologies (Special Issue on *RTIESTM-2016*) **7**(1): 170-174(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Forgery Detection Techniques: A Review

Lovepreet Kaur*, Raghuwinder Kaur** and Simran Kaur**
**Department of CSE & IT, BBSBEC, Faridkot, Punjab, INDIA*
***Assistant Professor, Department of EE, Engg. , A.I.E.T, Faridkot, Punjab, INDIA*
****Assistant Professor, Department of ECE, Engg. , A.I.E.T, Faridkot, Punjab, INDIA*

(Corresponding author: Lovepreet Kaur)
(Received 17 November, 2015 Accepted 19 December, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In ancient times, the images were used very rarely and the possibility of forgery in images was also rare. But now days, Images have gained a vital importance in our daily life as the use of images is increasing day by day for the purpose of communication and for other important fields. With the increase in usage of images, forgery in images has also been increased because of the presence of effective photo editing software's that helps in creating forged image very easily without any expert knowledge. So there is a need to detect forgery in images i.e. to analyze whether the image is real or fake. Such a problem is challenging because images are of many kinds and to detect forgery they work accordingly for e.g. for dissimilar images different techniques are required for detection based on type of image. By type of image here means some images contain human skin and some do not. Various techniques have been developed to detect forgery in images. The purpose of this review paper is to categorize and evaluate the forgery detection existing techniques. We also conclude some improvements that are possible for future research.

Keywords: Digital images, Forgery detection techniques.

I. INTRODUCTION

A picture is worth more than thousand words but it may have number of perceptions. Images are important in many fields such as e-commerce, forensics, Industrial photography etc. Due to rapid advancement in digital technology and availability of powerful image manipulation tools, it becomes very easy to modify the digital images at very low cost. Therefore, no one can take the authenticity of digital images for granted. This generates a great demand for detection tools that are transparent to tempering and can reveal whether an image is novel or forged. Detecting the forgeries in images has become a challenging task, involving a variety of issues.

Digital image forensics is an emerging field that analyses images to determine whether they are original or altered by forgeries. Substantial amount of work is carried out in the field of forgery detection. Digital image forensics can be classified into active forensics and passive forensics. In active forensics, a watermark or signature is created at the time of recording the information, which would limit their application in practice. There are millions of digital images in internet with digital signature or watermark. In such cases, active approach cannot be used to check the authenticity of images.

In contrast to these approaches, passive technology for image forensics works in the absence of any watermark or signature. This technology is popular as it does not require any prior information about the images. Many existing techniques are used to detect the traces of tempering. Fig. 1 shows classi- fication of forgery detection techniques.

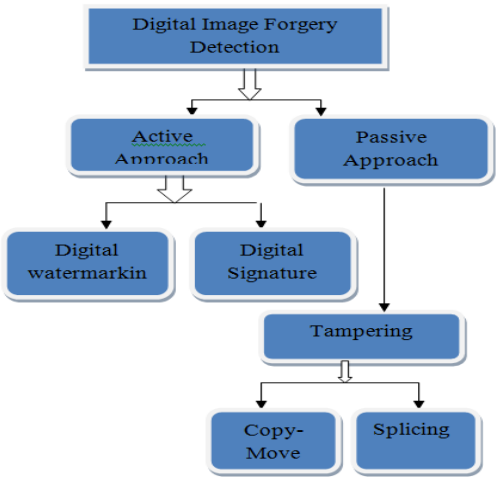

Fig. 1. Classification of Forgery Detection Techniques.

II. COPY MOVE OR CLONING

This is the most common type of forgery and is also known as cloning. In copy-move forgery, a part of any image region is cloned and pasted to distinct region of the same image in order to hide the details of the certain image. Recently, copy-move forgery detection has become a very active research area.

Fig. 2. Shows the copy-move forgery.

First attempt in identifying tampered areas was investigated by J. Fridrich *et al.* (2003) [3]. The author proposed a method of detecting copy-move forgery using discrete cosine transform (DCT) of overlapping blocks. .

W. Luo *et al.* (2006) [4] presented a copy-move forgery detection and localization method based on dividing an image into small overlapped blocks and finally identifying possible duplicated regions using intensity based characteristics features..

H. Huang *et al.* (2008) [5] proposed a new approach based on scale invariant features transform (SIFT) features which are stable with respect to changes in illumination, rotation and scaling. SIFT is used to detect the duplicated regions in the image.

S. Bayram *et al.* (2009)[6] used Fourier-Mellin transform (FMT) features, which are invariant to scale and rotation in order to detect copy-move forgery.

M. Bashar *et al.* (2010)[7] proposed a region duplication approach that adopts two robust features based on DWT and kernel principal component analysis (KPCA).

G. Mohammad *et al.* (2011)[8] used a dyadic wavelet transform (DYWT) to detect passive copy-move forgery detection.

P. Xunyu and L. Siwei (2011) [9] proposed a region duplication method by estimating the transform between matched SIFT keypoints that is robust to distortions based on image feature matching.

P. kakar and N. Sudha (2012[10]) described a new approach based on transform invariant features for detecting copy-paste forgeries with possible post-processing based on the MPEG-7 image signature tools.

M. AlSawadi et al. (2013)[11] proposed a method that utilizes three color components and LBP to find texture patterns. The neighborhood clustering technique is also introduced to reduce the false positives. In the experiments, the proposed method outperforms two other contemporary methods in different types of forgery cases. In a future work, the work will be extended to detect forged images where various types of post-processing are applied on the pasted part.

S. Debbarma et al. (2014) [12] in this paper, keypoints based forgery detection is analyzed using SIFT and SURF algorithm.

C.M. Hsu *et al.* (2015)[13] proposed an effective method for detecting duplicated regions based on the histogram of Gabor magnitude. The experimental results demonstrate that the proposed algorithm robust against actions aimed at concealing forgery, including slight image rotation, JPEG compression, blurring, brightness adjustment; furthermore, the computational complexity involved is low. This study, therefore, makes a valuable contribution to the field of multimedia forensics.

S. Wenchang *et al.* (2016)[14] proposes a novel approach, CMFD-PSO, to detecting CMF in digital images. This paper puts forward the concept of applying the PSO algorithm to CMF detection and integrates the PSO algorithm into SIFT – based framework to perform CMF detection. It devises rules to automatically determine customized parameter values for given images that are to be detected.

Table 1: Comparison of copy-move forgery detection methods.

Authors	Extracted Features	Pros/cons
Fridrich et al.(2003)	Detecting copy-move forgery using DCT of overlapped blocks.	Avoid computational burden. Block matching algorithm increases complexity.
Luo et al.(2006)	Identifying possible duplicated regions using intensity based characteristic features.	Lower computational complexity and more robust against stronger attacks.

Authors	Extracted Features	Pros/cons
Huang et al.(2008)	Copy-move forgery detection using SIFT descriptors.	Good recall rates. SIFT operator is quite slow. Generally does not work well with lightning changes and blur.
Bayram et al.(2009)	Fourier Mellin transform and lexical sorting is used for detection.	Robust against JPEG compression, Rotation and scaling. Increases complexity.
Muhammad et al.(2011)	Dyadic Wavelet Transform	A simplest approach thersholding classification is used for detection. Threshold selection is not always straight forward.
Alsawadi et al. (2013)	Linear binary pattern.	Provides best accuracy more than 95%. Performance will degrades when the pasted party undergoes rotation and scaling.
Debbrama et al. (2014)	SIFT and SURF is used for the purpose of feature extraction.	SIFT provides more accuracy as compared SURF. In this paper there is only one drawback that is the lack of keypoint detection in smooth or plain areas in the image.
Hsu et al. (2015)	Statistical features extracted from the Histogram of Oriented Gabor Magnitude (HOGM) blocks, of overlapping	Histogram of Oriented Gabor Magnitude is an effective method for detecting duplicated regions. In this Block matching provides best accuracy. Computational complexity associated with block matching.
Wenchang et al. (2016)	CMF detection with Particle Swarm optimization (CMFD-PSO)	CMFD-PSO can achieve better results than EPV-SIFT. In this forgery detection results depends on the selection of parameter values. So sometimes duplicated regions cannot be detected.

III. IMAGE SPLICING

Image splicing is another common form of image manipulation. This technology involves composites of two or more images which are combined to create a doctored image. Multiple images are merged into single image to create a composite image. An example of such type of forgery is shown in fig 3.

Fig. 3. Shows Image splicing**.**

There exist many technologies that are very effective in detecting composite images. Some of these are follows:

D. Fu et al. (2006)[15] suggested a method that uses Hilbert-Huang transform (HHT) to obtain the features for classification.

Z. Zhang et al. (2008)[16] developed a method that employed moment features extracted from the multi size block discrete cosine transform and image quality metrics which are sensitive to spliced images.

L. Qingzhang et al. (2009)[17] described a technique based on extraction of neighboring features of the DCT coefficients, SVM classifier is applied for detection of forged images.

X. Zhao et al. (2010)[18] proposed a method based on chroma space. In this Gray level run length texture feature is used. RLRN were used as unique features for detection of image splicing and SVM was used as classifier.

X. Wu *et al.* (2011)[19] developed a method that uses illuminant color inconsistency .Given color image is divided into many overlapping blocks. Based on the content of blocks a classifier is used to select illuminant estimation algorithm.

Z. He *et al*. (2012)[20] In this paper improvement was obtained and proposed a markov based approach. Markov features are expanded to capture not only the intra-block but also the inter-block correlation between block DCT coefficients. To manage a large number of features, SVM-REF is utilized and SVM is used for classification.

Z. Moghaddasi *et al*. (2014)[21] proposed a method based on singular value decomposition (SVD) feature extraction method applied in steganalysis. SVD-based features are merged with discrete cosine transform (DCT) for image splicing detection. Support vector machine is used to distinguish between authentic and spliced images.

Z. Moghaddasi et al. (2015)[22] proposed a SVD-based image splicing detection method and tested in different spatial and frequency domains (DCT, DWT and DFT). The result describes that SVD-DCT has the best detection rate compared to SVD, SVD-DWT, and SVD-DFT with only 25 dimensions.

Table 2: Comparison of image-splicing forgery detection methods.

Authors	Extracted features	Pros/cons
Fu et al.(2006)	Hilbert-Huang transform and wavelet decomposition based features.	In this paper SVM classifier provides 70% accuracy. SVM has good generalization performance but they can be slow in test phase.
Zhang et al.(2008)	Utilizes moment features extracted from the multi size block discrete cosine transform (MBDCT) and Image quality metrices (IQMs).	In this paper measures statistical difference between spliced and original image. IQMs show the assessment of visual quality among the considered IQMs.
Zhao et al.(2010)	Grey level run length number vectors.	RLRN (Run – Length Run-Number) features extracted from chroma channel provide much better performance than that extracted R, G, B and luminance channels.
Moghaddasi et al. (2014)	SVD-based features are merged with DCT	(SVD+SVD-DCT) has the best detection rate compared to the individual methods SVD and SVD-DCT.
Moghaddasi et al.(2015)	A low dimensional SVD based feature extraction method proposed and test in different spatial and frequency domain (DCT,DWT)	SVD-DCT has the best detection rate. SVD-DWT and SVD-DFT does not provide best results. Future Research is required to modify the SVD to improve the performance.

IV. CONCLUSION

Forgery is an illegal change in an image or documents that can be done easily with the help of various editing tools at minimal cost. So the detection of tampering in digital images is the interesting topic in today's research. Over the past few years many forgery detection techniques have been proposed. In this paper a survey regarding types of forgeries and forgery detection techniques and the comparison shows the advantages and disadvantages of different methods and techniques.

REFERENCES

1. G.K. Birajdar and V.H. Mankar, "Digital image forgery detection using passive techniques: A survey", vol. 10, (2013), pp. 226-245.
2. S. Mushtaq and A.H Mir "Digital image forgeries and passive image authentication Techniques: A survey", International Journal of advanced science and Technology, Vol.73 (2014), pp.15-32.
3. J. Fridrich, D. Soukal, J. Lukas "Detection of copy move forgery in digital images", Proc. of digital forensic research workshop, (2003), pp. 55-61.

4. W. Luo, J. Huang, G. Qiu, "Robust detection of region-duplication Forgery in digital image", Proc. of the 18th international conference on pattern recognition,(2006), pp. 746-9.
5. H. Huang, W. Guo, Y. Zhang, "detection of Copy-Move Forgery in digital images using SIFT algorithm", In: Proc. of the 2008 IEEE Pacific- asia workshop on computational intelligence and industrial application, (2008), pp. 272-6
6. S. Bayram, H. Taha, and N. Memon, "An efficient and robust method for detecting copy-move forgery" In: Proc. of 2009 IEEE International Conference on acoustics, speech and signal processing 2009, pp. 1053-6.
7. M. Bashar, K. Noda, N. Ohnishi, K. Mori, "Exploring duplicate regions in natural images", IEEE Trans image process 2010, pp. 1-40.
8. G. Muhammad, M. Hussain, K. Khawaji, G. Bebis, "Blind copy-move forgery detection using dyadic uncedimated wavelet transform", In: Proc. of 17th international conference on digital signal processing 2011, pp. 1-6.
9. P. Xunyu, L. Siwei, "Region duplication using image feature matching", IEEE Trans Inf Forensics Security, 2011;5(4):857-67.
10. P. Kakkar, N. Sudha, "Exposing Postprocessed copy-paste forgery through transform- Invariant features ", IEEE Trans. Inf Forensics security 2012;7(3): 1018-28.
11. M. Alsawadi, G. Muhammad, M. Hussain, G. Bebis, "Copy-move forgery detection using Local Binary Pattern and neighbourhood clustering, (2013), pp. 249-254.
12. S. Debbarma, A. B. Singh, K. M. Singh Informatics, "Keypoints based copy-move forgery detection of digital images," Electronics & Vision (ICIEV), 2014 International Conference on (2014), pp. 1-5.
13. C-M. Hsu. J-C. Lee and W-K. Chen "An efficient detection algorithm for copy-move forgery", 10th Asia Joint Conference on Information Security.(2015), pp. 33-36.
14. S. Wenchang; Z. Fei; Q. Bo; L. Bin, "Improving image copy-move forgery detection with particle swarm optimization techniques", China communications, IEEE journals and magazines. (2016)Vol. 13, pp. 139-149.
15. D. Fu, Y.Shi and W. Su, "Detection of Image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition", proc. of international workshop on digital watermarking,(2006), pp. 177-87.
16. Z. Zhang, J. Kang and Y. Ren, "An effective algorithm of image splicing detection", Proc. International conference on computer science and software engineering, (2008), pp.1035-9.
17. L. Qingzhong and H. Andrew, "A new aaproach for JPEG resizes and image splicing detection", Proc. ACM multimedia and security workshop, (2009), pp. 43-8.
18. X. Zhao, J. Li, S. Li and S. Wang, "Detecting digital image splicing in chroma spaces", Proc. International workshop on digital watermarking, (2010), pp. 12-22.
19. X. Wu and Z. Fang, "Image Splicing Detection Using Illuminant Color Inconsistency",International conference on Multimedia Information Networking and Security (MINES),(2011),pp. 600-603.
20. Z. He, W. Lu, W. Sun and J. Huang, " Digital image splicing detection based on Markov features in DCT and DWT domain ",Pattern Recognition, vol. 45, (2012), pp. 4292-4299.
21. Z. Moghaddasi, H. A. Jalab, R.M. Noor,"SVD-Imagesplicing detection", International conference on Information Technology and multimedia (ICIMU), (2014), pp. 27-30.
22. Z. Moghaddasi, H. A. Jalab, R.M. Noor, "A comparison study on SVD-based features in different transform for image splicing detection", IEEE International conference, (2015), pp. 13-14.