Passive Techniques of Digital Image Forgery Detection: Developments and Challenges

Chapter *in* Lecture Notes in Electrical Engineering · January 2018

DOI: 10.1007/978-981-10-4765-7_29

2 authors:

Santoshini Panda
Fakir Mohan University
3 PUBLICATIONS **36** CITATIONS
SEE PROFILE

Minati Mishra
Fakir Mohan University
51 PUBLICATIONS **308** CITATIONS
SEE PROFILE

Passive Techniques of Digital Image Forgery Detection: Developments and Challenges

Santoshini Panda[1*], Minati Mishra[2]

[1,2]P. G. Department of Information & Communication Technology
Fakir Mohan University, Balasore, Odisha
[1]*santoshinipanda11@gmail.com*
[2]*minatiminu@gmail.com*

Abstract. Photographs and images play an important role in our life but, in this technology era, equipped with powerful, low cost and easy to use photo editing tools, people often forge photographs. This practice has posed a question mark on the trustworthiness of images. Because carefully edited and forged images are very hard to be distinguished from their genuine and original copies therefore, forgery detection and separation of the forged images from the innocent ones has become a challenging issue for image analysts. Image forgery detection procedures are generally classified into two broad categories; the active and the passive detection techniques. This paper presents a state of the art review of different passive forgery detection techniques those are proposed by different authors over time.

Keywords: Copy-move forgery, Cloning, Splicing, watermark.

1. Introduction

Today, photo editing has become a common practice among people because of the easy to use and freely available image editing tools. Though, all edited images are not forged but some of those are. When forged images are available in huge numbers, it is important to detect and separate the genuine copies from the forged lots. Image forgery detection methods are generally classified into two categories, the active detection methods and/ or the passive methods. The active methods are generally termed as authentication techniques and are based on digital signatures or watermarks. The major drawback of active image authentication is, for verification of the authenticity of an image, a watermark or a digital signature need to be embedded into an image at the time of capture or immediately after the image is captured [1]. Passive forgery detection is an alternative to active authentication which requires no active information available for the purpose of authentication. These techniques detect forgery analyzing the image statistics in the absence of watermarks as well as the original image for comparison.

1.1 Image Manipulation Techniques

Though all image manipulation or image editing procedures do not fall into the image forgery category still it is certain that all forged images undergo some sort of

manipulation. The corrective manipulations techniques or the image enhancement techniques such as contrast and brightness adjustments, noise reduction techniques etc may not be included into forgery categories unless otherwise the manipulations fake some facts or make some changes to the image contents so as to convey some misleading information to the viewers [2]. According to authors of [1], image manipulation techniques can be divided into two categories: content preserving and content altering. Each of these techniques is further divided into different categories as shown in figure 1. Authors of [2] argue that steganography can also be classified as an image manipulation technique as that alters the image content invisibly. The subsequent sections of the paper discuss various types of image forgery and different forgery detection techniques.

2. Types of Image Forgery

Image forgery is categorized into four types such as, copy-move/ cloning, splicing, retouching and morphing [3]. Copy-move or cloning is procedure where a piece of an image is copy- pasted into some area of the image itself to create the forgery whereas, splicing is another method in which parts of two or more images are stitched together to create the forged image. Retouching is achieved by adjusting color, sharpness, brightness, noise, contrast etc. Morphing is a procedure that transfers an image to a different one through seamless transition between two images [4]. In figure 2 shown are four images out of which the second image is a spliced image obtained from first image and the fourth is a clone of the third.

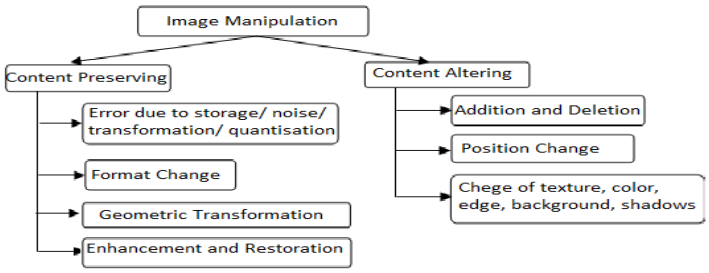

Fig 1. Types of Image Manipulation

Fig2. a, c: Original Images, b: Spliced Image, d: Cloned Image

3. Techniques of Digital Image Forgery Detection

Basically, the image forgery detection procedures fall into two classes. One is active detection and another is passive detection. Active detection requires in-built

digital signature and/or watermarking where as passive detection does not require any of these two. It works by analyzing the content and statistics of the image [5]. Image content based detection methods are further divided into the splicing detection and cloning detection methods. Cloning detection techniques are generally based on comparisons and matching. This falls into two major classes namely; the exhaustive search method and the overlapping block matching (OLBM) techniques. The exhaustive search method necessitates every possible part of an image to be compared with every other part of the image to detect a match. This gives rise to very high time complexity. Just like the exhaustive search method, simple OLBM method also can detect clones in a forged image, if the image is not subjected to further post processing such as intensity variation, noise contamination, compression etc. The time complexity of this method is less than the time complexity of the exhaustive search but, still remain as high as O (b^2B^2) where, b x b is the block size and B= (M-b+1) (N-b+1), M x N being the size of the image. In addition to the time complexity, the other dilemma with this method is choosing a right block size. If larger the blocks lead to smaller detection accuracy then smaller blocks are resulted with higher of false positive rates. The false positives are reduced by measuring the block shift and the search time can be improved using Vectorization and lexicographic sorting. Further reduction in dimension and improvement in search time is achieved by using DWT and SVD methods. DCT and PCA based methods provides robustness against intensity changes [6]. Coming to robust detection methods, the Luo, Huang and Qiu [7] suggested seven feature based detection technique provides robustness against JPEG compression, noise attacks and blurring but fails to detect intensity variant clones whereas, the four feature based intensity invariant detection model for JPEG compressed images (IIDMJPEG) proposed by Mishra and Adhikary detects intensity variant clones in JPEG compressed images as well as provides robustness against noise attack and blurring [8]. In figure 3 is presented a classification structure of various digital image forgery detection methods.

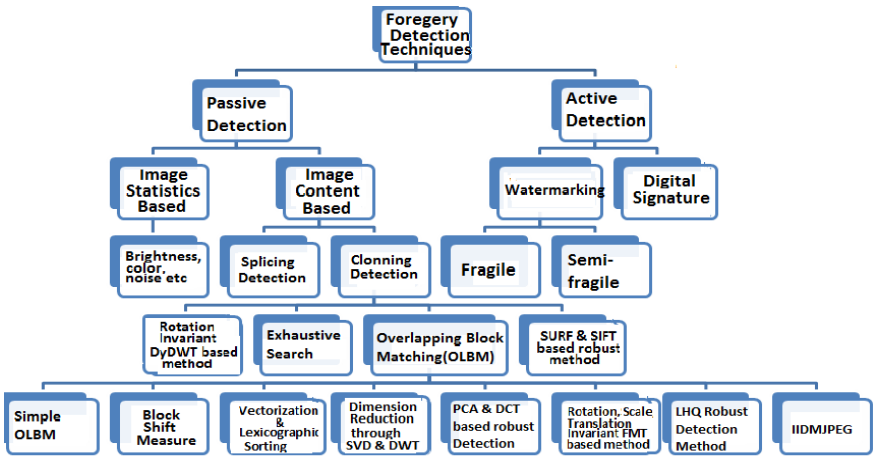

Fig3. Classification of Forgery Detection Techniques

3.1 Passive Detection: Non-robust Methods

The passive forgery detection techniques have evolved through several phases from the non-robust methods to highly robust techniques. The non-robust techniques fail to detect forgery when the forged image has been subjected to lossy compression, blurring, rotation, scaling noise attacks etc. On the other hand, the robust methods succeed in detecting forgeries even if the tampered image is subjected to one or more of these above mentioned post processing operations. This and the following sub-section present a brief record of the evolution of the passive detection methods.

Jessica Fridrich, David Soukal and Jan Lukas [9] give the idea about efficient detection method. First one is an exhaustive search method where an image and its circularly shifted version are compared for matched parts. Though this is an effective method the computational complexity of this method is very high it impractical for making it impossible for practical use even for medium-sized images. The second method suggested by the authors is the autocorrelation method where the forgery is localized by the peaks corresponding to the cloned and the original parts in an image. The Authors also suggested an overlapping block matching method that involves vectorization and lexicographic sorting. In this method, a square block of b×b pixels slides through an image one pixel at a time to give (M-B+1) (N-B+1) blocks. These blocks are matched to locate the clones. The steps of block based exact match are given in figure 4.

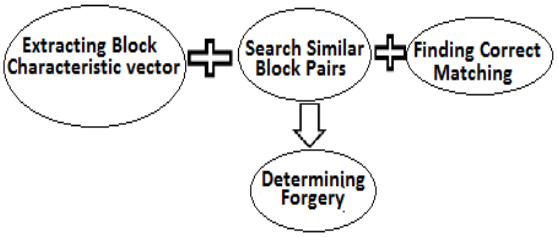

Fig 4. Forgery detection through block matching

S.Murali et al. [10] in their paper suggested a DCT based method for detecting forgery in a JPEG compressed image and a standard deviation based edge detection method. Zhouchen Lin [11] have proposed a robust method based on double quantization (DQ) effect and have applied a trained SVM (Support Vector machines) to take tampering decision. According to the authors DQ effect shows periodic peaks and valleys in the histogram of DCT coefficients and hence can be applied for tampering detection. Ruchita Singh, Ashish Oberoi and Nishi Goel [12] have used a DCT and SIFT based method for feature extraction and forgery detection. Zimba and Xingming [13] proposed two similar algorithms based on PCA and DWT. The method proposed by Popescu [14] divides an N×N image into $K=(N-b+1)^2$ overlapping. Each block is reshaped into b^2 long row vectors and inserted into a $K\times b^2$ feature matrix. To improve the time complexity, DWT is applied to the blocks and hence, the size of the feature vectors is reduced. They also proposed a method [15] based on principal component analysis and Eigen value decomposition (PCA-EVD) that reduces the dimension of the feature vectors and improves the computation time.

Babak Mahdian and Stanidlav Saic [16] proposed a blur invariant method that successfully detects clones even if the cloned regions are blurred and noisy. Zaho Junhong [17] presented an LLE (Locally Linear Embedding) - a non-liner dimension reduction technique that detects copy-move forgery as well as fused edges. Sam T. Roweis et al [18] have also used LLE for tamper localization. Ramandeep Kaur [19] has used Local binary pattern (LBP) - a texture descriptor for feature extraction and have used similarity criterion and Euclidean distance threshold for detection of clones.

3.2 Passive Detection: Robust Techniques

Jessica Fridrich, David Soukal and Jan Lukas [9] in their paper have also suggested a technique robust against JPEG compression along with the techniques discussed in the above sub-section. This method is same as that of the exact match with one difference that it considers of quantized DCT coefficients for comparison instead of the pixel representations for finding similarity.

N. Muhammad et al. in their paper [20] have proposed a dyadic Wavelet Transform (DyWT) and DWT based robust and improved forgery detection model. Wang X. et al. [21], in their paper, have suggested a DWT, DCT and Eigen vector based method that is invariant to JPEG compression and additive noise. In this method first DWT and DCT are applied to the image blocks and then the resulting coefficients are multiplied to form the Eigen vectors. Block match is calculated measuring the mean and variance of distances between Eigen values of Eigen vectors for forgery localization. Jing Zhang et al. [22] have combined phase correlation with DWT for their detection model. They have calculated spatial offset between copied and pasted region to compute the difference between the image and its shifted version. This method is claimed to reduce time complexity and is robust to jpeg compression. G. Li et al. [23] also have also suggested a DWT and SVD based model where SVD (Singular Value Decomposition) have been applied to the blocks of the low frequency sub band then the SV vectors are lexicographically sorted to locate the clones. This method is robust to JPEG compression up to quality level 70.

PCA based robust technique proposed by Popescu and Farid [24] efficiently detects duplicated region with an computational cost in the order of O(NlogN) but is sensitive to noise or lossy compression. In paper [25], Amtullah et al. have used a faster and robust to noise speeded up robust feature (SURF) – a rotation and scale invariant key point detector and descriptor based algorithm. To identify the duplicated regions, the authors of [26] have combined KD-tree with SURF. A K-dimensional tree or KD-tree is a binary tree with nodes as k-dimensional points and is common technique in nearest neighborhood search. A KD-tree with N-nodes needs $Olog_2N$ search operations. Prerna.C et al. [27] also used KD-tree with SHIFT and RANSAC (Random Sample Consensus) algorithms. RANSAC algorithm has been used to find out the unreliable key points. This technique is robust to additive noise and JPEG compression. There are many more publications [28], [29] on KD-tree based methods but all are not included here. Authors of [30], [31] have detected clones based on SIFT algorithm where they have extracted the SIFT descriptors and then matched those to identify the forgery. The SIFT (scale invariant features transform) algorithm works in four steps such as, the scale space extrema (SSE) detection, the key-point

localization, orientation assignment and key-point description. This method is claimed to be robust against noise attack, JPEG compression, rotation and scaling.

W. Luo, J. Huang and G.Qiu [7] in their paper introduced a seven feature based method that is robust against noise, blur attacks and lossy compression. Najah Muhammad et al. [32] have used multi-scale segmentation and denoising based efficient technique for clone detection. This method is claimed to be robust against noise and blurring attacks. In the paper hybrid copy-move forgery detection technique using regional similarity indices [33], the authors developed a forgery detection using local fractal dimension for image segmentation and estimating SSIM (Structural Similarity Index Measure) between each block pair in each segmented region to localize the forged regions. S.Bayram et al. [34] have suggested a FMT (Fourier-Mellin transform) based robust to noise, blur, rotation, scaling and JPEG compression method. They have used counting bloom filters (CBF) instead of lexicographic sorting for computation time improvement. Solario et al. [35] have suggested a one dimensional descriptor invariant to reflection and rotation based on log polar co-ordinates. In this method, the pixels of overlapping blocks are represented in log polar co-ordinates and summed along the angle to obtain the descriptor.

3.3 Comparison of Different Forgery Detection Methods

A comparison of various important forgery detection techniques evolved from time to time is given in the table 1 below.

Table 1: Comparison of Different Forgery Detection Techniques

Method used	Paper serial	Advantages	Disadvantages
7- feature based robust algo	[7]	Robust to blurring, noise, lossy compression	Not tested for rotation and scaling
4- feature based IIDMJPEG	[8]	Robust to blurring, noise, lossy compression. Can detect intensity variant clones	Not tested for rotation and scaling -
Exhaustive Search and Autocorrelation	[9]	Detects cloned images without post-processing.	Time complexity. Cannot detect if changes is subjected to post processing operations.
DCT	[10]	Detect forgery in JPEG compressed image.	Fails in case of rotation, scaling.
DCT and DQ	[11]	Fast, Robust against JPEG compression and various forgery methods, fine grained detection.	Not tested for rotation, scaling, intensity change.
DCT and SIFT	[12]	Reduced time complexity, robust against rotation, scaling and noise.	Not tested for rotation
DWT, PCA, EVD	[13]	Reduced feature dimension. Better accuracy.	Fails in case of rotation, scaling and heavy compression.
PCA and EVD	[15]	Reduced the dimension and improved computational time.	-
BLUR	[16]	Robust against noise, JPEG compression, blurring.	-
LLE	[17][18]	Detects copy-move forgery as well as fused edges.	-

DWT-DCT and Eigen Vector	[21]	Invariant to JPEG compression and additive noise	-
DWT, Phase correlation	[22]	Reduce time complexity and robust to JPEG compression	-
DWT-SVD	[23]	Robust to JPEG compression up to QF 70, less time complexity.	Not invariant to rotation and scaling.
PCA	[24]	Efficient method, low false positives	Sensitive to noise and lossy compression
SURF	[25]	Invariant to rotation and scaling. Faster and robust to noise	-
KD-tree, SIFT	[27]	Robust to additive noise and JPEG compression	-
SIFT	[30] [31]	Robust against noise attack, JPEG compression, rotation and scaling.	-
FMT	[34]	Robust to blurring, noise, scaling, lossy compression and transitional effects	Cannot detect forgeries which have rotation of above 10 degrees and scaling of 10%
log polar descriptor	[35]	invariant to reflection and rotation	-

4. Summary and Conclusion

Even after a lot of research has been carried out during the last decade, passive forgery detection still continues to be an open research area. Because copy-move forgery or cloning is a technique commonly used by manipulators to forge digital images so, copy-move forgery detection techniques form one of the most important classes of passive detection techniques. The overlapping block matching (OLBM) method suggested in 2003 by Fridrich, A. J. et al. was one of the important developments in the field of cloning detection. Many improvements have been suggested by various researchers from time to time to improve the time complexity of the algorithm as well as to make the detection algorithm robust against post processing operations such as changes in contrast , brightness and color, noise and blurring attacks, lossy compressions, geometric transformations such as rotation, scaling and translation to certain extends but still there exists the need to develop an efficient algorithm that will be able to detect forgeries even after multiple post processing operations and those have been subjected to more than 10% scaling and rotated by an angle greater than 10 degree.

References:

[1] Haouzia A., Noumeir R.: Methods for image authentication: a survey. Multimedia Tools and Applications, 39(1), pp.1–46, (2008).

[2] Mishra M., Adhikary M.C.: Digital Image Tamper Detection Techniques - A Comprehensive Study. International Journal of Computer Science and Business Informatics, 2(1), pp.1-12, (2013).

[3] Kaur H., Kaur K.: A Brief Survey of Different Techniques for Detecting Copy-Move Forgery. International Journal of Advanced Research in Computer Science and Software Engineering, 5(4), pp. 875-882, (2015).

[4] Shah H., Shinde p., and Kukreja J.: Retouching Detection and Steganalysis. International Journal of Engineering Innovation & Research, 2(6), pp. 487-490, (2013).

[5] Gupta A., Saxena N., and Vasistha S.K.: Detecting Copy-Move Forgery Using DCT. International Journal of Scientific and Research Publications, 3(5), pp. 1-4, (2013).

[6] Mishra M., Adhikary M. C.: Detection of Clones in Digital Images. International Journal of Computer Science and Business Informatics, 9(1), pp. 91-102, (2014).

[7] Luo, W., Huang, J., and Qiu, G.: Robust detection of region-duplication forgery in digital image. In: Proceedings of 18th International Conference on Pattern Recognition IEEE, vol. 4, pp.746-749, (2006).

[8] Mishra M., Adhikary M.C.: Robust detection of Intensity Variant Clones in Forged and JPEG compressed Images. ANVESA, 9(1), pp. 48-60, (2014).

[9] Fridrich, J., Soukal, D., and Lukas, J.: Detection of copy-move forgery in digital images. In Proceedings of Digital Forensic Research Workshop, (2003)

[10] Murali S., Govindraj B., Chittapur, Prabhakara H. S., and Basavaraj S. Anami.: comparison and analysis of photo image Forgery detection techniques. IJCA, 2 (6), pp. 45-56, (2012).

[11] Zhouchen L.: Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recognition, 42(11), pp. 2492-2501, (2009).

[12] Singh R., Oberoi A., and Goel N.: Copy-Move Forgery Detection on Digital Images. International Journal of Computer Applications, 98 (9), (2014).

[13] Zimba M., and Xingming S.: DWT-PCA (EVD) based copy-move image forgery detection. International Journal of Digital Content Technology and its Application, 5 (1), pp. 251–258, (2011).

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

[15] Zimba M., Xingming S.: Fast and robust image cloning detection using block characteristics of DWT coefficients. International Journal of Digital Content Technology and its Application, 5(7), pp. 359–367, (2011).

[16] Mahdian B., and Saic S.: Detection of copy–move forgery using a method based on blur moment invariants. Forensic Science International, 171(2), pp. 180-189, (2007).

[17] Junhong, Z.: Detection of Copy-Move Forgery Based on one Improved LLE Method. In: Advanced Computer Control (ICACC) IEEE, vol. 4, pp.547-550, (2010).

[18] Roweis S.T., Saul L.K.: Nonlinear dimensionality reduction by locally linear embedding. Science, 290(5500), pp. 2323 -2326, (2000).

[19] Kaur R.: Copy-Move Forgery Detection Utilizing Local Binary Patterns. International Journal of Emerging Technologies in Computational and Applied Sciences, 7(3), pp.290-294, (2013).

[20] Muhammad, N., Muhammad, H., Muhammad, G., and Bebis, G.: Copy-Move Forgery Detection using Dyadic Wavelet Transform. In: Computer Graphics, Imaging and Visualization (CGIV), Eighth International Conference on IEEE, pp.103-108 (2011).

[21] Wang, X., Zhang, X., Li, Z., and Wang, S.: A DWT-DCT based passive forensics method for copy-move attacks. In: 2011 Third International Conference on Multimedia Information Networking and Security, IEEE, pp.304-308, (2011).

[22] Zhang, J., Feng, Z., and Su, Y.: A New Approach for Detecting Copy-Move Forgery in Digital Images. In: Communication Systems, 11th IEEE Singapore International Conference on IEEE, pp.362-366, (2008).

[23] Li, G., Wu, Q., Tu, D., and Sun, S.: A Sorted Neighbourhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD. In IEEE International Conference on Multimedia and Expo, pp.1750-1753, (2007)

[24] Popescu A, Farid H.: Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Department of Computer Science, Dartmouth College, pp.1-1, (2004)

[25] Amtullah S., and Koul A.: Passive Image Forensic Method To Detect Copy-Move Forgery In Digital Images. IOSR-JCE, 16(2), pp.96-104, (2014).

[26] Shivakumar B.L., and Baboo L.D.S.S.: Detection of Region Duplication Forgery in Digital Images Using SURF. International Journal of Computer Science Issues, 8(4), (2011).

[27] Prerna C., Percy G. J., Angaline S., and Thanga B. I.: A key-point based copy-move forgery detection. International journal of advanced information science and technology (IJAIST), 12(12), pp.175-180, (2013).

[28] Sagawa, R., Masuda, T., and Ikeuchi, K.: Effective nearest neighbor search for aligning and merging range images, In: 3-D Digital Imaging and Modeling, Fourth International Conference on IEEE, (2003) 54-61

[29] Bentley J.L.: Multidimensional binary search trees used for associative searching. Communications of the ACM, 18(9), pp. 509-517, (1975).

[30] Huang, H., Guo, W., and Zhang, Y.: Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm. In: Computational Intelligence and Industrial Application, Pacific-Asia Workshop on IEEE, vol. 2, pp.272-276, (2008)

[31] Lowe D.G.: Distinctive Image features from Scale-Invariant Key points. International Journal of Computer Vision, 60(2), pp. 91-110, (2004).

[32] Muhammad, N., Hussain, M., Muhammad, G., and Bebis, G.: A Non-Intrusive Method for Copy-Move Forgery Detection, In: International Symposium on Visual Computing. Springer Berlin Heidelberg, pp.516-525, (2011).

[33] Oommen R.S., and Jayamohan M.: A Hybrid Copy-Move Forgery Detection Technique Using Regional Similarity Indices. International Journal of Computer Science and Information Technology (IJCSIT), 7(4), pp.127-134, (2015).

[34] Bayram, S., Sencar, T., and Memon, N.: An Efficient and Robust Method For Detecting Copy-Move Forgery. In: IEEE International Conference on Acoustics, Speech and Signal Processing, pp.1053-1056, (2009).

[35] Solorio, S. B., and Nandi, A.K.: Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling. In: Signal Processing Conference, 17th European, IEEE, pp.824–828, (2009).