Recent Block-based Methods of Copy-Move Forgery Detection in Digital Images

Resmi Sekhar
Assistant Professor
Lourdes Matha College of Science and Technology
Kerala, India

Chithra A S
Associate Professor
Lourdes Matha College of Science and Technology
Kerala, India

ABSTRACT
Photographs are taken as valid evidences in various scenarios of our day to day life. Because of the developments in the field of Image Processing, altering images according to ones need is not a difficult task. Techniques of Image Forensics play its crucial role at this juncture. One of the mostly found types of image tampering is Copy-Move forgery. A copy-move forgery is performed by copying a region in an image and pasting it on another region in the same image, mostly after some form of post-processing like rotation, scaling, blurring, noise addition, JPEG compression etc. Two types of copy-move forgery detection techniques exist in literature. They are the Block based methods and Key-point based methods. Both the methods have their own advantages and limitations. This paper presents a survey on the recent developments in block based methods.

General Terms
Image Processing, Image Forensics, Image Tampering Detection

Keywords
Image Forgery, Copy-move forgery detection, Block-Based methods

1. INTRODUCTION
Digital Image forensics is a young and emerging branch of image processing, which is aimed at obtaining quantitative evidence on the origin and truthfulness of a digital image .One of the principal tasks of image forensics is image tampering detection. Tampering literally means to interfere with something in order to cause damage or make unauthorized alterations. Images are treated as proofs in various scenarios and thus image tampering is defined as intentional manipulation of images for malicious purposes [1]. Image tampering dates its origin to the earliest twentieth century when it was used for political propaganda. Today, because of the advent of powerful image processing tools, image tampering is not a rare phenomenon and as a result the last decade marked tremendous developments in the field of image forensics techniques. Image forensics techniques can be classified under two different approaches, Active approaches and Passive/Blind approaches [2]. Active approaches were used traditionally by employing data hiding (watermarking) or digital signatures. Requirement of specialized hardware narrows its field of application. Passive approaches or blind forensic approaches use image statistics or content of the image to verify its genuineness.

Image tampering can be done with a single image or with multiple images. Splicing(combining contents from two or more images in a single image), Copy-move forgery, use of Image Processing operations, False Captioning etc. are treated as different forgery types [2]. Among this Copy-move forgery is the most commonly performed and most studied one. It is a type of forgery in which a region from the same image is copied and pasted on the same image in order to hide something or to duplicate something. This paper aims at reviewing some of the very recent blind methods in copy-move forgery detection. The rest of the paper is organized in the following way. Section 2 gives an overview of different approaches in Copy-Move forgery detection. Section 3 covers the different Block based methods followed by a comparison of the different methods in Section 4.Conclusion is given in Section 5.

2. COPY-MOVE FORGERY DETECTION
As stated earlier Copy Move forgery is performed by duplicating a region in the same image to hide something or to emphasize something. Fig 1 gives examples for Copy Move attack. [3]. A copy move forgery is easy to create. As the source and the target regions are from the same image, the image features like noise, color, illumination condition etc. will be same for the forged region and the rest of the image. This concept is used by most of the copy move detection techniques. A clever forger may also do some post-processing on the copied region like rotation, scaling, blurring, noise addition before the region is pasted. More over the image may be compressed with compression algorithms like JPEG. These factors make the forgery detection more complex. So the crucial point in such a forgery detection technique would be extraction of features, which are invariant to the above said post-processing operations, from the image. It is also revealed that a method that is robust to some form of post-processing may not be adequate to detect forgery with another method.

Generally, Copy-Move forgery detection techniques can be classified into two: Block based approaches and Key-point based approaches [4]. In both the approaches some form of pre-processing will be there. In block based methods, the image will be divided into overlapping blocks of specified size and a feature vector will be computed for these blocks. Similar feature vectors are then matched to find the forged regions. In Key-point based methods, feature vectors are computed for regions with high entropy. There is no subdivision into blocks. The feature vectors are matched to find the copied blocks. The common processing pipeline for copy move forgery detection is shown in Fig 2. [4].

Fig 1: A photo published on the front page of Le Maghreb, a Tunisian newspaper, on January 2012. The photo was digitally altered duplicating the crowd to appear larger [3].

3. BLOCK-BASED METHODS

The earliest of the block based approaches dates back to the method based on DCT coefficients of blocks [6], in 2003 and the one based on PCA of blocks in 2004 [7]. Most of the popularly used techniques for copy move forgery detection since then have been studied extensively and quantitatively in the work [4]. In their paper the authors reviewed most of the available approaches based on 15 feature sets. This paper surveys mainly the very recent approaches in copy move forgery detection.

One of the efficient block based methods which gave the most precise results [4] was presented in [8] during 2010. The work was aimed at detecting copy-rotate-move forgery using Zernike moments which have desirable properties like rotation invariance, robustness to noise etc. The average rate of precision achieved was 83.59%. Accurate results were obtained for rotation with 30◦. Detectability of copy-move forgery against intended distortions such as JPEG compression, additive white Gaussian noise, and blurring were tested. The method was found to be weak against scaling and affine transformations and it proposed the use of efficient data structures to reduce computational complexity.

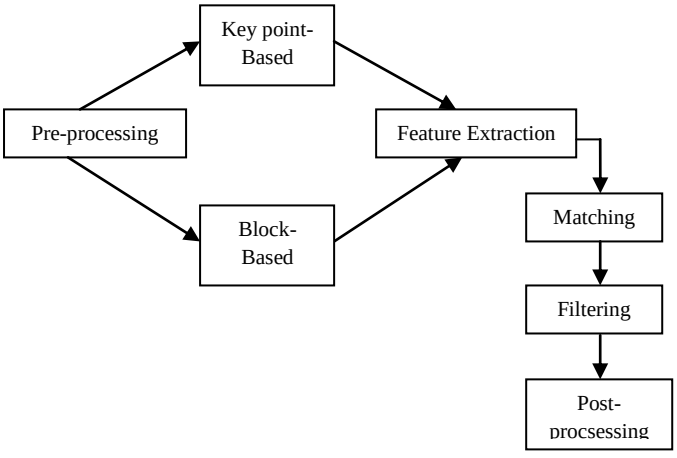

Fig 2: Common processing pipeline for copy-move forgery detection

Another method for rotation invariant copy-move forgery detection was proposed in [9]. It was based on a method called Same Affine Transformation Selection (SATS), which had the benefit of shift vectors with some additional computational complexity. Use of Kd tree algorithm for matching reduced the number of false positives. It can detect arbitrary variations in rotation and scaling in the copied part and is a processing scheme in which any suitable feature can be used in combination with the SATS post processing. It was tested in combination with the previous method of Ryu [8] and nearly 75% of the duplicated blocks with rotation were detected and the method was found to be accurate for JPEG compression with Q factor 50 to 100.

Reference [10] proposed a method to detect copy-move forgery with rotation, scaling and reflection. The method uses color dependent feature vectors. Here also the image is divided into overlapping pixel block and each block is mapped to a 1D descriptor invariant to reflection, rotation and scaling. Four features are computed for pixels in a block, where first three are average of red, green and blue components of the pixels and fourth one is calculated as entropy of the luminance channel. These features are then lexicographically sorted so that similar features come nearby. This is then followed by a refinement stage to remove the false positives. The results show that the method generates less false positives compared to previous methods handling rotation, scaling and reflection.

In 2012, [11] proposed a method using dyadic wavelets. Un-decimated dyadic wavelets were chosen because of their property of shift invariance. For the input image DyDWT is taken and only the LL1 and HH1 sub-bands are used further. LL1 sub-band is an approximation of the image and HH1 sub-band encodes noise in the image which is distorted while performing the forgery. Then the HH1 and LL1 sub-bands are divided into 16x16 pixel blocks and the Euclidean distance between each pair of blocks is found for both the sub-bands. The distances found using the LL1 are sorted in ascending order and distances found using the HH1 sub-band are sorted in the descending order. Pair of blocks appearing at the similar location in both the lists is treated as copied and moved blocks. Uniform regions in the image will not be identified as similar in the HH1 sub-band and thisavoids false positives. The method was tested for copy-move forgery with no rotation, with rotation and also for different levels of JPEG Q factors. The method was found to be advantageous than previous methods using DWT and the methods in [12] and [13].

The work in [14] put forward a method using DCT and circular blocks in 2012. After block subdivision DCT is applied to each block. As in DCT, the energy concentrates on low frequency coefficients; a circle block representation is adopted for each block. A circle block is divided into four quadrants and features extracted from each quadrant. So an 8x8 block is represented using 1x4 feature vector. These features are invariant for post-processing operations like additive white Gaussian noise. These feature vectors are sorted and Euclidean distance between adjacent feature vectors are calculated. The blocks with feature vectors at a distance less than a preset threshold are considered as candidates for forgery. The method is advantageous due to reduced computational complexity obtained as a result of reduced feature vector representation. The performance was found to be better than many previous methods discussed in [6, 7, 15 and 16].

Another work [17] in 2013 presented a method that takes only low frequency part of the image by performing a Gaussian pyramids decomposition. Low frequency part will be half the size of the image. Mixed moments are computed for the overlapping b x b sub-blocks whose total count will be Y= ([M/2]-b+1) x ([N/2]-b+1). A 7xY characteristic feature vector will be obtained thus. This matrix is lexicographically sorted and a spatial distance and Euclidean distance is computed. Blocks whose spatial distance is less than a predetermined threshold and whose Euclidean distance is greater than a predetermined threshold will be removed. The authors claim that the algorithm showed good detection and positioning effect in copy-move forgeries with rotation, scaling and translation. They establish the advantage of reduced number of blocks and reduced feature vector dimension against the methods in [6, 7].

Reference [18] in 2013 addressed the type of copy-move forgeries with more general affine transforms like rotation plus scaling, shearing and perspective transforms. The method operates in the luminance domain. As high frequency components are not stable when the image undergoes signal processing operations, low frequency components are useful in feature matching. So a low pass filter like Gaussian low pass filter is adopted to reduce the high frequency components. This filtered image is subdivided into circular blocks as the contents will be kept constant in circular blocks even after rotation. Polar sine transform is used to extract features and feature matrix is sorted. Euclidean distance between blocks is computed and blocks at a distance less than a predetermined threshold are saved for post-processing. Simulation results are provided for different types of attacks accompanied with scaling alone, rotation alone , rotation with scaling, region flipping, affine transforms like shearing and perspective projection, signal processing operations like additive white Gaussian noise, JPEG compression with different quality factors Gaussian blur etc. The authors claim their method to be as robust as [g] and robust to signal processing operations.

A method was developed in [19] to detect forgery in exemplar based inpainting images. The paper is primarily aimed at detecting forgeries using Criminisi's algorithm [20]. The result also establishes robust performance against copy-move forgery without scaling or rotation. The method is shown to be robust for plain copy-move and inpainting attacks. There exist a lot of performance improvement chances with the proposed method.

A recent method based of expanding blocks was proposed in [21] in 2013. In their approach they used the direct block comparison instead of comparison based on block features. The image is divided into overlapping blocks and a dominant feature, that is the average of the gray level values in that block, is computed for each block. The blocks are sorted and grouped into buckets, each group having similar features. i, i+1, i-1 groups form a bucket. Blocks are compared against blocks in the same bucket only. A statistical hypothesis test based on mean value of pixels is used here. A block is eliminated from the bucket if it does not match with any other block in the bucket. Comparisons starts with a small region, blocks with no matches are eliminated, the search region is expanded and the comparison is continued. As the region expands the number blocks in the bucket reduces and remaining blocks are considered as part of the copied region. The paper is tested by varying the values of different parameters, comparison with other algorithms based on DCT [6] and PCA [7], with different amount of blurring and JPEG compression ratio and for irregularly shaped regions. The algorithm is enhanced to detect forgery that applies slight darkening or lightening on the copied region, a type of forgery that has not been addressed before.

Table 1. Comparison of different method

Method	Feature length	Block Size	Image size	Advantages	Disadvantages	Performance with geometric operations and other modifications	Noise	JPEG compression	Time
Zernikie moments [8],2010	12	111969 (24*24)	400 x 320	JPEG compression, blurring and additive white Gaussian noise	Does not address scaling and affine transformation	Rotation through angle of 30 degree. combined attack not specified	Gaussian noise with SNR 30 db	JPEG compression with quality factor as low as 60	Approx. takes 50 sec to process one image

SATS with KD Tree [9], 2010	Depends upon which method used with SATS	Features are extracted on those blocks with minimum entropy 4.0(4*4)	640 x 480	Invariant to rotation and false positive rate is also low with reduced runtime	Detection accuracy reduces with increase in image size. Processing time is not evaluated to check the actual performance	Rotation through angle between 0 and 180 degree	--	JPEG compression with quality factor between 50 to 100	Run time decreases
Color dependent feature [10], 2011	4	24x24	300 x 400	Reduced false alarm rate even in images with intrinsic symmetries.	Does not address illumination variation, blurring etc. Images with large regions with very little textural information remain a challenge.	Horizontal reflection, rotation by random angle, scaling by random factor [0.95, 1.05], combined distortions including/excluding reflection	--	--	Not evaluated.
Dy DWT [11] , 2012	-	16 x16 for HH1 and LL1 bands only	200 x 200, 374 x 256	Reduced false positives. Advantageous than previous methods using DWT and other rotation invariant method like [12, 13]	Tested only for small rotation angle and good quality images	Rotation angle < 20 degree	---	JPEG compression with quality factor 90, 80, 60	Not evaluated. Will decrease as there is no feature extraction
Circular Block with DCT [14], 2012	4	8x8	128 x 128, 768x 512, 1600x1 000	Perfect detection for uniform background images, non-regular duplicate regions, high resolution images. Detect multiple copies - move.	Poor performance with poor image quality. Not robust to geometrical operations	AWGN with SNR=5, 10, 15, 20, 25, 30.	Gaussian σ= 0.5,1,1.5,2,2.5,3 and w=5	Not specified	Depends on image size. Varies from 1.5 sec to 2.9 min

Mixed Moments [17], 2013	7	8x8	Not Specified	Tested for rotation, scaling, brightness enhancement, contrast changes. Reduced number of blocks.	Qualitative evaluation not specified	Rotation angle and scaling factor not specified.	--	--	Not evaluated.
Polar harmonic transform [18], 2013	9	Circular block with diameter =16	Not specified	Addressed affine transforms like shearing and perspective projections that were rarely considered before.	Simulation results only available	Scaling with 0.7, 0.9, 1.1 (High accuracy). Rotation by 15, 30, 90 degrees (performance as good as [g]. Rotation with scaling, Region flipping shearing horizontal and vertical by 20 degree, perspective transforms distorted by two sets of parameters	--	--	Not evaluated
Method to detect inpainting [19], 2013	-	5x5	256 x 193, 270 x 180, 212 x 149	False alarms are less. Can be adopted to copy- move forgery detection with other post – processing	Addresses only plain copy-move. Fails if copied region is too small	--	--	--	112 sec to 191 sec depending on size of image
Expanding Blocks [21], 2013	-	16x16	256 x 256	Detection with irregularly shaped regions and for forged regions slightly darkened or lightened.	Slow in execution. Number of false positives more when compared to other methods.	Addresses irregular shaped regions, blurring by 3x3 to 15 x 15, regions pasted after slight darkening or lightening of copied region by a factor of 5, 2, 1	--	JPEG compression ratios 1, 0.95, 0.9, 0.85, 0.8. Better results for large ratio.	10.32 sec (reduced run time for increase in number of buckets)

4. COMPARISON OF THE METHODS

All the above methods basically work by dividing the image into overlapping blocks. The difference lies in the features used and comparison methods used. A comparison of the above discussed methods is given in Table 1. It summarizes the advantages, disadvantages, different issues addressed and the time complexities.

5. CONCLUSION

Copy-Move forgery in digital images is more prevalent during the past two or three decades and this emphasizes the need for developing efficient algorithms that can efficiently handle these types of forgeries. Different types of methods have been explored since 2004, which can handle different types of copy-move forgeries. Nevertheless, there exists a gap between the sophisticated image processing tools that make copy-move forgery straightforward and the available detection algorithms. A technique that is suitable for one type of post-processing on the copied region may not be efficient to handle another type of post-processing. Some of the recent developments in the field is discussed in this paper. A single system that can handle copy-move forgery of any type is a necessity.

6. REFERENCES

[1] Judith Redi, Wiem Taktak, Jean-Luc Dugelay: Digital image forensics: a booklet for beginners. Multimedia Tools Appl. 51(1): 133-162 (2011).

[2] Pravin Kakar "Passive Approaches for Digital Image Forgery Detection", Ph.D. Dissertation, School of Computer Engineering, Nanyang Technological University, Singapore, 2012.

[3] I.Amerini et al, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage", Signal Processing: Image Communication 28, 2013.

[4] Christlein V, C Riess , C Riess, E Angelopoulou, J Jordan, "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Trans on Information Forensica and Security, Vol 7 No 6, Dec 2012.

[5] H .T Sencar, N. D Memon, "Digital Image Forensics: There is More to a Picture Than Meets the Eye", springer , 2013.

[6] J. Fridrich, B. Soukal, and A. Lukáš, "Detection of copy-move forgery in digital images", in Proc. Digital Forensic Res. Workshop, 2003

[7] A.Popescu, H. Farid, "Exposing digital forgeries by detecting duplicated image regions", Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.

[8] S. Ryu, M. Lee, H. Lee, "Detection of copy-rotate-move forgery using zernike moments," in Proc. Int. Workshop Information Hiding, Springer , pp. 51–65, 2010.

[9] Christlein V, C Riess, E Angelopoulou, "On rotation invariance in copy-move forgery detection ", IEEE International Workshop on Information Forensics and Security (WIFS), 2010.

[10] S. Bravo-Solorio, A. K. Nandi, "Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling," in International Conference on Acoustics, Speech and Signal Processing, May 2011.

[11] Muhammad, G., Hussain, M., Bebis, G., "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Digital Investigation (9), 2012.

[12] Mahdian B, Saic S., "Detection of copy-move forgery using a method based on blur moment invariants", Forensic Science International 2007.

[13] Li G, Wu Q, Tu D, Sun S. "A sorted neighborhood approach detecting duplicated forgeries based on DWT and SVD", In: Proc. ICME 2007.

[14] Cao Y, Gao T, Fan L, Yang Q., "A robust detection algorithm for copy-move forgery in digital images", Forensic Sci Int. 2012 Jan.

[15] Huang Y, Lu W, Sun W, Long D, "Improved DCT-based detection of copy-move forgery in images", Forensic Science International 206 (1–3) 2011.

[16] S. Bayram, H.T. Sencar, N. Memon, "An efficient and robust method for detecting copy-move forgery", in: IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, New York, 2009.

[17] Zhong L, Xu W, "A robust image copy-move forgery detection based on mixed moments", IEEE International Conference on Software Engineering and Service Sciences (ICSESS), 2013 May.

[18] Li L, Li S, Zhu H, Wu X. "Detecting copy-move forgery under affine transforms for image forensics", Comput Electr Eng (2013), http://dx.doi.org/10.1016/j.compeleceng.2013.11.034.

[19] I-Cheng Chang, J. Cloud Yu, Chih-Chuan Chang, "A forgery detection algorithm for exemplar-based inpainting images using multi-region relation", Image and Vision Computing 31, 2013.

[20] A.Criminisi, P. Perez, K. Toyama, Region filling and object removal by exemplar-based image inpainting, IEEE Trans. Image Process. 2004.

[21] L Gavin, S Frank, L Hong-Yuan Markl, "An efficient expanding block algorithm for image copy-move forgery detection", Information Sciences 239, 2013.