Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 383 – 390

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Pixel based Image Forensic Technique for copy-move forgery detection using Auto Color Correlogram.

Ashwini V Malviya[a,*], Siddharth A Ladhake[b]

[a]*Sipna College of Engineering and Technology, Amravati,444701,India*
[b]*Sipna College of Engineering and Technology, Amravati,444701,India*

Abstract

The credibility of a digital image plays a generous role in blind Image forensics. We focus on detection of a typical kind of forgery, referred to as copy-move forgery, which is commonly practiced in the field of blind image forensics. In this kind of forgery as the forged region belongs to same image, it introduces inconsistency at pixel level in the tampered image. In the proposed work, we exploit a content based image retrieval feature extraction technique for detection of forgery. Auto Color Correlogram, which is a low complexity feature extraction technique, is employed to obtain feature vectors from the forged image. ACC is not used for detection of copy-move forgery in the previous detection schemes. The scheme is also successful in detecting forged region which is scaled or rotated on pasting, also effectively detects multiple region duplication within the image.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: copy-move forgery detection; Auto Color Correlogram; blind image forensic; pixel based approaches

1. Introduction

With technology flourishing all over the world, the use of different software tools in every field is common. The tampering of a digital image is neither new nor recent. But the powerful photo editing software packages which are easily available make it very easy to manipulate an image. The credibility of digital image or the authenticity of the

* Corresponding author. Tel.: +919766315429; fax: +0-000-000-0000 .
E-mail address: ash.malviya@gmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.050

image is a challenging task in blind image forensic. There are several types of tampering. It is difficult to determine the kind of tampering the image is subjected to.

Out of numerous forgeries we concentrate on the copy-move forgery. In this kind of forgery the portion from the image is copied and pasted in the same image either to hide an undesirable object or to enhance the content of the image. This forgery is also referred to as copy-paste forgery or cloning. On the basis of fact that the manipulated image does not show any traces of tampering when viewed by naked eyes, but it does create glitches at pixel level. This makes detection of this forgery possible. There are several methods for detection of copy-move forgery. In the next section of the paper, we discourse the methods employed for detection of this forgery.

2. Related work

The common method used by several researchers for forgery detection is dividing the image into blocks and then extracting features of the blocks. Considering the time complexity reduction, DCT [2] and PCA[3] was applied to the blocks to fetch feature vectors from the block. Lexicographical sorting was used to sort the vectors. Similarity measures like Euclidean distance determined the forged region by comparing the blocks. In the method proposed by [4], the image is divided into blocks and block characteristics are derived for each block and are the matched to detect the forgery. In another passive approach by G. Li in [5] used a combination of DWT and SVD, to obtain a reduce dimension representation, and further obtained SV vectors are sorted to get an exact match.

Many a times, retouching of the copied portion to be camouflaged with the image content is carried out to make forgery untraceable. Huang et al. [6] obtained the scale invariant features transform descriptors of an image, as they are immune to transformations. Later I. Amerini et al. [11], improvised the SIFT technique for detection of forgery. Bayram et al.[9], exploited the Fourier Mellin transform for feature extraction and detected the forgery by counting bloom filters.

B. L. Shivakumar et al. [10], introduced the speed up robust features laterally with KD tree to detect the cloned region effectively. Jing Ming Guo et al. [13], presented an efficient algorithm using ANMS along improvised daisy descriptor to identify the forgery. . Leida Li et al. [14] divided the image in circular blocks after filtering it. Feature vectors derived by extracting Polar Harmonic Transform are then sorted lexicographically and identical portion are detected by post processing of matching similar block pair.

Recently Gabor magnitude of image was used for feature extraction by Chen-Ming Hsu et al. [15]. In this approach Gabor filter is applied to the blocks of image and features are extracted by histogram of Gabor magnitude. Further similar matches are detected by sorting and post processing. The cluster expanding block algorithm is improvised in the method proposed by Cheng-Shian Lin et al. [16]. In this approach the computational time is reduced. The method is effective in improving the computation time by 10%.

It is very evident from the literature that the forgery detection techniques discussed have their pros and cons. Many of the schemes propose feature extractions which are invariant to transformations such as blurring, distortion, rotation, scaling and translation. But such schemes are expensive and complex. In this paper we exploit the Auto Color Correlogram (ACC) of an image to extract features. ColorAutoCorrelogram is used expansively for Image Retrieval schemes. The color Correlogram proposed by [7], was enhanced for spatial color indexing as ACC by Tungkasthan et al. [8]. The proposed scheme for feature extraction is simple and robust.

3. Proposed Method

The proposed method has the following steps:

- Preprocess the image by filtering noise and divide the image into M x N blocks.
- Subject each block to 8Z affine transformation.
- Feature extraction of each block by extracting Auto Color Correlogram of each block.
- Finding match using similarity measure to detect the forgery.

The query image is prepped by filtering the image for removing noise. Further the image is divided into overlapping blocks. To make the forgery undetectable, many a times the copied region before pasting is subjected to

transformation such as rotation and scaling. Also the forged region is retouched to blend with the background. Taking this into account, the method differs from the traditional methods previously employed. The image is divided into blocks and each block is subjected to 8Z affine transformation. The figure 1 shows the 8Z affine transformation of a single highlighted block of the image. Further Auto Color Correlogram of each block is extracted.

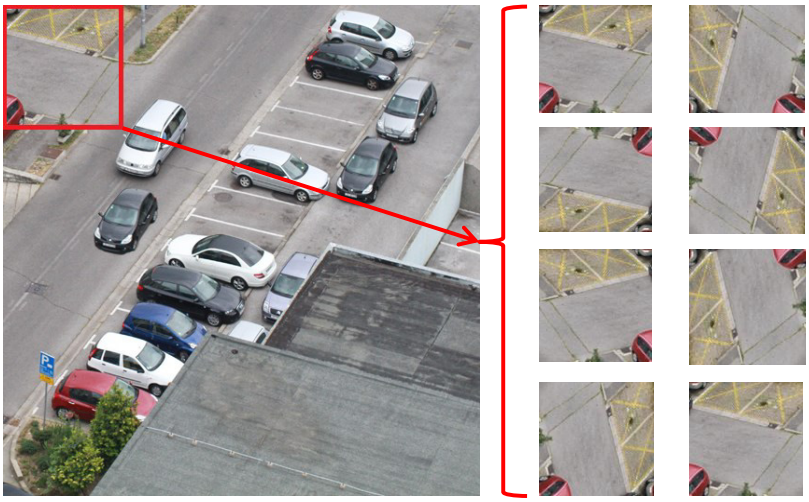


Fig. 1. Affine transformation of each block

3.1. AutoColorCorrelogram

Auto Color Correlogram (ACC) is an integration of Correlogram and Color correlation. ACC Algorithm was introduced by [8], for spatial color indexing. The feature is used basically in image retrieval system. The ACC takes into account all the pixels of Color C_j at a particular distance from all the pixels of color C_i to compute the mean color. It is formulated as follows:

$$ACC(i,j,k) = Avg\ \gamma^{(k)}_{C_i VC_j}(I)$$

$$= \left\{ Avg\gamma^{(k)}_{C_i C_{jr}}(I), Avg\gamma^{(k)}_{C_i C_{jg}}(I), Avg\gamma^{(k)}_{C_i C_{jb}}(I) \middle| C_i \neq C_J \right\} \quad (1)$$

Where $I(x,y)$ is the original image with $x=1,2,\ldots,M$ and $y=1,2,\ldots,N$. It is quantized in $C_1, C_2, \ldots\ldots, C_m$ colors, where kϵ[min(M,N)] is the distance between the pixels, VC_j gives the RGB value of the color m of the image [8].The arithmetic mean colors are obtained by the following formula:

$$Avg\ \gamma^{(k)}_{C_i VC_{jx}}(I) = \left. \frac{\prod^{(k)}_{C_i VC_{jx}}(I)}{\prod^{(k)}_{C_i C_j}(I)} \right| x = r,g,b \quad (2)$$

The denominator gives total of color C_j pixel color values separated by k distance from color C_i pixels, and VC_{jx} gives RGB color value of C_j, $C_j \neq 0$. N is number of accounting color C_j at distance k from color C_i, formulated as,

$$N = \prod_{C_iC_j}^{(k)}(I) = \begin{cases} P(x_1, y_1)\epsilon C_i | P(x_2, y_2)\epsilon C_j; \\ k = min\{|x_1 - x_2|, |y_1 - y_2|\}; \end{cases} \quad (3)$$

3.2. Forgery Detection

The feature extracted from each blocks forms row in a matrix. Manhattan distance is used as similarity measure for finding the exact match. Euclidean distance is used in many of the previous literature for matching the features for copy-move forgery detection techniques. We differ from the rest by using Manhattan distance to determine the distance between two feature vectors. Compared to Euclidean distance, Manhattan distance gives low computational complexity. The Manhattan distance is also referred as L1 norm. The Manhattan distance between two pints $s=(x_1, y_1)$ and $t=(x_2, y_2)$ is formulated as

$$MH\ (s,\ t) = |x_1 - x_2| + |y_1 - y_2| \quad (4)$$

Instead of two dimensions, if the points have n dimensions, such as $a = (x_1, x_2, \ldots, x_n)$ and $b = (y_1, y_2, \ldots, y_n)$ then, above equation can be generalized by defining the Manhattan distance between a and b as

$$MH(a, b) = |x_1 - y_1| + |x_2 - y_2| + \cdots + |x_n - y_n| \ = \sum |x_i - y_i| \quad (5)$$

For $i = 1, 2\ldots, n$.

The simplicity and robustness of the L1 norm makes it appropriate for comparing auto color Correlogram of two blocks. The features of each block are compared with the feature vector of every other block of the image to find the match. The method uses the d_1 distance metric [7], as follows,.

$$|I - I'|_{\gamma,d1} \triangleq \sum_{i,j\epsilon[m],k\epsilon[d]} \frac{\left|\gamma_{C_iC_j}^{(k)}(I) - \gamma_{C_iC_j}^{(k)}(I')\right|}{1 + \gamma_{C_iC_j}^{(k)}(I) + \gamma_{C_iC_j}^{(k)}(I')} \quad (6)$$

Where I and I' are two blocks of the image, features of each block will be compared with every other block for finding the match.

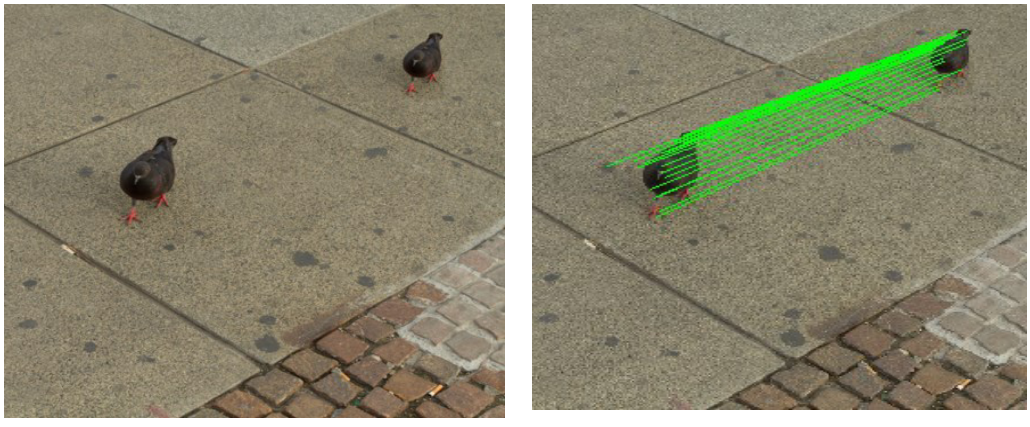
4. Experimental Visual Results

The image database used is CoMoFoD database which is made available online by [17]. It consists of 260 image sets, of small and large categories. We have considered the 200 image set in small image category (512x512). The method introduced in this paper is been implemented on small image category. Various transformations such as translation, rotation, scaling, distortion and combination are applied to the images in the database.

Figure 2, shows the detection by proposed method. Here the pasted region has not undergone any kind of transformation. Figure 3, shows detection of forgery, when the copied part is scaled on pasting. The scheme is accurately able to detect the forgery. Figure 4, shows an image tampered with multiple copy-move attacks in the image. The proposed scheme is competent in detection of multiple forgeries in single image.

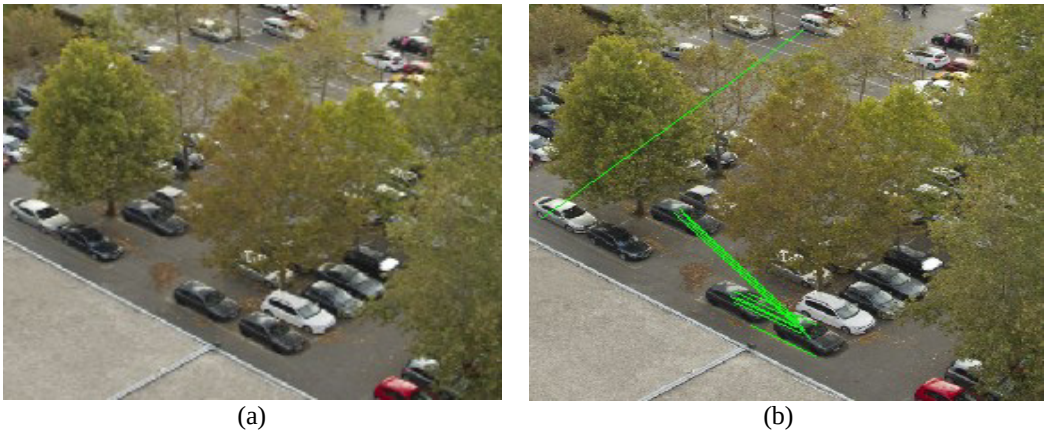
(a) (b)

Fig. 2. (a) The Plain Copy-move forged image. (b) Forgery Detection



(a) (b)

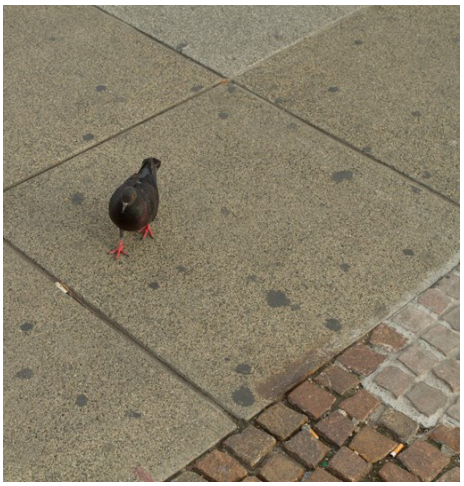
Fig. 3. (a) The scaled forged region. (b) Forgery Detection



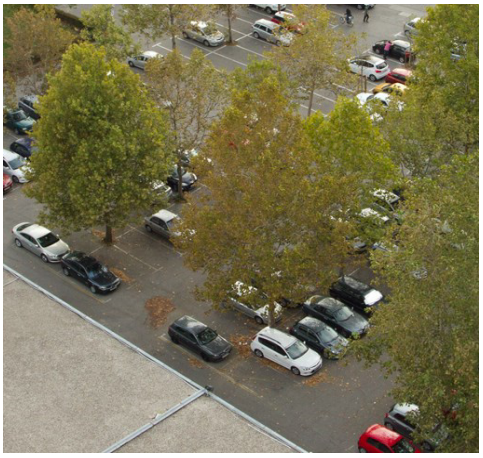
(a) (b)

Fig. 4 (a) A multiple Copy-move forged image. (b) Forgery Detection

(a)



(b)



(c)

Fig. 5 (a), (b) and (c) Original images which were then tampered plain, scaled and multiple copy-move forgery

It is clear from figure 5, that the copy-move forgery is carried out in varying behavior. The car is copied without any transformation as seen in figure 2(a). While the bird is scaled to a smaller size in the image, before pasting, as shown in figure 3(a). For image in figure 4(a), the black car is copied twice to enhance the content of the image. Thus the proposed scheme is accurate in detecting transformed duplicated region.

5. Experimental Statistical Results

Matlab R2010b version is used on 64 Bit Windows with 8 GB RAM to evaluate timing performance. 400 random images from the database are considered for copy-move forgery detection in our system. The detection of forgery is accessed by the true positives and false positive outputs. The parameters used to assess our technique are precision p_r , recall r_c and F1 score, which are calculated as follows:

$$p_r = \frac{t_p}{t_p+f_p} \qquad r_c = \frac{t_p}{t_p+f_n} \qquad F1 = \frac{2p_r r_c}{p_r+r_c} \tag{7}$$

Forged images correctly detected are Forged images correctly detected are t_p. Images wrongly detected as forged are termed as f_p Tampered images that are falsely missed are termed as f_n. The results obtained for the database are presented in Table 1.

Table 1. Experimental results for 400 Images.

Images	True Positive(t_p)	False Positive(f_p)	False Negative(f_n)	Precision(p_r)	Recall(r_c)	F1
400 database images	352	16	32	.9565	.9167	.9362

A comparison with prevailing methods [12] also shows that the proposed method efficiently detects the forgery. The table 2 shows a comparative analysis of few previous methods employed for copy-move forgery detection.

Table 2. Comparative Result

Feature extraction methods	Precision (%)	Recall(%)	F1 (%)
DCT	78.69	100	88.07
PCA	84.21	100	93.20
SURF	91.49	89.58	90.53
Proposed ACC	95.65	91.67	93.62

4. Conclusion

The copy-move forgery or cloning is extensively practiced to enhance the content of the image. Various methodologies, varying in terms of segmentation of image, feature extraction, sorting and detection schemes have been proposed by researchers. The problem is interesting in itself. A lot of effort has been done on identifying relevant features for detecting duplicity of object in an image. The proposed method uses an ACC which has not been used for copy-move forgery detection. The scheme is successful in accurately detecting the duplicated region. Also it is robust to transformations, such as scaling, translation and rotation. ACC is simple and a low complexity feature extraction scheme, along with the L1 norm, it is effective in detecting multiple copy-move forgeries in same image.

References

[1] H. Farid, “A Survey of Image Forgery Detection,” Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, Mar. 2009.
[2] J. Fridrich, D. Soukal, and J. Luk´a˘s, “Detection of copy-move forgery in digital images,” in Proceedings of Digital Forensic Research Workshop,Aug. 2003.
[3] A. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Department of Computer Science, Dartmouth College, Tech. Rep. TR2004-515, 2004. [Online]. Available: www.cs.dartmouth.edu/farid/publications/tr04.html
[4] W. Luo, J. Huang, and G. Qiu, “Robust Detection of Region-Duplication Forgery in Digital Images,” in International Conference on Pattern Recognition, vol. 4, , pp. 746–749. Aug. 2006
[5] G. Li, Q. Wu, D. Tu, and S. Sun, “A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD,” in IEEE International Conference on Multimedia and Expo, , pp. 1750–1753. Jul. 2007

[6] H. Huang, W. Guo, and Y. Zhang, "Detection of Copy-Move Forgery in Digital Images Using SIFT Algorithm," in Pacific-Asia Workshop on Computational Intelligence and Industrial Application, vol. 2, , pp. 272–276. Dec. 2008
[7] Jing Huang, Kumar S.R, Mitra, M.,Wei-Jing Zhu and Zabih, R. "Image Indexing Using Color Correlograms" in IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1997.
[8] Tungkasthan, A., Intarasema, S. ,and Premchaiswadi, W. "Spatial Color Indexing using ACC Algorithm" in Seventh International Conference on ICT and Knowledge Engineering, ,pp. 113 – 117,2009
[9] S. Bayram, H. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in IEEE International Conference on Acoustics, Speech, and Signal Processing, Apr. 2009, pp. 1053–1056.
[10] B. L. Shivakumar and S. Baboo, "Detection of Region Duplication Forgery in Digital Images Using SURF," International Journal of Computer Science Issues, vol. 8, no. 4, pp. 199–205, 2011.
[11] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra. "A SIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE Transactions on Information Forensics and Security, vol. 6, iss. 3, pp. 1099-1110, 2011.
[12] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches" in IEEE Transactions On Information Forensics And Security,pp. 1841-1854, 2012.
[13] Jing Ming Guo, Yun-Fu Liu, Zong-Jhe Wu, "Duplication forgery detection using improved DAISY descriptor " in Elsevier International Journal - Expert Systems with Applications 40 (2013) pp.707–714
[14] Leida Li, Shushang Zhu, Hancheng Wu, Xiaoyue, "Detecting copy-move forgery under affine transforms for image forensics" in Computers & Electrical Engineering, Elsevier Ltd, Volume: 40, Issue: 6, pp. 1951-1962, 2014
[15] Chen-Ming Hsu , Chungli, Taiwan, Jen-Chun Lee and Wei-Kuei Chen, "An Efficient Detection Algorithm for Copy-Move Forgery" in 10th sia Joint Conference on Information Security, pp 33-36, May 2015
[16] Cheng-Shian Lin , Chien-Chang Chen and Yi-Cheng Chang "An Efficiency Enhanced Cluster Expanding Block Algorithm for Copy-Move Forgery Detection" in International Conference on Intelligent Networking and Collaborative Systems (INCOS),Sept 2015 , pp. 228 – 231
[17] Tralic D., Zupancic I., Grgic S., Grgic M., "CoMoFoD - New Database for Copy-Move Forgery Detection", in Proc. 55th International Symposium ELMAR-2013, pp. 49-54, September 2013