DCT-PCA Based Method for Copy-Move Forgery Detection

Kumar Sunil[1], Desai Jagan[1], and Mukherjee Shaktidev[2]

[1] Faculty of Engineering & Technology,
Mody Institute of Technology & Science, Laxmangarh, India
skvasistha@ieee.org, jagandesai@yahoo.com
[2] Moradabad Institute of Technology, Moradabad, India
mukherjee.shaktidev@gmail.com

Abstract. Copy move forgery detection is emerging as one of the hot research topic among researchers in the area of image forensics. There are many techniques suggested to detect such type of tampering with the original image but, many issues still remained either unsolved or there is a lot of scope for performance improvement. The most commonly used algorithm to detect such type of tampering is block matching algorithm. Robustness against post processing operations and the time taken by the detection techniques are few of the major challenges. Change of intensity of the copy moved part is one of the post processing operations that may be employed by the attacker to evade the image forgery detection methods. This is successfully addressed in the proposed algorithm. Discrete cosine transform and principal component analysis have been used to represent and compress the feature vector of overlapping blocks respectively. Features , invariant to local change of intensity are created using down sampling of low frequency DCT coefficients.

Keywords: Blind forgery detection techniques, image forensics, intensity invariant forgery detection.

1 Introduction

Image forgery now a days is a challenge for the authorities relying on the visual information. In the early days, when computers were not available easily for everybody, there was a tendency to believe what we see. But manipulation of the digital images has become very easy with the availability of fastly improving hardware and sophisticated software. The visual document has to be authenticated before drawing any conclusion based upon it. So, detecting the manipulations in digital images is not only important but also necessary. Image forgery detection techniques may be classified as per Figure 1. A few such techniques are listed in [1].Active forgery detection methods like watermarks are already being used to protect digital images. But using such techniques has their limitations, as the source of capturing the images may not be controlled and authenticated always. Blind forgery detection is used to detect manipulations in the absence of active techniques. Digital image forgery may

S.C. Satapathy et al. (eds.), *ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of CSI - Volume II*, Advances in Intelligent Systems and Computing 249,
DOI: 10.1007/978-3-319-03095-1_62, © Springer International Publishing Switzerland 2014

be performed in many different ways [2].Out of these the commonly used method is copy move forgery, where parts of the same image are used either to hide some other parts of image or to amplify some fact. In case of natural images, existence of two same regions is not common. So, the similarity created as a result of copy move attack is exploited to detect copy move forgery. One of the most frequently used method for detecting such type of forgery is to use block matching algorithm [3][4].In the block matching algorithm the image is divided into overlapping blocks and the blocks are matched to find the duplicated regions. Many people have used it to find duplication of the region with different features representing a block of image [5][6]. There may be some post processes performed, like edge smoothing, blurring, noise adding and change of intensity, but even after the post processing operations almost identical regions created in the manipulated image.

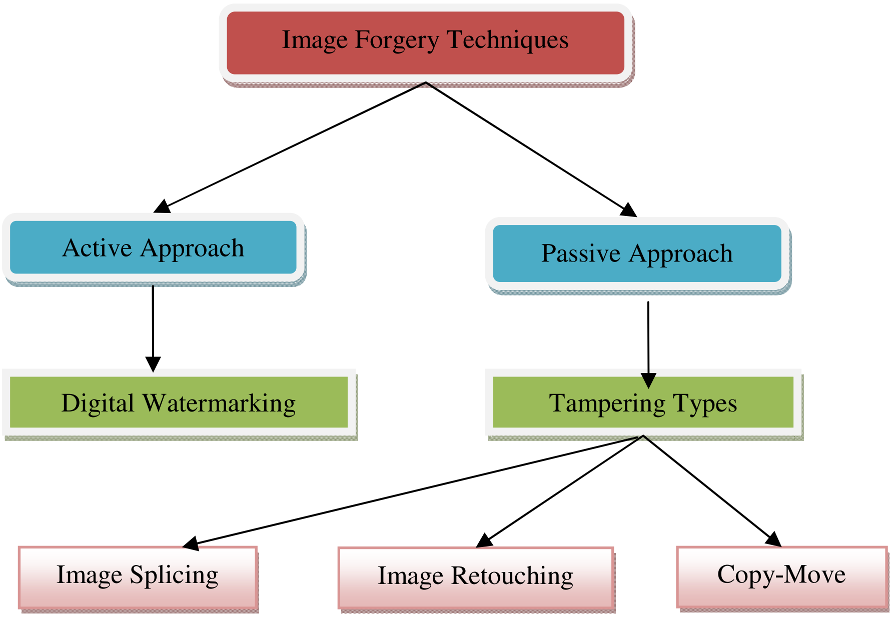

Fig. 1. Classification of image forgery

2 Related Work

One of the landmark method for copy move forgery detection was suggested by Fridrich[3]. He suggested a block matching forgery detection method based on discrete cosine transform (DCT). Popescu proposed a similar method [4], which used principal component analysis (PCA) instead of DCT. DCT is supposed to be a good feature for digital images and has been utilized by [7] [8] [9].In [7], the authors proposed a method to make the similarity criteria more robust by calculating the component ratio for matching the feature vectors. In [8], effort has been made to reduce time complexity by applying DWT. In [9], both low and high frequency bands of DyWT are used to achieve robustness. When the length of feature vector is large, handling the DCT coefficients become more difficult. In such cases the lower frequency coefficients are only retained to curtail the number of coefficients. This process has been done manually and it is difficult to suggest a threshold for faithful representation of feature vector. PCA is good at reducing the dimensionality of the data and has been utilized in [4].The method using PCA is quite fast but lack robustness. There are some methods that can detect more sophisticated post-processing, like Mahdian's work [10] can detect the duplicated region even the copy-move region been blurred or added noise. However, some issues have been reported by the researchers [10][11] in the algorithms, like the time taken by the algorithm to detect the matching blocks. In the present paper efforts have been made to address the issue of robustness in the form of intensity invariance with good time complexity and the experimental results have shown that the performance of the method is good with improved robustness.

3 Proposed Method

The proposed method addresses a particular type of robustness against change of intensity of the copy moved region. The manipulator may increase or decrease the brightness of the copy moved region to fit in some other part of the image. In such cases the DC component of the DCT feature vector will be significantly different even for the copy moved regions and evade the existing DCT based forgery detection techniques. However other components in the feature vector will be same. So the low frequency coefficients have been down sampled using very large quantization factor. The updated feature vector is invariant to the intensity variations of the copy moved part. However, it is assumed that the intensity variation will be uniform at least over the single block. It has been proved that PCA can be used directly in DCT domain [12]. So PCA is applied to reduce the dimensionality of the feature vector. To further reduce the time taken by the algorithm DCT coefficients are calculated in parallel for the overlapping blocks. Also to make the final decision process efficient morphological operations are used to remove the isolated pixels and only retain the significant connected components. The algorithm structure is as follows:

(1) The input image is a gray scale image I of the size m x n. If it is a color image, it can be converted to a grayscale image using the standard formula I = 0.299R + 0.587G + 0.114B.

(2) A fixed-sized b x b window is slided one pixel along from the upper left corner to the button right, dividing I into (m-b +1)(n-b +1) blocks.

(3) For each block, apply DCT and reshape the b x b coefficient matrix to a row vector in zigzag order.

(4) Down sample the low frequency coefficients by using large quantization factor such that the DC component is very close to zero.

(4) Do PCA to the array of row vector to reduce the dimensionality and result a m-b +1)(n-b +1) x qb^2 matrix A.

(4) Use lexicographical sorting on A to sort the row vectors according to their similarity.
(5) For each row a_i in A, test its neighboring rows a_j which satisfy the threshold condition of minimum distance between duplicated rows (N_n).
(6) If the distance between similar blocks (N_d) is greater than block size, then a shift vector ‘s’ is calculated and normalized.
$s= (s_1, s_2) = (i_1-j_1, i_2-j_2)$, where (i_1, j_1) and $(i_{2,}, j_2)$ are similar block coordinates . Then the shift vector’s existing frequency is increased by one.
(7) The frequency matrix is sorted and third value is taken to be threshold frequency (N_f). Also it should be more than b x b.
(8) For all the blocks having shift value greater than the threshold mark (N_f) the block points in the dark image are registered as white points.
(9) Finally apply morphological operations to remove the isolated points and show the binary image as output representing copy moves regions with white regions.

4 Experimental Setup and Results

To check the performance of the proposed algorithm, different sized images are taken. The image dataset contains 90 images with varying texture and intensity distributions. The dataset includes some images created specifically for the experiment and some from the dataset [13] with intensity variation of the copy moved part ranging from -50 to +80. The intensity of copy move part is varied using Photoshop. The algorithm is implemented in MATLAB 2012a on the machine equipped with Intel i5 1.8 GHz Core 2 duo processor and 8GB DDR3RAM. N_n (number of rows selected for potential similar block vector) is selected 30.The number of components retained in the feature vector after applying PCA are ¼ of the original components (q=0.25). The value of q is set experimentally. Lower values have shown adverse effect on the efficiency of the algorithm.

4.1 Visual Results

Fig. 2(a). Original image barrier.bmp

Fig. 2(b). Tampered image without any intensity variation of copy moved region

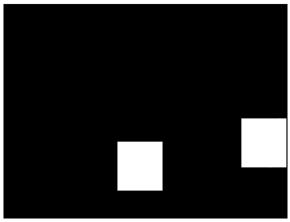

Fig. 2(c). Detection result of proposed method

Fig. 3(a). Original image barrier.bmp

Fig. 3(b). Tampered image with intensity variation of (+10) in copy moved region

Fig. 3(c). Detection result of proposed method

Fig. 4(a). Original image logo.bmp

Fig. 4(b). Tampered image with intensity variation of (+80) in copy moved region

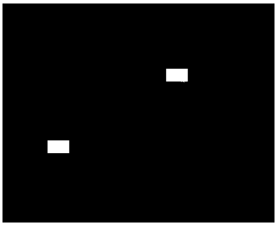

Fig. 4(c). Detection result of proposed method

Fig. 5(a). Original image cap.bmp

Fig. 5(b). Tampered image with intensity variation of (-50) in copy moved region

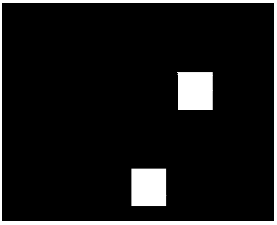

Fig. 5(c). Detection result of proposed method

Fig. 6(a). Original image pen.bmp

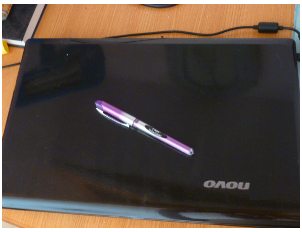

Fig. 6(b). Tampered image with intensity variation of (-2) in copy moved region

Fig. 6(c). Detection result of proposed method

4.2 Comparison with the Method Suggested in [3]

Table 1. Performance comparision

Image name/Image size	Intensity variation in the copy moved part	Block size	Execution Time in Seconds		Copy Move attack detected successfully	
			Method in [3]	Proposed method	Method in [3]	Proposed method
barrier.bmp (800x600)	0	8x8	92.3	71.72	yes	yes
	+10	8x8	96.03	79.85	no	no
	+10	4x4	93.98	72.4	no	yes
logo.bmp (640x480)	+50	8x8	58.86	52.11	no	yes
	+80	8x8	59.65	53.44	no	yes
	-10	8x8	59.12	52.71	no	yes
cap.bmp (640x480)	-50	8x8	61.23	53.43	no	yes
	+20	8x8	59.29	51.9	no	yes
pen.bmp (640x480)	-2	8x8	59.24	53.65	no	yes

4.3 Observations

Figure 2-6 show the visual results of the proposed algorithm on some selected images from the dataset. Table I provides comparative analysis for the images shown in figure 2-6.The method in [3] fails to detect the manipulation even with slight change in the intensity of the copied moved part. The default block size of 8x8 works well in 95% of

trials, however when the copy moved region is significantly smaller, then the block size has to be changed to 4x4 as shown in Figure 3. The proposed method has successfully detected the copy moved part with intensity changes. Also the time taken by the method is less comparable to [3].

5 Conclusion and Future Work

Another post processing technique has been introduced as change of intensity of the copy moved region. The proposed method successfully detects copy move attack in the presence of such post processing technique. The attacker may perform this operation to fit in some other part of the image to deceive the available DCT based methods. However, the feature vector may be enhanced to include the other types of invariance in a single method in future.

References

[1] Lin, E., Podilchuk, C., Delp, E.: Detection of image alterations using semi-fragile watermarks. In: Proc. SPIE, Security and Watermarking of Multimedia Contens II, vol. 3971, pp. 52–163 (2000)

[2] Birajdar, G.K., Mankar, V.H.: Digital image forgery detection using passive techniques: A survey. Digital Investigation, 1–20 (2013)

[3] Fridrich, J., Soukalm, D., Lukáš, J.: Detection of copy-move forgery in digital images. In: Digital Forensic Research Workshop, Cleveland, OH, pp. 19–23 (2003)

[4] Popescu, A.C., Farid, H.: Exposing Digital Forgeries By Detecting Duplicated Image Regions. Tech. Rep. TR2004-515, Dartmouth College (2004)

[5] Kumar, S., Das, P.K., Mukherjee, S.: Copy-Move Forgery Detection in Digital Images: Progress and Challenges. International Journal on Computer Science and Engineering 3(2), 653–663 (2011)

[6] Al-Qershi, O.M., Khoo, B.E.: Passive detection of copy-move forgery in digital images: State-of-the-art. Forensic Science International 231(1), 284–295 (2013)

[7] Huang, Y., Lu, W., Sun, W., Long, D.: Improved DCT-based detection of copy-move forgery in images. Forensic Science International 206(1), 178–184 (2011)

[8] Ghorbani, M., Firouzmand, M., Faraahi, A.: DWT-DCT (QCD) based copy-move image forgery detection. In: 2011 18th International Conference on Systems, Signals and Image Processing (IWSSIP), pp. 1–4 (2011)

[9] Muhammad, G., Hussain, M., Mirza, A.M., Bebis, G.: Dyadic wavelets and dct based blind copy-move image forgery detection. In: IET Conference on Image Processing (IPR 2012), pp. 1–6 (2012)

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

[11] Bacchuwar, K.S., Ramakrishnan, K.: A Jump Patch-Block Match Algorithm for Multiple Forgery Detection. In: International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing, pp. 723–728 (2013)

[12] Chen, W., Er, M.J., Wu, S.: PCA and LDA in DCT domain. Pattern Recognition Letters 26(15), 2474–2482 (2005)

[13] Christlein, V., Riess, C., Jordan, J., Riess, C., Angelopoulou, E.: An Evaluation of Popular Copy-Move Forgery Detection Approaches. IEEE Transactions on Information Forensics and Security 7(6), 1841–1854 (2012)