Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, No.4, April : 2023

IMAGE FORENSIC FOR DIGITAL IMAGE COPY MOVE FORGERY DETECTION

Mr A.D.Sivarama Kumar, Assistant Professor,
Pagadala Haritha, Kankara Naga jyothi, Miriyala Hari Krishna B.Tech Student
Department Of CSE,SVR Engineering College,Nandyal

ABSTRACT:
Due to the powerful image editing tools images are open to several manipulations; therefore, their authenticity is becoming questionable especially when images have influential power, for example, in a court of law, news reports, and insurance claims. Image forensic techniques determine the integrity of images by applying various high-tech mechanisms developed in the literature. In this paper, the images are analyzed for a particular type of forgery where a region of an image is copied and pasted onto the same image to create a duplication or to conceal some existing objects. To detect the copy-move forgery attack, images are first divided into overlapping square blocks and DCT components are adopted as the block representations. Due to the high dimensional nature of the feature space, Gaussian RBF kernel PCA is applied to achieve the reduced dimensional feature vector representation that also improved the efficiency during the feature matching. Extensive experiments are performed to evaluate the proposed method in comparison to state of the art. The experimental results reveal that the proposed technique precisely determines the copy-move forgery even when the images are contaminated with blurring, noise, and compression and can effectively detect multiple copy-move forgeries. Hence, the proposed technique provides a computationally efficient and reliable way of copy-move forgery detection that increases the credibility of images in evidence centered applications.

I.INTRODUCTION
With the advancements in imaging technologies, the digital images are becoming a concrete information source. Mean-while, a large variety of image editing tools have placed the authenticity of images at risk. The ambition behind the image content forgery is to perform the manipulations in a way, making them hard to reveal through the naked eye, and use these creations for malicious purposes. For instance, in 2001, after the 9/11 incident, several videos of Osama bin Laden over the social media were found counterfeited through the forensic analysis [1]. In the same way, in 2007, an image of tiger in forest forced the people to believe in the existence of tigers in the Shanxi province of China. The forensic analysis,however, proved the tiger to be a “paper tiger” [2]. Similarly, in 2008, an official image of four Iranian ballistic missiles was found to be doctored, as one missile was revealed to be duplicated [3]. Hence, the famous saying “seeing is believing” [4, 5] is no longer effective. Therefore, ways that can ensure the integrity of the images especially in the evidence centered applications are required.
In recent years, an exciting field, digital image forensics, has emerged which finds the evidence of forgeries in digital images [6]. The primary focus of the digital image forensics is to investigate the images for the presence of forgery by applying either the active or the passive (blind) techniques[2].The active techniques such as watermarking [7] and digital signatures [6] depend on the information embedded

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, No.4, April : 2023

(a) The original images (b) The copy-move forged images
Figure 1: An example of copy-move forgery

a priori in the images. However, the unavailability of the information may limit the application of active techniques in practice [8]. Thus, passive techniques are used to authenticate the images that do not require any prior information about them [8–10].

Images are usually manipulated in two ways such as image splicing and region duplication through copy-move forgery. In image splicing, regions from multiple images are used to create a forged image. However, in copy-move forgery, image regions are copied and pasted onto the same image to conceal or increase some important content in the pictured image. As copied regions are apparently identical with compatible com-ponents (i.e., color and noise), it becomes a challenging task to differentiate the tempered regions from authentic regions. Furthermore, a counterfeiter applies various postprocessing operations such as blurring, edge smoothing, and noise to remove the visual traces of image forgeries. An example of copy-move forgery is shown in Figure 1.

In the present work copy-move forgery detection is addressed through the discrete cosine transform (DCT) and Gaussian RBF kernel PCA that are used to investigate the similarity between duplicated regions. The benefits of our algorithm compared against several existing CMFD methods are

(i) utilization of the lower length of feature vectors;
(ii) lower computational cost;
(iii) robustness against various postprocessing operations over the forged regions;
(iv) ability to detect multiple copy-move forgeries.

The rest of the paper is organized as follows: Section 2 presents the related work regarding copy-move forgery detec-tion (CMFD). Section 3 presents the details of proposed method. Experimental results are presented in Section 4.Finally, the conclusions are drawn in Section 5.

II.LITERATURE SURVEY

Various CMFD techniques have been proposed so far to effectively address the region duplication problem. In this regard, the research is intended towards the representation of image regions in a more powerful way to accurately detect the duplicated regions. In [11], Fridrich et al. for the f irst time presented the copy-move forgery detection technique using DCT on small overlapping blocks. The feature vectors are formed using DCT coefficients. The similarity between blocks is analyzed after sorting the feature vectors lexicographically. In [13], image blocks are represented through principal component analysis (PCA). Exploiting one of the features of PCA, the authors used about half of the number of features utilized by [11]. It makes this technique effective but failed to detect copy-move forgery with rotation. In [15], a sorted neighborhood technique based on Discreet Wavelet Trans-form

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, No.4, April : 2023

(DWT) is proposed. The image is decomposed into four subbands and applied the Singular Value Decomposition (SVD) on low frequency components for getting the feature vector. The technique is robust to JPEG compression up to the quality level 70 only. In [16], a technique based on blur moment invariants up to seventh order for extracting the block features and kd-tree matching is introduced. In [12], the application of scaling and rotation invariant Fourier-Mellin Transform (FMT) is suggested in combination with bloom filters on the image blocks for detecting the image forgery. In [14], an improved DCT-based technique is proposed by introducing a truncating process to reduce the dimension of feature vector for forgery detection. In [17], a solution through DCT and SVD is proposed for detecting image forgeries. The algorithm is shown to be robust against compression, noise, and blurring but fails when images are even slightly rotated. In [18], an efficient expanding block technique based on direct block comparison is proposed. In [19], circle block extraction is performed and the fea-tures are obtained through rotation invariant uniform local binary patterns (LBP). The technique is robust to blurring, additive noise, compression, flipping, and rotation. However, this technique failed to detect forged regions rotated with arbitrary angles. In [20], the authors employed a new pow-erful set of keypoint-based features called MIFT for finding similar regions in the images. In [21], the authors extracted feature vectors from circular blocks using polar harmonic transform (PHT) for detecting image forgeries. In [22], an adaptive similarity threshold based scheme is presented in the block matching stage. The detection of forged regions is determined using thresholds proportional to blocks standard deviations. In [23], a method using the Histogram of Oriented Gradients (HOG) is suggested to detect the copy-move forged regions. In [24], the multiscale Weber's law descriptor (multi-WLD) and multiscale LBP features are extracted for image splicing and copy-move forgery detection from chrominance components. The authors employed SVM for classifying an image as authentic or forged.

III.PROPOSED METHOD

In this paper, copy-move forgery detection is performed through the DCT and Gaussian RBF kernel PCA using the squared blocks. The reason to use the DCT for block rep-resentation is the robustness against several postprocessing operations, for example, compression, blurring, scaling, and noise [25], as it is a common practice in image forgery that the counterfeited images always undergo various postpro-cessing operations. Hence, it makes the forgery detection very difficult. Although the DCT is effective against mentioned transformations, still there are situations where the block representations through DCT will be nominal; for example, if rotation operation is applied over the forged regions, the DCT representations results are affected as well. To overcome this limitation we apply Gaussian RBF kernel PCA over the DCT frequency coefficients due to their rotation invariant nature compared against PCA [25]. Another motivation to use kernel PCA with DCT is the nonlinear nature of RBF kernel PCA and linear nature of DCT. Hence, it makes the feature representation more diverse and also appears as a better choice compared to PCA that is also linear in nature like DCT. Gaussian RBF kernels have some other advantages such as having fewer hyperparameters; hence, they are numerically less difficult as kernel values are bounded between 0 and1.

3.1. Framework of the Proposed Algorithm. The discussion above draws forth the framework of CMFD that is described in Figure 2. The steps of the proposed CMFD technique are given as follows:

(1) Dividing the grayscale image into fixed sized overlap-ping blocks.
(2) Applying DCT to each extracted block.
(3) Extracting Gaussian RBF kernel PCA-based features from each DCT square block.
(4) Matching similar block pairs.
(5) Removing the isolated block and output the dupli-cated regionS.

IV. CONCLUSION

In this paper, we focused on finding the ways through which we can assure the detection of copy-move forgery in digital images. The main consideration of this paper was to reduce the dimension of the feature length and find the forged objects in the suspected image. Therefore, we have applied DCT and kernel PCA for feature extraction which considers the identical objects found in the forged image. Furthermore, this technique does not require any prior information embedded into the image and works inthe absence of digital signature or digital watermark. From the results, a conclusion can be drawn which is that the proposed technique not only effectively detects multiple copy-move forgeries and precisely locates the forged areas but also has nice robustness to postprocessing operations such as Gaussian blurring, AWGN, and compression. Moreover, comparing the detection performance of the proposed technique with existing standard copy-move forgery systems [11–14], the results of our technique are reasonably good in terms of average TPR and FPR.

REFERENCE

[1] N. Krawetz, “A pictures worth digital image analysis and forensics,” Black Hat Briefings, 2007.

[2] S. Lian and Y. Zhang, “Multimedia forensics for detecting forgeries,” in Handbook of Information and Communication Security, pp. 809–828, Springer, New York, NY, USA, 2010.

[3] Y. Li, “Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching,” Forensic Science International, vol. 224, no. 1–3, pp. 59–67, 2013.

[4] H. Farid, “Digital doctoring: how to tell the real from the fake,” Significance, vol. 3, no. 4, pp. 162–166, 2006.

[5] B. B. Zhu, M. D. Swanson, and A. H. Tewf ik, “When seeing isn’t believing [multimedia authentication technologies],” IEEE Signal Processing Magazine, vol. 21, no. 2, pp. 40–49, 2004.

[6] H. Farid, “Image forgery detection: a survey,” IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16–25, 2009.

[7] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, Burling-ton, Mass, USA, 2007.

[8] M. A. Qureshi and M. Deriche, “A bibliography of pixel-based blind image forgery detection techniques,” Signal Processing: Image Communication, vol. 39, pp. 46–74, 2015.

[9] T. Qazi, K. Hayat, S. U. Khan et al., “Survey on blind image forgery detection,” IET Image Processing, vol. 7, no. 7, pp. 660– 670, 2013.

[10] T. Mahmood, T. Nawaz, R. Ashraf et al., “A survey on block based copy move image forgery detection techniques,” in Proceedings of the International Conference on Emerging Tech-nologies (ICET ’15), pp. 1–6, Peshawar, Pakistan, December 2015.

[11] J. Fridrich, D. Soukal, and J. Luka´˘s, “Detection of copy-move forgery in digital images,” in Proceedings of Digital Forensic Research Workshop, Cleveland, Ohio, USA, August 2003.

[12] S. Bayram, H. T. Sencar, and N. Memon, “An efficient and robust method for detecting copy-move forgery,” in Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP ’09), pp. 1053–1056, April 2009.

[13] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Tech. Rep. TR2004-515, Dartmouth College, Hanover, NH, USA, 2004.

[14] Y. Huang, W. Lu, W. Sun, and D. Long, “Improved DCT-based detection of copy-move forgery in images,” Forensic Science International, vol. 206, no. 1–3, pp. 178–184, 2011.

[15] 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 Proceedings of IEEE International Conference on Multimedia and Expo (ICME ’07), pp. 1750–1753, IEEE, Beijing, China, 2007.

[16] B. Mahdian and S. Saic, “Detection of copy-move forgery using a method based on blur moment invariants,” Forensic Science International, vol. 171, no. 2-3, pp. 180–189, 2007.

[17] J. Zhao and J. Guo, “Passive forensics for copy-move image forgery using a method based on DCT and SVD,” Forensic Science International, vol. 233, no. 1–3, pp. 158–166, 2013.