JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DETECTING DIGITAL IMAGE COPY-MOVE FORGERY THROUGH ADVANCED IMAGE FORENSICS

[1] Dr. Jaynesh H. Desai

[1]Assistant Professor, Bhagwan Mahavir College of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India

Abstract : In light of the widespread use of strong image manipulation tools, the authenticity of photos has been a subject of increasing question. This is especially true in situations where the impact of the images is significant, such as in the context of legal processes, the distribution of news, and insurance claims. The purpose of this study is to investigate the field of picture forensics by utilizing sophisticated methods derived from the existing body of research in order to determine the authenticity of photos that have been subjected to possible modifications. The focus is on a particular type of forgery known as the copy-move attack. This type of forgery involves the replication and transposition of a portion of an image within the same image. The purpose of this is to either generate duplicates or to disguise elements that are already present. In order to uncover instances of this counterfeit, a methodical methodology is utilized. This method involves the segmentation of images into square blocks that overlap one another, and the Discrete Cosine Transform (DCT) components are utilized as representations for these blocks. Gaussian Radial Basis Function (RBF) kernel Principal Component Analysis (PCA) is applied in order to achieve a reduced-dimensional feature vector representation. This is done in recognition of the challenges that are posed by the high dimensionality of the feature space. As a result, the efficiency of the subsequent feature matching stage is improved. Experiments of a rigorous nature are carried out in order to evaluate the effectiveness of the suggested method by contrasting it with the most advanced techniques currently available. Even in situations when photos are contaminated with blurring, noise, and compression, the results of these trials indicate the precision of the proposed technique in recognizing copy-move forgeries. This is the case especially in situations where the images are compressed. Particularly noteworthy is the fact that the method has a commendable capacity to identify several instances of copy-move forgeries. Consequently, the strategy that was provided emerges as a method that is both computationally efficient and reliable for detecting copy-move fraud. This, in turn, strengthens the credibility of images in applications that are oriented around evidentiary objectives. Its ability to work consistently under a wide range of settings demonstrates that it has the potential to be an invaluable instrument for maintaining the authenticity of visual information in an era that is characterized by the widespread utilization of sophisticated picture altering technologies.

IndexTerms **- CMFD, DCT, Image Forgery, PCA.**

I. INTRODUCTION

As imaging technology continues to progress, digital images are increasingly becoming a source of information that can be backed up by concrete evidence. In the meantime, the authenticity of photos has been put in jeopardy by a wide range of image manipulation programs. The goal of the image content forgeries is to be able to perform the modifications in such a way that they are difficult to detect with the naked eye, and then to exploit these creations for harmful purposes. Through the use of forensic analysis, for example, it was discovered that multiple videos of Osama bin Laden that were shared on social media in the year 2001, following the events of September 11, 2001, were stolen [1]. In the same manner, in 2007, a photograph of a tiger in the forest convinced the inhabitants of the Shanxi province of China to believe that tigers actually live in the region. Nevertheless, the forensic investigation proved that the tiger in question was a "paper tiger" [2]. In a similar manner, in 2008, it was discovered that an official photograph of four Iranian ballistic missiles had been altered, and it was discovered that one of the missiles had been copied [3]. Consequently, the well-known proverb "seeing is believing" [4, 5] is no longer applicable in this context. Since this is the case, it is necessary to have methods that can guarantee the authenticity of the photographs, particularly in applications that are evidence-based.

Digital image forensics is a fascinating topic that has evolved in recent years. Its primary objective is to identify and locate evidence of forgeries within digital photographs [6]. One of the basic goals of digital image forensics is to study digital photographs to determine whether or not they include any instances of forgery. This can be accomplished through the use of either active or passive (blind) procedures [2]. Watermarking [7] and digital signatures [6] are examples of active approaches that are dependent on the information that is embedded in the document.

(a) The original images (b) The copy-move forged images

Figure 1: An example of copy-move forgery

It is possible that the application of active approaches in practice could be restricted due to the lack of availability of the information [8]. Therefore, passive procedures are utilized in order to authenticate the photographs, which do not necessitate any prior information regarding them [8–10].

Two methods are typically utilized in the process of image manipulation. These methods include image splicing and region duplication by copy-move forging. It is possible to produce a forged image using the process of image splicing by combining parts of multiple photographs. The copy-move forgery, on the other hand, involves copying and pasting image portions onto the same image in order to hide or amplify certain significant content that is present in the image that is being photographed. The process of distinguishing between tempered regions and legitimate regions gets more difficult due to the fact that copied regions appear to be identical with compatible components (i.e., color and noise). In addition, a counterfeiter will use a variety of postprocessing procedures, such as blurring, edge smoothing, and noise, in order to eliminate any visible signs of picture forgeries. Figure 1 illustrates an example of a copy-move fake that was committed.

In the current work, the detection of copy-move forgeries is addressed by employing the discrete cosine transform (DCT) and the Gaussian RBF kernel principal component analysis (PCA), both of which are utilized to explore the similarities between duplicated regions.

Compared to a number of other CMFD approaches that are already in use, the advantages of our algorithm are as follows:

1) The employment of feature vectors with a shorter length.
2) A reduced computational cost.
3) The capacity to detect numerous copy-move forgeries.
4) The robustness against various post-processing procedures over the forged regions; and
5) The ability to utilize the shorter length of feature vectors.

II. Literature Survey

In order to properly handle the issue of region duplication, a number of different CMFD approaches have been presented up until this point. Taking this into consideration, the research is geared toward the depiction of image regions in a more effective manner in order to reliably detect repeated parts. Using DCT on small overlapping blocks, Fridrich et al. introduced the copy-move forgery detection technique for the very first time in [11]. This research was published in the journal.

The DCT coefficients are utilized in the formation of the feature vectors. Immediately following the lexicographic sorting of the feature vectors, an analysis of the similarity between blocks is performed. PCA, which stands for principal component analysis, is used to represent image blocks in [13]. Utilizing one of the characteristics of principal component analysis (PCA), the authors utilized approximately half of the total number of features utilized by [11]. However, it was not successful in detecting copy-move fraud when rotation was used. This technique is effective regardless.

It is proposed in [15] that a sorted neighborhood technique that is based on the Discreet Wavelet Transform may be utilized. In order to obtain the feature vector, the image is first split into four subbands, and then the Singular Value Decomposition (SVD) algorithm is applied to the relatively low frequency components. The method is only capable of withstanding JPEG compression up to the quality level 70 quality level.

For the purpose of extracting block features and kd-tree matching, a method that is based on blur moment invariants up to seventh order is shown in [16]. When it comes to identifying instances of picture counterfeiting, the application of scaling and rotation invariant Fourier-Mellin Transform (FMT) in conjunction with bloom filters on the image blocks is recommended in reference [12].

An enhanced DCT-based technique is proposed in [14], which involves the implementation of a truncating procedure for the purpose of reducing the dimension of the feature vector for the purpose of forgery detection. Regarding the detection of image forgeries, a technique that utilizes DCT and SVD is proposed in reference [17]. The algorithm has been demonstrated to be resistant to compression, noise, and blurring; nevertheless, it is unable to function properly when images are rotated even slightly.

A method for enlarging blocks that is both effective and efficient and is based on direct block comparison is proposed in [18]. In [19], the process of circular block extraction is carried out, and the features are obtained by means of rotation-invariant uniform local binary patterns (LBP). Blurring, additive noise, compression, flipping, and rotation are all types of noise that can be handled by the approach.

On the other hand, this method was not successful in identifying faked sections that were rotated at arbitrary angles. For the purpose of locating regions in the photos that are similar to one another, the authors of [20] utilized a powerful new collection of keypoint-based features that they named MIFT. With the use of polar harmonic transform (PHT), the authors of [21] were able to extract feature vectors from circular blocks in order to identify instances of picture reproduction.

An adaptive similarity threshold-based technique is provided in [22] during the block matching step of the process mentioned above. A threshold that is proportionate to the standard deviations of the blocks is used to determine whether or not fabricated regions have been detected. A technique that makes use of the Histogram of Oriented Gradients (HOG) is proposed in [23] as a means of identifying sections that have been forged by copy-move. With the use of chrominance components, the multiscale Weber's law descriptor (multi-WLD) and multiscale

LBP features are retrieved for the purpose of detecting picture splicing and copy-move fraud in [24]. The authors used support vector machines (SVM) to determine if an image was genuine or fabricated.

III. Proposed Method

In the present study, the detection of copy-move forgery is carried out by utilizing the DCT and Gaussian RBF kernel PCA, with squared blocks serving as the data structure. It is a standard practice in the field of image forgery that counterfeited images always go through a variety of postprocessing processes. The reason for using the discrete cosine transform (DCT) for block representation is that it is resilient against a number of postprocessing techniques, such as compression, blurring, scaling, and noise [25]. Because of this, it is extremely challenging to detect instances of forgeries. Despite the fact that the DCT is effective against the transformations that have been stated, there are still circumstances in which the block representations obtained by the DCT will be nominal.

For instance, if the rotation operation is applied over the forged regions, the results of the DCT representations will also be altered. In order to circumvent this constraint, we use Gaussian RBF kernel PCA over the DCT frequency coefficients. This is because, in contrast to PCA, the DCT coefficients are rotation invariant [25]. In addition, the nonlinear character of RBF kernel PCA and the linear nature of DCT are two more reasons why kernel PCA should be used in conjunction with DCT. Additionally, it looks to be a better choice in comparison to principal component analysis (PCA), which is likewise linear in nature like DCT. This is because it makes the feature representation more diversified. Gaussian RBF kernels provide a number of additional benefits, including the fact that they have a smaller number of hyperparameters. As a result, they are numerically simpler because the values of the kernels are restricted to the range of 0 to 1.

Structure of the algorithm that is being proposed:

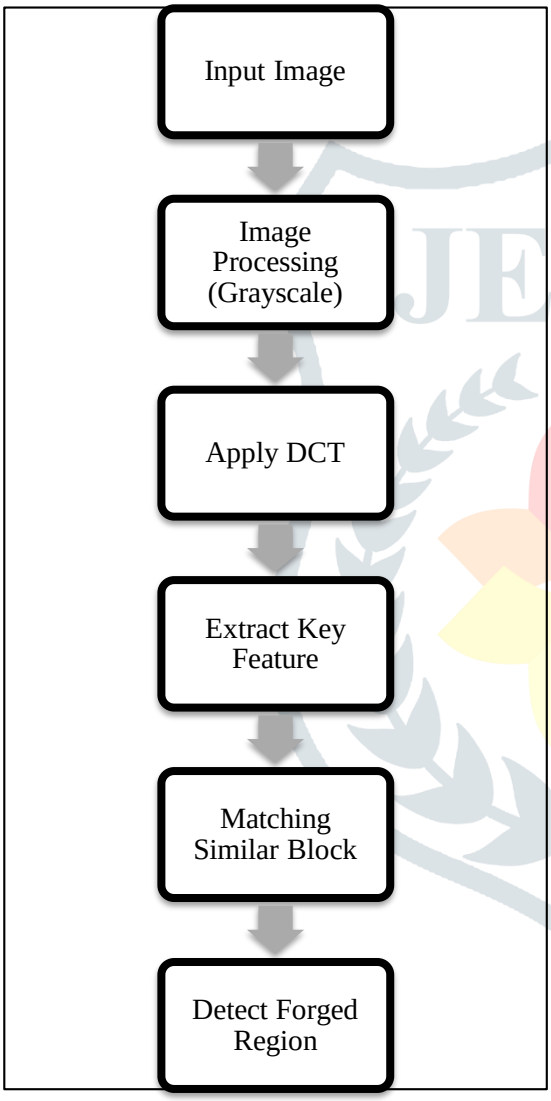

Figure 2: Proposed Framework for Image Forgery Detection

The framework of CMFD is brought to light by the topic that was presented earlier. The following is a list of the phases that make up the CMFD approach that has been proposed:

Step 1 – Input Image.

Step 2 – Dividing the grayscale image into fixed sized overlap-ping blocks.

Step 3 – Applying DCT to each extracted block.

Step 4 – Extracting Gaussian RBF kernel PCA-based features from each DCT square block.

Step 5 – Matching similar block pairs.

Step 6 – Removing the isolated block and output the duplicated regions.

IV. Conclusion

In the present study, our primary objective was to investigate the many methods that can be utilized to guarantee the detection of copy-move fraud in digital photographs. In this particular piece of writing, the primary focus was on minimizing the length of the feature dimensions and locating the fabricated things that were present in the suspicion image. In order to extract features, we have utilized DCT and kernel principal component analysis, both of which take into account the same objects that were discovered in the fabricated image. In addition, this method does not necessitate the incorporation of any prior information into the image, and it is effective even in the absence of a digital signature or digital watermark. A conclusion can be derived from the findings, which is that the proposed method not only successfully identifies multiple copy-move forgeries and exactly locates the areas that have been forged, but it also demonstrates a high level of robustness to postprocessing procedures such as Gaussian blurring, AWGN,

and compression. Furthermore, when the detection performance of the proposed technique is compared with the performance of current standard copy-move forgery systems [11–14], the findings of our technique are reasonably good in terms of the average TPR and FPR

REFERENCES

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

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

[19] 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.

[20] 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.

[21] 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.

[22] 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.