



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

IMAGE TAMPER DETECTION USING NON ALIGNMENT OF JPEG GRIDS

Jyoti¹, Mandeep Kaur²

University Institute of Engineering and Technology,
Panjab University, Sector 25, Chandigarh
INDIA

Abstract: Digital images have a very significant role in various fields like criminal and forensic investigations, medical imaging and journalism. But due to wide availability of powerful editing software, image forgery has become much easier. The aim of this paper is to detect the forgery on JPEG compressed images when splicing (copy-paste) will result in non alignment of JPEG grids. JPEG is widely used image compression format for digital images. Blocking artifacts introduced during this operation can be used as footprints to detect tampering. Detection is based on the fact that blocking artifact grids (BAG) usually mismatches after copy paste operation. An attempt is made to enlist all existing references related to block artifact grid extraction. These techniques have been designed to determine whether the content is authentic or modified without the knowledge of any prior information about the image under analysis and thus are passive in nature. Study of these methods will be helpful in finding out new algorithms to detect image tampering using grids inconsistency.

Keywords: Image forensics, passive – blind methods, JPEG artefacts, image tampering, BAG

I. Introduction

Digital images are powerful and widely used communication medium. Without a doubt, image authenticity is significant in many social areas. There are many methods of digital image tampering. . Therefore image forensic technologies are becoming increasingly important. The objective of this paper is to detect copy paste tampering on JPEG compressed images.

There are two types of image forgery detection techniques- one is active and other is passive. Digital Watermarking and Signature are two main active techniques. Watermarking assumes inserting of digital watermark at the source image and then verifying at the receiver end. Digital signature is encoded at the sender side and decoded at receiver end to ensure its integrity. Both these techniques are intrusive in nature and reduce the quality of image.

Passive techniques verify authenticity of images without using pre extracted information. These techniques do not need any prior information about the image and thus are defined as passive .These methods are also called blind methods. By word blind we refer to those methods using only the image function to perform the forgery detection task. Various artifacts are introduced by different blind methods that are categorized as Noise Inconsistency [1], blur [2], Sharpening [3] , lightening[4], projective geometry [5] and JPEG compression properties [6,7,8]. Such artifacts are used to detect whether images are forged or not.

In this paper, we focus on detection of JPEG image tampering using non-alignment of grids. In copy-paste tampering, copied image parts are placed at proper place to hide or add an object, so the BAG in the original image and the BAG in the target image are usually mismatched. The aim of this survey is to provide overview of the various proposed methods and highlight their advantages. This study will be helpful in designing new algorithms and also improve the existing methods.

The organization of the paper is as follows: The explanation of technique and the methods proposed to detect tampering based on this technique is given in Section II and III. Conclusion is given in section IV.

II. Different JPEG artifacts

JPEG standard is a widely used image format which is a lossy type of compression. Various artifacts are inserted into image during compression. Such artifacts can be exploited to find out whether the image has been tampered with or not. A copy paste tampering is carried out by taking a region from source image and pasted on target image to create a fake image .This study assumes that that either the source or the target images(or both) are JPEG compressed and fake image is saved in JPEG form after the manipulation.

To detect these artifacts different forensic tools are used .These tools are based on different methods like non grid alignment [9], double compression [10], JPEG ghost[11] , non aligned double JPEG compression[12].

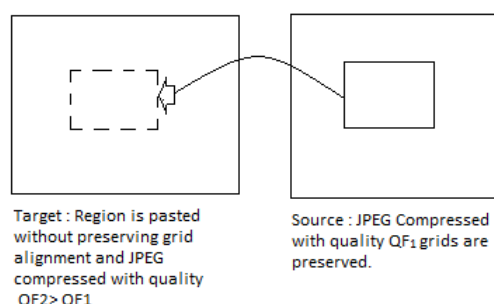
The focus of this paper is to detect forgery using grids inconsistency (non alignment of grids).JPEG divides an image into 8 by 8 pixel blocks to calculate DCT coefficients and perform quantization. This process of dividing

an image into blocks introduces horizontal and vertical breaks into image, which are called blocking artifact grid (BAG).

A. Detection of copy paste tampering using non alignment of grids

In this technique source image is JPEG compressed with quality QF_1 . A Region is cropped from source and pasted without preserving grid alignment on the target image which is again compressed with a quality factor $QF_2 > QF_1$. Detection relies on a statistical analysis of image blockiness. When used to detect cut & paste tampering, regions where JPEG grids are not aligned are considered as tampered [13].

Figure 1: Non alignment of grids



III. Existing techniques

Proposed methods of identifying tampering based on blocking artifact grid (BAG) are studied and discussed in this section. These methods use different image processing functions to detect the traces of tampering. Study of these methods will be helpful in finding out new algorithms to detect image blockiness caused by non alignment of grids.

Shuiming Ye and Ee-Chien Chang [14] proposed a method for checking quality inconsistencies in blocking artifacts by estimating quantization table based on power spectrum of the histogram of the DCT coefficients. In this method, first image is segmented and then blocking artifact consistency of these segments are checked. Suspicious area is selected for evaluation and the other areas are used to estimate the quantization table and the blocking artifact matrix (BAM) of the image is calculated based on the estimated table. If blocking artifact inconsistencies are detected, the image is suspicious.

In [15], LI Xiang-hua and Zhao Yuqian proposed a method in which tampered region is detected by computing the averaged sum of absolute difference (ASAD) images between the examined image and a resaved JPEG compressed image at different quality factors. This method further helps in detecting the tampered region of the copy-paste tampered image that is conducted between JPEG compressed images. It can also be used to detect tampered regions of small sizes. It also detects multiple tampered regions in one tampered image. Proposed method is related to the JPEG quality factor, it does not estimate the primary quantization matrix.

Dijana Tralic and Juraj Petrovic [16] discussed a method for detection of copy-paste manipulation on JPEG digital images. The detection method was implemented through extracting and analyzing blocking artifact grids (BAGs), introduced by block processing during JPEG compression. Extraction and analysis of the BAG mismatch can be used as an indication of image forgery whether copied area was taken from the same image or not. Also, this approach works efficiently for images where borders of copied area were smoothed by averaging values of neighboring pixels. This approach allowed effective detection of copied areas on doctored images. Another advantage of this method is its independence of the size of the copied area.

WeiQi Luo and Zhenhua Qu [17] develop the blocking artifact characteristics matrix (BACM) for images that are cropped from another JPEG image and re-saved as JPEG images. BACM exhibits a symmetrical shape for the original JPEG images and that this symmetrical property will be altered by cropping and recompression operations. This paper presents a method that exploits this property of the BACM for effectively detecting cropping and recompression.

In [18], Weihai Li and Yuan Yuan proposed a novel blind approach to detect copy-paste method in doctored JPEG images and it also locates the doctored area. The method works well even when a JPEG image is multi-compressed, by extract the DCT block artifact grid and detect mismatch of the grid.

Limited work has been done in this area. Study of this paper will be helpful for designing new methods to detect tampering based on Non alignment. Different tools to detect other JPEG artifacts like JPEG Ghost, double compression, non alignment of Grids can be applied also to make the detection process more robust. A. Double compression without preserving grid alignment (DC).

IV. Conclusion

Passive image forensics is a great challenge in image forensic techniques. Simple and effective methods are presented to check whether an image has experienced copy paste operations. If so, to further determine tampered region by block artifacts grid extraction.

BAG can be extracted through image quality inconsistencies based on blocking artifacts caused by JPEG compression. Future work could be done on discovery of other image quality inconsistency measure. Detection of doctored images has also important role due to many powerful image processing techniques that can be used for creation of such images. Future work will include testing approach for similar problems such as hiding objects by painting some image area.

JPEG image forensics approach is proposed to detect copy-paste forgery based on the check of block artifact grid mismatch. The approach works well even when a JPEG image is truncated or multi-compressed, by extract the DCT block artifact grid and detect mismatch of the grid. Future work of this algorithm is to improve the BAG marking algorithm to achieve clearer grid map and reduce computation load. Fusion of different tools should be applied to improve efficiency and accuracy of detecting.

References

- [1] B. Mahdian and S. Saic, "Using noise inconsistencies for blind image forensics," *Image and Vision. Computing.*, vol. 27, no. 10, pp. 1497–1503, Sep. 2009.
- [2] G. Cao, Y. Zhao, and R. Ni, "Edge-based Blur Metric for Tamper Detection," vol. 1, no. 1, pp. 20–27, 2010
- [3] Z. Y. and N. R. Cao Gang, "Detection Of Image Sharpening Based On Histogram Aberration And Ringing Artifacts," *IEEE ICME*, 2009, pp. 1026–1029.
- [4] H. Farid, M. Bravo, Image forensic analyses that elude the human visual system, in: *SPIE Symposium on Electronic Imaging*, San Jose, CA, 2010.
- [5] W. Zhang, X. Cao, Z. Feng, J. Zhang, P. Wang, Detecting photographic composites using two-view geometrical constraints, in: *IEEE International Conference on Multimedia and Expo*, 2009, pp. 1078–1081.
- [6] H. Farid, Exposing digital forgeries from jpeg ghosts, *IEEE Transactions on Information Forensics and Security* 1 (4) (2009) 154–160.
- [7] J. Fridrich, J. Lukas, Estimation of primary quantization matrix in double compressed jpeg images, in: *Proceedings of DFRWS*, vol. 2, Cleveland, OH, USA, August 2003.
- [8] B. Mahdian, S. Saic, Detecting double compressed jpeg images, in: *The 3rd International Conference on Imaging for Crime Detection and Prevention (ICDP-09)*, London, UK, December 2009.
- [9] Z. Lin, J. He, X. Tang, and C.-K. Tang, "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognition.*, vol. 42, no. 11, pp. 2492–2501, Nov. 2009.
- [10] W. Luo, Z. Qu, J. Huang, and G. Qiu "A novel method for detecting cropped and recompressed image block." *Acoustics, Speech and Signal Processing*, vol. 2, pp. II-217, 2007
- [11] H. Farid, "Exposing Digital Forgeries From JPEG Ghosts," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 1, pp. 154–160, Mar. 2009
- [12] T. Bianchi, and A. Piva. "Detection of non-aligned double JPEG compression with estimation of primary compression parameters." *Image Processing (ICIP)*, pp. 1929-1932, 2011.
- [13] W. Luo, Z. Qu, J. Huang, and G. Qiu "A novel method for detecting cropped and recompressed image block." *Acoustics, Speech and Signal Processing*, vol. 2, pp. II-217, 2007
- [14] S. Ye, Q. Sun, E. C. Chang, Detecting digital image forgeries by measuring inconsistencies of blocking artifact, in: *ICME*, 2007, pp. 12–15.
- [15] Shih, F. Y., and Y. Q. Shi. "Passive detection of copy-paste forgery between JPEG images." *Journal of Central South University* 19.10 (2012): 2839-2851.
- [16] Tralic, Dijana, Juraj Petrovic, and Sonja Grgic. "JPEG image tampering detection using blocking artifacts." *Systems, Signals and Image Processing (IWSSIP)*, 2012 19th International Conference on. IEEE, 2012
- [17] Luo, Weiqi, et al. "A novel method for detecting cropped and recompressed image block." *Acoustics, Speech and Signal Processing*, 2007. ICASSP 2007. IEEE International
- [18] W. Li, Weihai, Yuan Yuan, and Nenghai Yu. "Detecting copy-paste forgery of jpeg image via block artifact grid extraction." *International Workshop on Local and Non-Local Approximation in Image Processing*. 2008.