International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 4, April 2014 ISSN 2319 - 4847

Image Tamper Detection based on JPEG Artifacts

Mandeep kaur, Jyoti and Prakriti

University Institute of Engineering and Technology,
Panjab University, Chandigarh, India.

Abstract

Digital images have a very significant role in various fields like medical imaging, journalism, criminal and forensic investigations. But the easy availability of photo editing software and tools has made the process of verifying the authenticity and integrity of digital images extremely difficult. Image forensics, which uses passive-blind methods to detect image forgery, has become a hot research field. As compared to watermarks and digital signatures which are intrusive in nature, image forensic techniques uses simple image functions to detect certain footprints left by the tampering operations that are not visible by naked eye. The focus of this paper is to study the various footprints related to JPEG artifacts that are introduced in an image while performing cut & paste (splicing) forgery. Since JPEG is a widely used compression format for storage and transmission over internet, it will be applicable in a scenario where either source or target images are JPEG compressed or the image undergoes compression after splicing is performed. An attempt is made to categorize the various artifacts and present an overview of various blind methods proposed to detect such JPEG related tampering traces. This study will be helpful in developing new image forensic methods/tools to detect such kind of tampering and also improving the robustness and FPR of current tamper detection methods.

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

1. INTRODUCTION

Trustworthiness of digital images has a key role in many fields such as forensic and criminal investigation, intelligence services, insurance processing, medical imaging, journalism etc. Modifying a digital image without any obvious traces is not a difficult task now with the sophisticated computer graphics algorithms and image editing software available, such as Adobe Photoshop, GIMP, etc. Image forgery detection techniques are therefore needed to verify the integrity and authenticity of the digital images.

Image forgery detection techniques are broadly categorized as - *active and passive*. Active approach uses intrusive methods like watermarks and digital signature. These methods are non blind and can also deteriorate image quality. Passive techniques verify authenticity of images without using pre-extracted or pre-embedded information. Popularly known as *blind methods* as the presence of original image is not needed to verify the authenticity of a image and therefore has applications in the field of *image forensics*. They uses simple image functions to identify certain inconsistencies or footprints introduced as a result of tampering operation, which are not visible by naked eye for example inconsistency in noise [1], blur[2] , sharpening [3],Copy move or duplicate region[4], inpainting[5] etc. Such variations in the inherent statistics of an image can be used to detect whether an image is forged or not.

In this paper we focus on identifying various artifacts that are introduced when multiple JPEG compression is performed within a specified region of a digital image during the cut and paste operation. Methods can be designed to exploit such artifacts and determine if an image is tampered or not. Since JPEG is widely used compression format for storage and transmission of digital images. Various cases exist in this scenario depending on the compression status and properties of the digital images. That is, the source and target images may not be previously compressed or they may be JPEG compressed at different quantization levels. Moreover, the final image obtained after splicing can also be compressed with different compression properties. The various JPEG artifacts thus introduced due to splicing can be categorized as follows:

- Double Compression (DC)
- Blocking Artifacts (BA)
- JPEG Ghost(JG)
- Shifted Double Compression (Shifted - DC)

The organization of the paper is as follows: The explanation of different JPEG artifacts and the methods proposed in the literature to detect tampering based on these artifacts is given in Section II and III. Discussion of the methods is done in section IV. Finally the conclusion is given in Section V.

2. JPEG ARTIFACTS INTRODUCED BY CUT & PASTE FORGERY (SPLICING)

Verifying and proving the authenticity and integrity of a digital image is a major challenge for the research community. A forensic expert in most of the cases has only the forged image whose authenticity has to be tested. In such a scenario

passive blind methods are useful as they verify the integrity of digital images and detect the traces of tampering without using any pre-extracted or pre-embedded information. These methods are based on the fact that the forgeries can bring into the image specific detectable changes (e.g., statistical changes) that act as footprints. The blind methods use simple image function to detect such footprints. The images can undergo various kind of forgeries like copy-paste (near duplicate regions), cut-paste etc. The cut & paste tampering is carried out by taking a region R of a one digital image and is pasted onto another target digital image T, thus creating a tampered image T. The objective is usually to hide a portion of an image, conceal certain facts or alter the meaning conveyed by the image. Various artifacts are introduced when multiple JPEG compression is performed within a specified region of a digital image during the cut and paste operation. The superimposition of multiple compression steps (with aligned or misaligned 8x8 grids), characterized with different quality factors typically introduces number of inconsistencies that can be used as footprints for the detection of tampering. The study assumes that either the source or the target image (or both) are JPEG compressed and the tampered image T is saved in JPEG format after manipulation. A classification of such artifacts given in the following subsections:

2.1 Double compression (DC):

In this type of image forgery the source may or may not be JPEG compressed. A region from the source image is cropped and pasted on target JPEG image without preserving the grid alignment (DCNGA). This result is achieved by assuming that as a consequence of the cut and paste operation the destination image is compressed twice. Such a double compression is detected by the study of double quantization (DQ) effect [6]. Since such an effect cannot be revealed in areas where the two compression grids were not aligned, *regions wherein DQ effect is not revealed are considered as tampered*. If the JPEG image is compressed over and over again, then the number of different JPEG coefficients between two sequential versions decreases monotonically[7].

An improved method of detecting double compression under the hypothesis that former is compressed twice while latter just once is proposed by Bianchi [8]. It is based on probability models of DCT coefficients of regions that are JPEG compressed once and twice. This method provides better performance when compared with DCNGA especially when $QF_2<QF_1$.

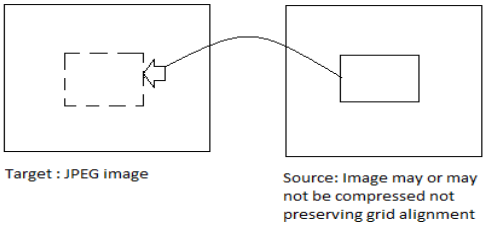

Figure 1: Double Compression

2.2 Blocking Artifacts (BA)

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 $QF2 > QF_1$. Detection relies on a statistical analysis of image blockiness. *The tampering detection process looks for regions having non aligned grids are considered as tampered* [9].

When the image is JPEG compressed, blocking artifact inconsistencies such as block mismatching and object retouching are introduced into an image. The detection method is implemented through extracting and analyzing blocking artifacts grids (BAG). BAG usually mismatches after performing cut- paste operations.

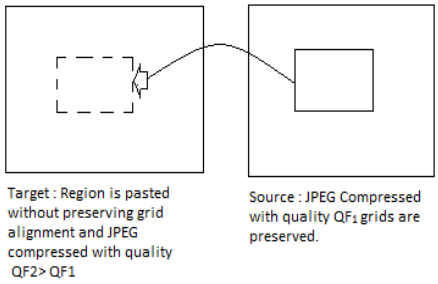

Figure 2: Blocking Artifacts

2.3 JPEG Ghost (JG)

JPEG ghost is a technique to detect whether a part of an image was initially compressed at a lower quality then the rest of the image [10]. JPEG ghost depicts the region where the coefficients were previously compressed with a higher quantization step. A region from a JPEG image is cropped and pasted onto other target JPEG image, preserving grid

alignments. If original images are of different JPEG compression quality then composite image may contain a trace of original or previous compression qualities. *Regions where JPEG ghost are revealed are considered as tampered*.
The disadvantage of this technique is that it only works in case where tampered region is of lower quality than the image into which it is inserted. Advantage of this approach is that it can detect small regions that have been altered.

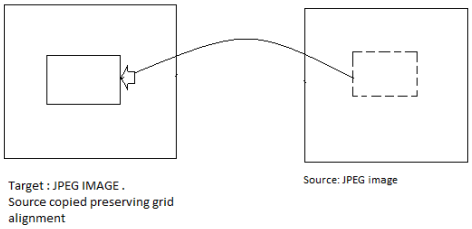

Figure 3:JPEG Ghost

2.4 Shifted Double Compression (Shifted - DC)
In Non-aligned double JPEG compression (NDJC), a portion of JPEG compressed source image is cut and pasted onto another JPEG compressed target image without preserving grid alignments. This kind of tampering is detected by method that depends on the integer periodicity of the DCT coefficients. This method evaluates how a subset of the DCT coefficients (the DC coefficients, on which the quantization effects are more evident) cluster around a given lattice for any possible JPEG grid shift. This measure is compared with a threshold to decide whether grids are aligned or not. A method to detect such artifacts has been proposed by Bianchi [11].

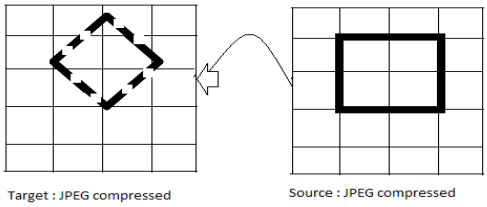

Figure 4: Shifted - DC

3. PREVIOUS WORK:
The research in the field of image forensics has lead to large number of passive-blind methods looking after different footprints. The various methods available in literature for identifying tampering based on JPEG artifacts are studied and are grouped in the corresponding category as discussed in section 2. The methods proposed uses different image processing functions to detect the traces of tampering.

3.1 Double compression (DC)
In [12] ,Tomas Pevny proposed a method for detection of double compression in JPEG for application in steganography that is based on DCT coefficients. Here primary quantization matrix is compared with secondary matrix. Important feature of the proposed method is its ability to detect double-compression not only for cover images but also for images processed using steganographic algorithms. This is first complete solution to the problem of estimation of the primary quality factor in double-compressed JPEG images. In [13], Zhenhua Qu estimated primary quantization matrix in double compressed JPEG images using ICA based identification algorithm. The method used in this algorithm can be extended for colour images. Jing Zhang and Haiying Wang [14] discussed a method for detecting double compression in JPEG 2000 images based on DWT.
In [15], Fangjun Huang proposed a method that has the potential to detect triple JPEG compression, four types JPEG compression etc. Detection of double compression using single quantization matrix is a challenging problem. In [16], FangLing SHI basically improves accuracy of checking whether images are double compressed or not. In [17] ,Yu Chen and Carmen Cheh method is given to improve the accuracy of JPEG image tampering detection. This paper presents a method that detect by differentiating between JPEG single and double compressed quantization histograms. Athulya B and Manoj Ray D [18] provides detailed study of digital image forgery on JPEG images. When a tampered JPEG image is double compressed, final image will have different compression properties than that of single compressed images. This difference in the blocking artifacts is used to detect recompression.
Babak Mahadian [19] presented a detection method based on histograms of DCT coefficients. Method proposed in this paper produces less number of false positives. Zhang Ting [20] detects doctored region in an image by investigating the statistical characteristics of DCT coefficients and then analyze the differences of double compression effect between doctored and non-doctored region. In [21], Tiziano Bianchi and Alessandro Piva proposed probability models for DCT

coefficients of singly and doubly compressed images. Based on such models the probability for each DCT block to be forged is derived.

3.2 Blocking Artifacts(BA)

Shuiming Ye and Ee-Chien Chang [22] 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 [23] ,LI Xiang-hua and Zhao Yu-qian 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. The method is computationally simple and effective. Dijana Tralic and Juraj Petrovic [24] 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. Weiqi Luo and Zhenhua Qu [25] develop the blocking artifact characteristics matrix (BACM) for images that are cropped from another JPEG image and re-saved as JPEG images.

3.3 JPEG Ghost (JG)

In [26] Ergong Zheng and Xijian Ping discussed a passive approach to detect composite JPEG images by measuring inconsistencies of blocking artifacts. Algorithm proposed by them is suitable for smaller regions having low complexity. This algorithm fails when the composite images are saved with lower quality factor than that of the original image. In [27] Fabian Zach and Christian Riess presented a method for automating the detection of JPEG ghosts used for discriminating single and double JPEG compression.

3.4 Shifted Double Compression (Shifted - DC)

Yi-Lei Chen and Chiou-Ting Hsu [28] proposed a method to discover traces caused by recompression. These compression artifact abnormalities, either in spatial or frequency domain, have been used to detect recompression in JPEG images. Tiziano Bianchi and Alessandro Piva [29] gave a method to detect the presence of non-aligned double JPEG compression (NA-JPEG). The method is based on a single feature which depends on the integer periodicity of the DCT coefficients when the DCT is computed according to the grid of the previous JPEG compression.

Zhang Yu-jin and Wang Shi-lin [30] presented a method for the detection of SD JPEG compressed image using Intra-Block and Inter-Block Correlations. Salma Hamdy and Haytham [31] proposed a method to estimate the quantization table from the peaks of the histogram of DCT coefficients. Tiziano Bianchi and Alessandro Piva [32] gave a method to discriminate between original and forged regions in JPEG images .This algorithm manually selects a suspected region in order to test the presence or the absence of double compression artifacts.

4. Discussion

Image forensics deals with authenticity of images. The methods reviewed in the previous section were experimented in ideal laboratory conditions. But in real world applications, these image forensic methods exhibit high false positive rates. This is because the images are tampered by using more than one image processing tool. The presence of other tampering traces effect the performance of an image forensic tool. Moreover, the kind of tampering an image has undergone is not known in advance. This makes the process of identifying and verifying the appropriate tool and tampering very uncertain. This paper presents various JPEG artifacts that are introduced when multiple JPEG compression is performed within a specified region of a digital image during the cut and paste operation. A copy paste detection methods helpful in detecting tampered regions of all sizes and also it can detect multiple tampered regions in a single image. JPEG Ghost approach, discussed in section III, explicitly detects whether part of an image was compressed at a lower quality than the saved JPEG quality of the entire image. Lack of automation makes difficult to visually differentiate between single and double compressed images. For detecting double quantization effect, a quantization matrix is used to locate image forgery with great accuracy. Non aligned JPEG compression can be detected using DCT histograms. It suffers from the drawback that histogram fails in case of heavily compressed images.

As a suggestion for future work, various tools could be developed to reduce the false positive rates of the existing methods. Tampering could also be done by applying more than one editing tool. In such cases, tampering can be efficiently detected using fusion of different forensic tools outcomes.

5. Conclusion

JPEG is widely used compression format for storage and transmission of digital images. The paper presents various artifacts that are introduced when multiple JPEG compression is performed within a specified region of a digital image during the cut and paste operation. The study will be helpful in designing new methods that can exploit such artifacts to determine image forgery and also improve the robustness of existing methods.

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] F. Peng, Y. Nie, and M. Long, "A complete passive blind image copy-move forensics scheme based on compound statistics features.," *Forensic Sci. Int.*, vol. 212, no. 1–3, pp. e21–5, Oct. 2011.

[5] Y. Q. Zhao, M. Liao, F. Y. Shih, and Y. Q. Shi, "Tampered region detection of inpainting JPEG images," *Opt. - Int. J. Light Electron Opt.*, vol. 124, no. 16, pp. 2487–2492, Aug. 2013.

[6] 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.

[7] F. Huang, J. Huang, S. Member, and Y. Q. Shi, "Detecting Double JPEG Compression With the Same Quantization Matrix," vol. 5, no. 4, pp. 848–856, 2010.

[8] T.Bianchi, A.De.Rosa, and A.Piva." Improved DCT coefficient analysis for forgery localization in JPEG images." *Acoustics, Speech and Signal Processing (ICASSP)*, 2011, pp. 2444-2447.

[9] 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

[10] H. Farid, "Exposing Digital Forgeries From JPEG Ghosts," *IEEE Trans. Inf. Forensics Secur.*, vol. 4, no. 1, pp. 154–160, Mar. 2009.

[11] 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.

[12] T.Penvy, and J.Fridrich. "Detection of double-compression in JPEG images for applications in steganography." *Information Forensics and Security*, no. 2, pp. 247-258, 2008.

[13] Q. Zhenhua, W. Luo, and J.Huang. "A convolutive mixing model for shifted double JPEG compression with application to passive image authentication." *Acoustics, Speech and Signal Processing(ICASSP)*, pp. 1661-1664, 2008.

[14] J. Zhang, H. Wang, and Y. Su, " Detection of Double-Compression in JPEG2000 Images," *2008 Second Int. Symp. Intell. Inf. Technol. Appl.*, pp. 418–421, Dec. 2008.

[15] F. Huang, J. Huang, S. Member, and Y. Q. Shi, "Detecting Double JPEG Compression With the Same Quantization Matrix," vol. 5, no. 4, pp. 848–856, 2010.

[16] F. Shi, B. Kang, H. Li, and Y. Zhu, "A new method for detecting JEPG doubly compression images by using estimated primary quantization step," *2012 Int. Conf. Syst. Informatics*, no. Icsai, pp. 1810–1814, May 2012.

[17] V. L. L. Thing, Y. Chen, and C. Cheh, " An Improved Double Compression Detection Method for JPEG Image Forensics," *2012 IEEE Int. Symp. Multimed.*, pp. 290–297, Dec. 2012.

[18] I. Journal, C. Applications, and K. M. Ray, "Tamper Detection and Identification of Cropped Blocks in JPEG Images," vol. 70, no. 20, pp. 36–39, 2013.

[19] B. Mahdian and S. Saic, "Detecting double compressed JPEG images," *3rd Int. Conf. Imaging Crime Detect. Prev. (ICDP 2009)*, pp. P12–P12, 2009.

[20] Z. Ting and W. Rangding, "Doctored JPEG image detection based on double compression features analysis," *2009 ISECS Int. Colloq. Comput. Commun. Control. Manag.*, vol. 1, no. c, pp. 76–80, Aug. 2009.

[21] T.Bianchi, A.De.Rosa, and A.Piva." Improved DCT coefficient analysis for forgery localization in JPEG images." *Acoustics, Speech and Signal Processing (ICASSP)*, 2011, pp. 2444-2447.

[22] S. Ye, Q. Sun, and E. Chang, "Detecting digital image forensics by measuring inconsistencies of blocking artifact," pp. 12–15, 2007

[23] X. Li, Y. Zhao, M. Liao, F. Y. Shih, and Y. Q. Shi, "Passive detection of copy-paste forgery between JPEG images," *J. Cent. South Univ.*, vol. 19, no. 10, pp. 2839–2851, Oct. 2012.

[24] D. Tralic, J. Petrovic, and S. Grgic, "JPEG image tampering detection based on blocking artifacts," pp. 11–13, April 2012.

[25] "A novel method for detecting cropped and recompressed image block," Guangdong Key Lab . of Information Security Technology," pp. 217–220, 2007.

[26] E. Zheng, X. Ping, and T. Zhang, "Detecting Composite JPEG Images in Transform Domain," *2010 Int. Conf. Multimed. Inf. Netw. Secur.*, pp. 340–344, 2010.

[27] F. Zach, C. Riess, and E. Angelopoulou, "Automated Image Forgery Detection through Classification of JPEG Ghosts."

[28] Y.-L. Chen and C.-T. Hsu, "Detecting Recompression of JPEG Images via Periodicity Analysis of Compression Artifacts for Tampering Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 2, pp. 396–406, Jun. 2011.

[29] T.Bianchi, and A,Piva. "Detection of nonaligned double jpeg compression based on integer periodicity maps." *Information Forensics and Security*, no. 2, pp. 842-848 ,2012.

[30] Y. Zhang, S. Li, and S. Wang, "Detecting shifted double JPEG compression tampering utilizing both intra-block and inter-block correlations," *J. Shanghai Jiaotong Univ.*, vol. 18, no. 1, pp. 7–16, Jan. 2013.

[31] S.Hamdy, H.El-Messiry, M.Roushdy "Quantization Table Estimation in JPEG Images." *International Journal of Advanced Computer Science and Applications-IJACSA*, no. 6, pp.17-23,2010.

[32] T. Bianchi, A. Piva, and S. Member, "Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts," vol. 7, no. 3, pp. 1003–1017, 2012.

AUTHOR

Mandeep Kaur received her B.Tech degree in Computer Science and Engineering from BCET, Punjab Technical University, Punjab (India) in 1999 and received her Master's in Engineering (Information Technology) from PEC, Panjab University, Chandigarh (India) in 2004. She is associated with University Institute of Engineering and Technology, Panjab University, Chandigarh (India) since 2005. Her area of interests include Digital image processing and Image forensics.

Jyoti received her B.Tech degree in Computer Science and Engineering from BMSCE, Punjab Technical University, Punjab (India) in 2012 and persuing her Master's in Engineering (Information Technology) from Panjab University, Chandigarh (India).Her area of research is Digital image processing and Image forensics.

Prakriti received her B.Tech degree in Computer Science and Engineering from IET Bhaddal, Punjab Technical University, Punjab (India) in 2012 and is currently persuing her Master's in Engineering (Information Technology) from UIET, Panjab University, Chandigarh (India) . Here area of research is Digital image processing and Image forensics.