International Association of Scientific Innovation and Research (IASIR)
(An Association Unifying the Sciences, Engineering, and Applied Research)

ISSN (Print): 2279-0063
ISSN (Online): 2279-0071

International Journal of Software and Web Sciences (IJSWS)
www.iasir.net

TAMPER DETECTION USING DOUBLE COMPRESSION JPEG ARTIFACT-A REVIEW

Prakriti[1], Mandeep Kaur[2]
[1,2] University Institute of Engineering and Technology, Panjab University, Sector 25, Chandigarh INDIA

Abstract: Image *authentication and image tamper detection. Double JPEG compression might occur when a portion is cut from an image which may or may not be: Image tamper detection using passive-blind techniques has become a hot research field. It uses non-intrusive methods which uses image functions to detect tampering. The tampering operation changes the inherent statistical properties of an image which is not visible by naked eye and thus can be used as footprint by the tamper detection algorithm. The focus of the current paper is to study the artifacts introduced by JPEG recompression which can act as a footprint in passive JPEG compressed and pasted on another JPEG target image to create a fake image that may have traces of double compression. Detection of double JPEG compression finds an important place in digital image forensics. The present paper provides a review of various existing methods and their drawbacks. The study will be helpful in overcoming the limitations of existing methods and designing new image tamper detection techniques*

Keywords*: Double compression JPEG artifact, image forensics, JPEG artifact , nonaligned double JPEG compression ,passive- blind methods ,tampering detection.*

I. Introduction

In recent years digital image forensics has evolved as a propitious field to identify, detect and authenticate digital images. Digital images are used as photographic evidence by the government agencies, legal authorities, media organizations and by many other. Due to low cost, handy and foolproof tools and techniques, tampering of digital photographs has become easier and tamper detection has become more challenging. The two common approaches for image authentication and tamper detection are classified as Active and Passive approach. The active approach uses intrusive techniques like Digital Watermarks and Digital Signature. Digital Watermarking embeds a message at the source side that as a watermark which can be extracted later on to verify the authenticity of an image. Digital watermarks mostly are inseparable from the digital image they are embedded in, and undergo the same transformations as the image itself resulting in depreciation in quality. Therefore any manipulations before the watermark was embedded cannot be detected using this method.Watermarking system was not applicable on images or videos from surveillance cameras, military cameras etc. Digital signature is encoded at the sender side and decoded at receiver end to ensure its integrity. Therefore, nowadays the focus is on Passive techniques, popularly known as Blind methods , verify authenticity of images without using pre extracted or pre embedded information[1], [2],[3].It is based on the fact that the inherent statistical characteristics of an image changes whenever tampering is done. These inconsistencies are used as a footprint for detection of tampering. Various artifacts are introduced by different blind methods that are categorized as noise inconsistency[4], blur[5] , sharpening [6],copy move[7], in painting[8] ,image splicing[9] etc. such artifacts are used to detect whether images are forged or not. Since, JPEG is widely used file format for storage and compression ,various artifacts are introduced due to splicing are double Compression without preserving grid alignment[10] , blocking Artifacts due to non alignment of grids[11], JPEG ghosts[12], non aligned JPEG without preserving grid alignment[13]. The objective of the paper is to focus on double compression JPEG artifact for tamper detection in images. The paper is organized as follows. In Section II there is an introduction about JPEG artifacts introduced by copy paste forgeries .Under it we briefly review basics of double compression method one of the artifact introduced by copy paste forgeries. Section III discusses different approaches to the method and previous work done. Discussion about the method is done in Section IV followed by the Conclusion and Future Scope in Section V ending up with references and acknowledgement.

II. JPEG artifacts introduced by copy paste forgeries

The images can undergo various kind of forgeries like copy-paste ,cut-paste etc. The cut & paste tampering is done by taking a region R of a one digital image and pasted onto another target digital image T, thus creating a tampered image T. The objective is usually to hide a portion of an image, modify 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 multiple compression steps (with aligned or misaligned 8x8 grids) implemented and characterized with different quality factors 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.One of the artifact double JPEG compression is discussed below-

*A. **Double compression***

Double joint photographic experts group (JPEG) compression means that a JPEG image is compressed once again by JPEG compression.In double compression source may or may not be JPEG compressed. A region from the source image is cropped and pasted on JPEG target image without preserving grid alignment. Result is achieved by assuming that destination image is compressed twice resulting in monotonically decreasing the number of different JPEG coefficients between two sequential versions. Such a double compression is detected by study of double quantization effect [14] as shown in Fig 1. For example, for forging an existing JPEG image, the image is decompressed, then different manipulation methods such as splicing can be applied on to the image, and the modified image is then recompressed back into a JPEG image. The action of JPEG double compression causes periodic effects on the DCT coefficients which are used to verify if the image has undergone tampering.
Unaltered original image has a quantization matrix called as primary quantization matrix. Whereas the resaved image has a quantization matrix called as secondary quantization matrix. If the primary and secondary quantization matrix are not identical, then the re–saving operation brings out image specific changes. In other words, saving a picture twice results in double compression.
Considering an example of generic discrete 1-D signal f(x). Quantization is a point-wise operation described by a one- parameter family of functions:

$$q_a(u) = \left\lfloor \frac{u}{a} \right\rfloor$$

Where a is the quantization step (positive integer), and u denotes a value in the range of f(x). De-quantization of the signals brings the quantized values back to their original range: q_a^{-1} (u) = au. The function $q_a(u)$ is not invertible, and that de-quantization process is not the inverse function of quantization process. Double quantization is a point-wise operation described by a two-parameter family of functions:

$$q_{ab}(u) = \left\lfloor \left\lfloor \frac{u}{b} \right\rfloor \frac{b}{a} \right\rfloor$$

where a and b are the quantization steps. Note that double quantization can be represented as a sequence of three steps: quantization with step b, followed by dequantization with step b, followed by quantization with step a.
Double compression can be discussed in 2 situations:
Firstly,when the image is compressed in order to reduce the memory requirement it is called simple double JPEG compression whereas , when the image is resaved after performing copy paste tampering on the image it is called Shifted Double JPEG Compression.
To better understand why the double quantization of a signal introduces periodic artifacts, the dependence between the histograms of single and double quantized signals is determined in double JPEG compression. The main property of double JPEG compression is that it brings out a detectable effect like periodic zeros and double peaks.
An improved method of detecting double compression under the hypothesis that former is compressed twice while latter just once is proposed by Bianchi [15]. 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 double compression without preserving grid alignments, especially when $QF_2 < QF_1$.

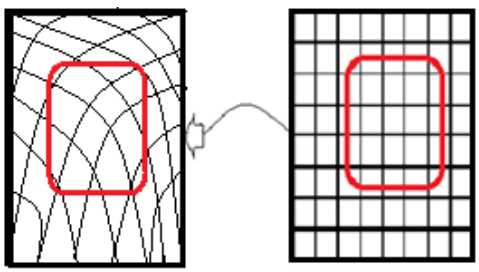

Fig. 1. Double Compression

III. Study of existing methods

Jing Zhang[16] proposed a method for the detection of double compression in JPEG 2000. This method calculates the difference between the sub-band DWT coefficient histograms between single and double JPEG compression which introduces specific artifacts visible in the histograms of these coefficients. A quantitative measure for these artifacts is devised, and used to discriminate between single and double JPEG2000 compressed images. The proposed technique detects double JPEG 2000 compression accurately.

Fangjun Huang [17] pointed out that different quantization matrixes wee used for primary and secondary compressions till date.So a method was proposed to detect double JPEG compression with the same quantization matrix.A JPEG image is recompressed with the same quantization matrix showing a sequential decrease in the quantized DCT coefficients.A proper ratio is calculated on the JPEG coefficient of recompressed test image via implementing a random perturbation strategy.This method is not only applicable for the detection of double compression but can also detect triple and sometimes for times compression and so on.

Bianchi and Piva [18] discussed an algorithm relying on DC(Direct Current) coefficients statistics allowing us to apply single threshold detector. The observations that DCT coefficients exhibit an integer periodicity when the blockwise DCT is computed according to the grid of the primary JPEG compression are taken into consideration. This method can also detect grid shift and the quantization step of the DC coefficient of the primary compression.

FangLing SHI [19] analyzed different features between JPEG double and single compression quantization histogram and estimated values and then proposed a method in which the extracted features were categorized into two classifier with the SVM(Support Vector Machine) technology, then a simulation experiment is conducted to differentiate between double compressed JPEG images and single compressed JPEG images. Method proposed is practical and applicable to real life experiments. It basically improves accuracy of checking whether images are double compressed or not. This method laid foundation for detecting image distortion and image computer forensics. Disadvantage of this method is that it is time consuming.

In [20] ,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. It considers the characteristics of the random distribution of high value bins in the DCT histograms of real-world images. For this method we have used publicly available CASIA authentic and tampered image data set of 9501 JPEG images[21].20 rounds of experiments with small set of images were performed leaving high number of images in each round for testing purpose showing robustness and accuracy of our method. Experimentally we prove, average improvement in the true negative and positive rate. Our method can supported automated and reliable digital image evidence authenticity verification. It had better performance.

Athulya B and Manoj Ray D [22] 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. To hide the information of the target image a portion of digital image is copied and pasted either on the same or different image in order to hide.BACM(Blocking artifact characteristics matrix) properties are used to detect whether an image is cropped or not.

In [23], Zhenhua Qu estimated primary quantization matrix in double compressed JPEG images using ICA(Independent Component Analysis) based identification algorithm. A convolutive mixing model is used for better interpreting the Shifted Double JPEG problem.The independency between BDCT(Blockwise Discrete Cosine Transform) coefficients weakens due to Shifted Double JPEG compression. The method used in this algorithm can be extended for color images and JPEG 2000.Babak Mahdian[24] proposed a double compressed detection method based on histograms of DCT coefficients and SVM. The method produces a significantly less number of false positives.

In [25],Tomas pevny introduced a method for detection of double compression in JPEG for application in steganography that is based on DCT coefficients. Primary quantization matrix is compared with secondary matrix. This method detects 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.

Zhang Ting [26] proposed a method based on SVM multi-class classification for detecting doctored JPEG image. Algorithm analyzes recompression statistical characteristics and concludes that the area not possessing double compression features are termed as suspected doctored region. SVM is used to located the doctored blocks and the doctored region consists of all the connected blocks. Method can detect copy paste forgery within or between JPEG images with low computational complexity and detects doctored region in an image by looking into the statistical characteristics of DCT coefficients and then analyze the differences of double compression effect between doctored and non-doctored region.Algorithm fails when the size of tempered area is small and also limits for detecting images with single details and similar texture.

In [27], Tiziano Bianchi and Alessandro Piva proposed probability models for DCT coefficients of singly and doubly compressed images. Hypothetically it is considered that original areas undergoes double compression while forged areas will have single compression.Method is based on the observation that DCT coefficients exhibit an integer periodicity when the blockwise DCT is computed according to the grid of the primary JPEG.

The improved system is validated by computing the ROC for the forgery detector based on thresholding the probability map.

IV. Discussion

JPEG is widely used image compression format providing better compression ratio. Tampering of images results in change of compression factor. Therefore detecting tampering in images is an important field to be discussed. The presence of tampering is detected by analyzing some artifacts introduced by JPEG recompression.

In this paper double compression approach has been discussed. Images exhibit aligned or non aligned double JPEG compression. In Double quantization we use a quantization matrix to locate image forgery with great accuracy. It is not possible to visually differentiate between single and double compressed images. To verify double quantization of signals dependence between the histograms of single and double quantized signals is compared. Methods proposed are practical and applicable to real life experiments. Different tools can be combined to detect every possible type of JPEG artifacts.

V. Conclusion and future scope

JPEG is widely used compression format for storage and transmission of digital images. Double compression introduced by JPEG artifacts helps to detect single and double compression in images. As a suggestion for future work, there is a need to generate a common test images database which would help researchers to test, evaluate their methods. More robust and precise detection methods could be developed to overcome the limitations of the existing methods and to reduce the false positive rate. Efficient and less time consuming algorithms need to be formulated.

References

[1] Mahdian, Babak, and Stanislav Saic. "A bibliography on blind methods for identifying image forgery." Signal Processing: Image Communication 25.6 (2010): 389-399.

[2] Birajdar, Gajanan K., and Vijay H. Mankar. "Digital image forgery detection using passive techniques: A survey." Digital Investigation (2013).

[3] Luo, Weiqi, Zhenhua Qu, Feng Pan, and Jiwu Huang. "A survey of passive technology for digital image forensics." Frontiers of Computer Science in China1, no. 2 (2007): 166-179.

[4] 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.

[5] Wang, Junwen, et al. "Image Forgery Forensics Based on Manual Blurred Edge Detection." Multimedia Information Networking and Security (MINES), 2010 International Conference on. IEEE, 2010.

[6] Z. Y. and N. R. Cao Gang, "Detection Of Image Sharpening Based On Histogram Aberration And Ringing Artifacts," IEEE ICME, 2009, pp. 1026–1029.

[7] Bayram, Sevinc, Husrev T. Sencar, and Nasir Memon. "An efficient and robust method for detecting copy-move forgery." Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on. IEEE, 2009.

[8] 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.

[9] Zhang, Zhen, Jiquan Kang, and Yuan Ren. "An effective algorithm of image splicing detection." Computer Science and Software Engineering, 2008 International Conference on. Vol. 1. IEEE, 2008.

[10] 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.

[11] 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.

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

[13] 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.

[14] Barni, Mauro, and Andrea Costanzo. "A fuzzy approach to deal with uncertainty in image forensics." Signal Processing: Image Communication (2012).

[15] 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.

[16] 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.

[17] 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.

[18] Bianchi, Tiziano, and Alessandro Piva. "Detection of nonaligned double jpeg compression based on integer periodicity maps." Information Forensics and Security, IEEE Transactions on 7.2 (2012): 842-848.

[19] 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.

[20] 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.

[21] CASIA Image Tempering Detection Evaluation Database Version 2.0, http://forensics.idealtest.org

[22] 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.

[23] 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.

[24] Mahdian, Babak, and Stanislav Saic. "Detecting double compressed jpeg images." (2009): 12-12.

[25] Pevny, Tomas, and Jessica Fridrich. "Detection of double-compression in JPEG images for applications in steganography." Information Forensics and Security, IEEE Transactions on 3.2 (2008): 247-258.

[26] Ting, Zhang, and Wang Rangding. "Doctored JPEG image detection based on double compression features analysis." Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on. Vol. 2. IEEE, 2009.

[27] Bianchi, Tiziano, Alessia De Rosa, and Alessandro Piva. "Improved DCT coefficient analysis for forgery localization in JPEG images." Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on. IEEE, 2011.

Acknowledgements

The authors are thankful to Dr. Savita Gupta Co-ordinator CSE and also to Librarian Mr Raj Kumar and his staff ,University Institute of Engineering and Technology, Panjab University Chandigarh for providing the necessary facilities for the preparation of the paper.