Image Tamper Detection using JPEG Signatures

Surbhi Gupta[1], Neeraj Mohan[2] and Nitika Kapoor[3]

[1] Associate Professor, CSE
Chandigarh University, Mohali, India

[2] Assistant Professor, CSE
I. K. Gujral Punjab Technical University, Jalandhar, India

[3] Assistant Professor, CSE
Chandigarh University, Mohali, India

Abstract

Images tampering means altering the image content using methods like resampling, seam modification, rotation, copy-move, and splicing etc. Image forensic techniques are required to check the authenticity of the questioned image. Two different approaches followed for tamper detection are active and passive. While active include methods like watermarking and signatures, passive works on hidden features of imaging. This paper proposes a passive approach to detect tampering in JPEG images using its blocking features present due to double compression in these images. 20 statistical features from Blocking Artifact Characteristics Matrix has been extracted. An 8X8 block is utilized to construct the feature set. Experiment conducted proved that the proposed approach performs better in classifying images as original or tampered.

Keywords:JPEG signatures; Quantisation Artifacts; Tamper detection; Double Compression

1. INTRODUCTION

Tamper detection is a research area which emerged due to the increasing use of multimedia. From newspaper in morning, social websites in noon till news in evening we see images whole day and do believe their worth. But all images we see may not be authentic. They may be resampled, enhanced, rotated, filtered, or impainted. Copy-paste and Splicing of images are common to create an entire new image. This paper deals with an improved technique to identify tampering in JPEG images as it is the most common prey of image tampering. This proposed work is based on compression artifact detection. First the state of art is presented and then the characteristics of JPEG blocking and feature extraction are discussed. Lastly, the details regarding experiment conducted and results obtained are discussed.

2. RELATED WORK

Forensic analysis of JPEG images usually rely on DCT or quantization artifacts for classifying the image as original or tampered. First such technique based on quantization artifact was proposed by [1] in 2003. The author presented Blocking Artifact Characteristic Matrix (BACM) and Maximum Likelihood Estimation Model. Further, in [2] author used BACM to determine cropping and double compression of JPEG images based on the symmetry of BACM. Then author in [3] investigated the periodic property of blocking artifact. Paper [4] reported that edge direction information could be utilized for detecting blocking artifacts. Paper [5] proposed a method to detect jpeg re-compression using Blocking Artifact Grid extraction based on horizontal and vertical distortions in image blocks. Another category of JPEG image forensics is based on features extracted from the DCT and DWT Histogram. First work in this direction was done by [6] in 2004 by detecting the presence of double JPEG

compression based on periodic artifacts in the DCT coefficient's histogram. Later [7] improved the algorithm given by [6] by using Transition Probability Matrix. A novel technique is proposed in paper [8], which is based on the difference between the sub-band DWT coefficient histograms of single and double JPEG compressed images. Later, the random distribution of high value bins in the DCT histograms of JPEG images is studied in paper [9]. Author claimed to improve the accuracy of JPEG image tampering detection. Paper [10] worked on localizing the tampering by analyzing the image block wise and then region wise. Paper [11] mentioned that the double JPEG compression could be either aligned are non-aligned. It can be identified by analyzing the probability models of DCT coefficients. Recently, author in [12] designed an automated tool and merged different algorithms for splice detection and tampering localization for JPEG images.

3. PROPOSED TECHNIQUE

The proposed technique is based on blocking artifacts which appear in the image due to double compression as mentioned in [2]. Proposed approach presents six new features in addition to 14 features explored by [2].

Proposed Algorithm:

Step1: Consider an image I. transform the image I to grayscale such that

$$I_g = \text{rgb\_to\_gray}(I) \quad (1)$$

Step2: Subdivide the image into blocks of 8X8 pixels.

Step3: Calculate the difference in intensities of each pixel group of each block as:

$$d(x,y) = |(a(x,y) + a(x+1,y+1)) - (a(x+1,y) + a(x,y+1))| \quad (2)$$

Calculate $d(x+4, y+4)$.

Step 4. Calculate the difference between $d(x,y)$ and $d(x+4, y+4)$ i.e.

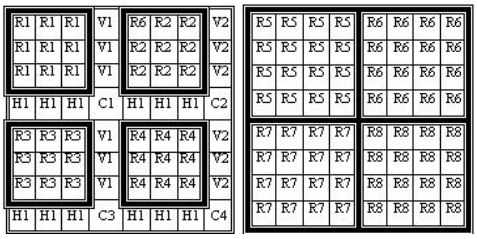
$$D(x,y) = |d(x,y) - d(x+4, y+4)| \quad (3)$$

Step 5. Then the BACM matrix is derived as

$$B(x,y) = \frac{\sum_{n=1}^{k} D_n(x,y)}{k} \quad (4)$$

Where n represents a block, k is the total number of blocks in the image and x & y denote the pixel positions from 1 to 8 i.e. $1 \leq x, y \leq 8$.

Step 6. Then features are extracted from this BACM to detect the tampered image. 14 features from [2] have been extracted as such. Block is divided in four sub-regions R1, R2, R3 and R4; two vertical parts V1 and V2; two horizontal parts C1 and C2; and four centre points C1, C2, C3 and C4 as shown in Fig. 1.



(a) (b)

FIG. 1 (a), (b) BLOCK DIVISION IN VARIOUS REGIONS FOR FEATURE EXTRACTION

The first set of features are based on symmetry of four horizontal H1, H2 and vertical regions V1, V2.For H1 feature F1 is extracted as:

$$F1 = \sum_{y=1}^{3} |B(4,y) - B(4,8-y)| \quad (5)$$

Similarly features are extracted for H2, V1and V2.The next set of features are based on symmetry of four regions R1, R2, R3 and R4. Feature F5 is based on symmetry of R1 and R2 and is extracted as:

$$F5 = \sum_{x=1}^{3} \sum_{y=1}^{3} B(x,y) - B(x,8-y)$$

(6)

Similarly we calculate further features as: F6 based on the symmetry of blocks R3 and R4, F7 based on the symmetry of blocks R1 and R3, F8 based on the symmetry of blocks R2 and R4, F9 based on the symmetry of blocks R1 and R4 and F10 based on the symmetry of blocks R2 and R3.

Step 7: Then 4 new features, F11-F14, are extracted based on mean of four sub-regions i.e. R5, R6, R7 and R8 as:

$$F11 = \sum_{i=1}^{4} \sum_{j=1}^{4} B(i,j) \quad (7)$$

Further 6 six features, F15-F20, are extracted based on percentage of occupancy of centre point C1 against different regions R1, R2, R3, R4, H1 and V1. These are calculated as:

$$F15 = \frac{C1}{\sum_{x=1}^{3} \sum_{y=1}^{3} B(x,y)} \quad (8)$$

$$F19 = \frac{C1}{\sum_{y=1}^{7} B(4,y) - C1} \quad (9)$$

Thus a total of 20 features are mined from the BACM of the image so that it can be successfully classified as single or doubly compressed.

4. RESULTS AND DISCUSSION

The code for features extraction has been written in Matlab 2012. Original and Tampered version of JPEG images has been taken for experiments. The following is an example of feature extraction by proposed technique and its comparison with Luo et al. [2] approach.

(a) (b)

FIG 2. (A) ORIGINAL IMAGE (B) TAMPERED IMAGE

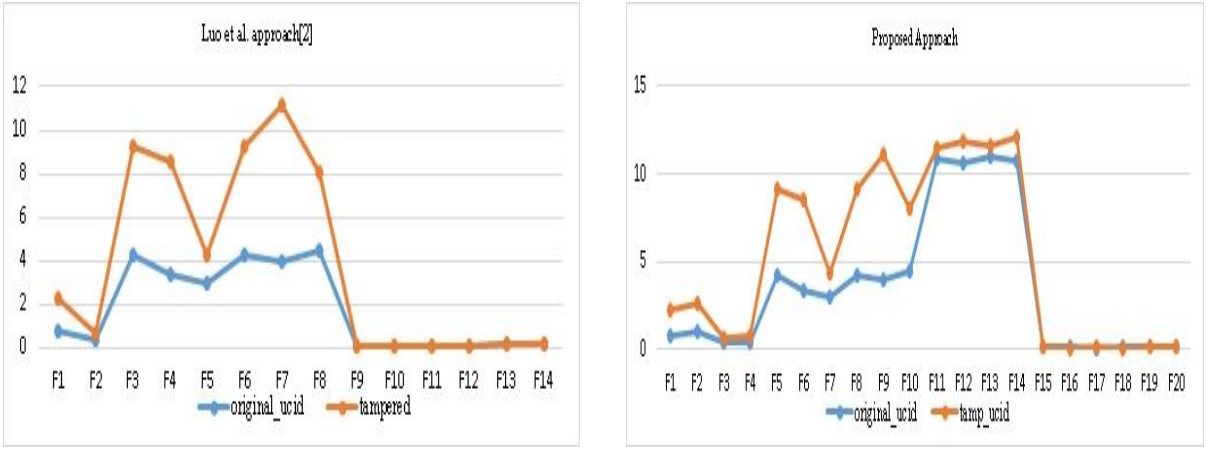


FIG. 3 COMPARISON OF PROPOSED APPROACH WITH APPROACH USED IN [2]

Fig. 2(a) and (b) shows the images taken for experiment. Fig. 3 shows the graphical view of the deviation of values of original image from tampered ones. The proposed method highlights the deviation in tampered image.

5. CONCLUSION AND FUTURE SCOPE

Presented approach aims at identifying tampered images based on quantization artifact which appears in JPEG image due to the double compression. Extracted feature values indicate that

the questioned image is doubly compressed and thus could be a victim of tampering. The Future scope of the presented approach is that a machine classifier based on these features could be designed to automate tamper detection in digital images.

References:

[1] Z. Fan and R. L. De Queiroz, Identification of bitmap compression history: JPEG detection and quantizer estimation, Image Processing, IEEE Transactions on, 12(2), 2003, pp. 230-235.

[2] W. Luo, Z. Qu, J. Huang and G. Qiu, A novel method for detecting cropped and recompressed image block, ICASSP 2007, IEEE International Conference on, Vol. 2, pp. 217-220.

[3] Y. L. Chen and C. T. Hsu, Image tampering detection by blocking periodicity analysis in JPEG compressed images. In Multimedia Signal Processing, IEEE 10th Workshop on, 2008, pp. 803-808.

[4] F. Pan, X. Lin, S. Rahardja, E. P. Ong and W. S. Lin, Measuring blocking artifacts using edge direction information. In Multimedia and Expo, ICME'04, IEEE International Conference on, 2004, Vol. 2, pp. 1491-1494.

[5] D. Tralic, J. Petrovic and S. Grgic, JPEG image tampering detection using blocking artifacts. In Systems, Signals and Image Processing (IWSSIP), 19th International Conference on, 2012, pp. 5-8.

[6] A. C. Popescu, Statistical tools for digital image forensics (Ph. D. thesis), Hanover, Department of Computer Science, Dartmouth College, 2004.

[7] Y. L. Chen, and C. T. Hsu, Image tampering detection by blocking periodicity analysis in JPEG compressed images, In Multimedia Signal Processing, IEEE 10th Workshop on, 2008, pp. 803-808.

[8] Z. Zhang, J. Kang and Y. Ren, An effective algorithm of image splicing detection, In Computer Science and Software Engineering, International Conference on, IEEE , 2008, Vol. 1, pp. 1035-1039.

[9] V. L. Thing, Y. Chen and C. Cheh (2012), An improved double compression detection method for JPEG image forensics, In Multimedia (ISM), IEEE International Symposium on, 2012, pp. 290-297.

[10] M. Barni, A. Costanzo and L. Sabatini, Identification of cut and paste tampering by means of double-JPEG detection and image segmentation, In Circuits and Systems (ISCAS), Proceedings of, IEEE International Symposium on, 2010, pp. 1687-1690.

[11] T. Bianchi and A. Piva, Image forgery localization via block-grained analysis of JPEG artifacts, Information Forensics and Security, IEEE Transactions on, 2012, 7(3), 1003-1017.

[12] M. Fontani, T. Bianchi, A. De Rosa, A. Piva and M. Barni, A Forensic Tool for Investigating Image Forgeries", International Journal of Digital Crime and Forensics (IJDCF), 2013, 5(4), 15-33.