Fuzzy based Image Forgery Localization Using Blocking Artifacts

K.Karthikeyan and R.Sowmya Lakshmi

Abstract: Image forgery is nowadays widely used as digital images are easy to manipulate due to high availability of powerful image processing tools. It is possible to add or remove ob-jects from an image without leaving any visible traces of tampering. This paper describes a method for detection of copy-paste manipulation on JPEG digital images. It is a type of image forgery in which a part of the image is copied to another location in the image with the intent to cover or add an important image object. The detection method was implemented through extracting and analyzing blocking arti-fact grids (BAGs), introduced by block processing during JPEG compression. Analysis was based on fact that BAGs usually mismatch after performing copy-paste operations. Proposed method was demonstrated on two doctored images.

***Index Terms*— doctored images, image tampering, JPEG images, copy-paste forgery, blocking artifacts**

I. INTRODUCTION

Modern image processing tools have made manipulation of digital images easier to carry out and harder to uncover. Many doctored images are used in everyday life, but development of new techniques enabled introduction of more sophisticated methods for their detection.

Image authentication methods can generally be classified as active or passive. Active methods involve embedding of some information into an image when it is archived, and include digital watermarks [1,2] and signatures. Image tam-pering usually destroys or modifies this embedded information, so it can be easily detected. Main issue with this approach is its application in modern devices which usually do not contain any module for digital watermarking or sig-natures. Passive methods on the other hand involve check-ing the integrity of an image, and include analysis of image statistics [3], trails detection [4], consistency verification [5] and rationally judgment [6]. Every detection technique is effective for some kind of tampering attempts, but tamper-ing an image is still easier to perform than detecting a tampered image.

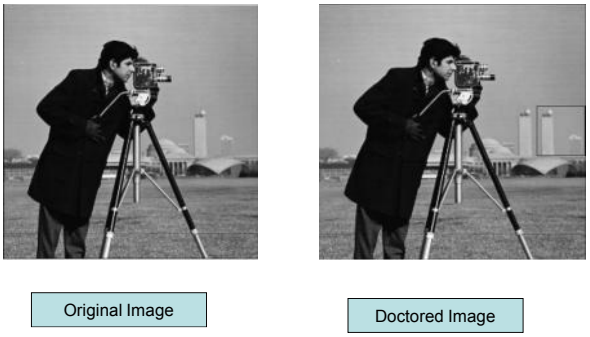
JPEG standard is a widely used image format which utilizes a lossy type of compression. There are many different techniques for detection of JPEG image tampering, such as double quantization effect hidden among the DCT coefficients [7] or checking the uniformity of quantization remainders [8].

K.Karthikeyan is a PG Scholar,Applied Electronics,University College Of Engineering,Bit Cambus -Tiruchirappalli and R.Sowmya Lakshmi is working as Assistant Professor,Department Of ECE,University College Of Engineering,Bit Cambus –Tiruchirappalli, *E.Mail: 3k.sep23@gmail.com*

One of properties of JPEG standard is that it divides an image into 8 by 8 pixel blocks to calculate DCT coefficients and perform quantization. This process of breaking an image into blocks introduces horizontal and vertical breaks into image, which are called blocking artifact grid (BAG). 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.

Figure 1 shows an example of detecting a copy-paste forgery by analyzing the blocking artifacts. It is possible to see that the original image has properly aligned BAG. After copying a rectangle and pasting it inside of the oval, BAG mismatch is visible if the copied area is compared to the neighbored area.

Illustration of Image forgery:



II.LITERATURE REVIEW

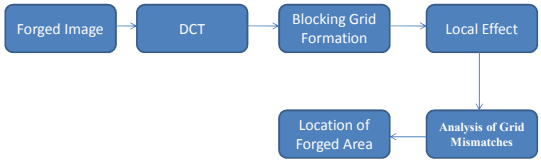
Approaches belonging to the first category include , whereas the presence of nonaligned double JPEG compression has been investigated. Based on the observation that the distribution of the first digit of DCT coefficients in single JPEG compressed images follows the generalized Benford distribution, in the statistical distribution of first digits in quantized DCT coefficients is used as feature set for detecting double JPEG compression. Their performance however does not seem adequate, and they are outperformed by later works, e.g., in , starting from the
observation that recompression induces periodic artifacts and discontinuities in the image histogram, a set of features is derived from the pixels histogram to train a support vector machine (SVM) allowing us to detect an A-DJPG compression. A promising approach is the one introduced by Popescu *etal*. Here, it is proposed to detect the presence of double aligned JPEG compression by observing that

consecutive quantizations introduce periodic artifacts into the histogram of DCT coefficients; these periodic artifacts are visible in the Fourier domain as strong peaks in medium and high frequencies. Their
seminal work has been the basis of the work presented , where double JPEG compression is detected by computing a tampering probability map of the image according to a proper statistical model of DCT coefficients. In an improved version of the model proposed in is presented, leading to a significant improvement of the accuracy of the probability map estimation and consequently of the algorithm performance. In [5], a different approach to detect areas which have undergone a double JPEG compression is proposed. The method works by comparing differently compressed versions of the image with the possibly tampered one;

III.PROPOSED METHOD

The block based transform coding, as used in JPEG stand-ard, causes accuracy of blocking artifacts along block boundaries [9]. They are a result of loss of transform coeffi-cients in the process of independent quantization of each block. Those blocking artifacts can be extracted from an image to serve as a base for detection of copy-paste forgery on an image.

Forgery Detection System:



3.1. Blocking artifact grid extraction

First step in the detection of copy-paste forgery is to extract BAG of an image. In JPEG images, after quantization pro-cess, values of high frequency AC coefficients of a DCT block are usually equal to zero. If all DCT blocks are properly aligned (there was no copy-pasting forgery to cause BAG mismatching), high frequency coefficients will be equal to zero. Opposite to that, if BAG mismatches exist, the AC coefficients on higher frequencies will contain some values. Another case when high frequency AC coefficients will not be equal to zero is appearance of areas that consists of complex textures. However, in that case, AC coefficients will be much smaller than those found in case of BAG mis-matching.
Location of blocking artifacts can be obtained by calcu-lating local effect [10] of 8 by 8 pixel window

$$LE = \sqrt{\frac{\sum_{i=8 \| j=8} S_{ij}^2}{S_{11}^2}},$$

where *Sij* marks AC coefficients of pixels in selected win-dow. Local effect is defined by values of AC coefficients in right column and bottom row. BAG extraction is accomplished by sliding an 8 by 8 pixel window across the whole image, and calculating local effects for every window. Figure shows an example of BAG extraction on an image. It is possible to see that local effect map, shown on figure, contains dark pixels on location with small local effect, and vice versa. Pixels on the blocks' borders have smaller value and they form BAG. After the calculation of local effect map, BAG was extracted by leaving only the local minimal value for every 8 by 8 pixel window of the image.

Similar detection method was used in paper by Li, Yuan, and Yu where it effectively detected copy-paste forgery whether the copied area was taken from the same image or not. In our approach, testing was additionally performed on some images which were processed with aim to hide borders of the copied area.

3.2. Analysis of grid mismatches

Analysis of grid mismatches was performed with few simple searching methods, using the map of local minimal values. First step was marking all points that belong to the grid of the initial image. This processing procedure was based on the assumption that BAG of copied area must be mismatched when compared to the grid of the initial image. In most cases this assumption will be correct so it is possible to ignore all points that belong to BAG of the original image. Assumption is incorrect only in case when the copied area was placed on such location that its BAG remains aligned with BAG of the image (the probability of getting such situation is equal to 1/64). The next step of the analysis was detecting a new, shifted grid that belongs to the copied area. The search was
This step also includes discarding all block areas that appear as black areas on the map of local minimal values. Those areas are the result of homogeneous surfaces in an image because in that case most of DCT coefficients have the same LE value.
Detection of shifted grid was finally performed by the following algorithm. First, the search for shifted blocks was conducted by detecting 4 local minimum points that form vertices of a square with a side length of 8 pixels. Every copied area is assumed to have at least one such segment. In other words it is assumed that the copied area is not smaller than a 16 by 16 pixel block. If any such square artifact was found, the next task was to detect all additional artifacts in that area appearing in one of two forms: "|_" if they consist

of 3 points and "|" if they consist only of two points at a distance of 8 pixels. This search was repeated until no more structures were found at distance of 8 pixels in horizontal or vertical axes of any previously found artifact. Also, to increase the probability of identifying the pasted region of the image, another search was performed identifying all independent "|_" and "|" structures.

IV. EXPERIMENTAL RESULTS

The copied area was placed in such position where it could easily cheat human eye. In this example copied area was taken from the same image, but detection would be equally effective if copied area was taken from a different JPEG image.

After the BAG extraction and analysis, copy-paste forgery was detected because of the mismatch of blocking artifacts in that area. Percentage of correct detection was used as a measure for indication of deviation of BAG on copied area and original image. In this example, 70.51% of copied area was successfully detected, and size of false positive block detection was 0.3419% of the image.

V.REFERENCES

[1] H. Farid, "A survey of image forgery detection," *IEEE Signal Processing Mag.*, vol. 2, no. 26, pp. 16–25, 2009.

[2] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *Proc. 6th Int. Workshop Information Hiding*, Berlin, Germany, 2004, pp. 128–147, Springer-Verlag.

[3] D. Fu, Y. Q. Shi, and W. Su, "A generalized Benford's law for JPEG coefficients and its applications image forensics," in *Proc. SPIE, Security, Steganography, Watermarking of Multimedia Contents IX*, P.W. Wong and E. J. Delp, Eds., San Jose, CA, Jan. 2007, vol. 6505, pp. 1L1–1L11.

[4] B. Li, Y. Shi, and J. Huang, "Detecting doubly compressed JPEG images by usingmode based first digit features," in *Proc. IEEE 10thWorkshop Multimedia Signal Processing*, Oct. 2008, pp. 730–735.

[5] H. Farid, "Exposing digital forgeries from JPEG ghosts," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 154–160, Mar. 2009.

[6] X. Feng and G. Doërr, "JPEG recompression detection," in *Media Forensics and Security II*, Feb. 2010, vol. 7541, Ser. Proc. SPIE, pp. 75410J–75410J-12.

[7] Z. Lin, J. He, X. Tang, and C.-K. Tang, "Fast, automatic and finegrained tampered JPEG image detection via DCT coefficient analysis," *Pattern Recognition*, vol. 42, no. 11, pp. 2492–2501, Nov. 2009.

[8] T. Bianchi, A. D. Rosa, and A. Piva, "Improved DCT coefficient analysis for forgery localization JPEGimages," in *Proc. ICASSP 2011*,May 2011, pp. 2444–2447.

[9] W. Luo, Z. Qu, J. Huang, and G. Qui, "A novel method for detecting cropped and recompressed image block," in *Proc. ICASSP*, 2007, vol. 2, pp. II-217–II-220.

[10] M. Barni, A. Costanzo, and L. Sabatini, "Identification of cut and paste tampering by means of double-JPEG detection and image segmentation," in *Proc. ISCAS*, 2010, pp. 1687–1690.

[11] Y.-L. Chen and C.-T. Hsu, "Image tampering detection by blocking periodicity analysis JPEG compressed images," in *Proc. IEEE 10th Workshop Multimedia Signal Processing*, Oct. 2008, pp. 803–808.

[12] T. Bianchi and A. Piva, "Detection of nonaligned double JPEG compression based on integer periodicity maps," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, Apr. 2012.

[13] T. Pevný and J. Fridrich, "Detection of double-compression for applications steganography," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 247–258, Jun. 2008.

[14] Z. Fan and R. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Trans. Image Process.*, vol. 12, no. 2, pp. 230–235, Feb. 2003.

[15] 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 Security*, vol. 6, no. 2, pp. 396–406, Jun. 2011.