Forensics, Anti-forensics and Counter Anti-forensics for JPEG Compressed Images

Surbhi Gupta¹, and Parvinder Singh Sandhu²

Abstract--- With the advancement in information technology and image processing software the manipulation of the images has increased considerably from past few decades. Retouching or tampering of the images has been so prevalent that nowadays one can hardly believe their originality. Image authenticity is done using forgery detection techniques. These methods are broadly classified as active and passive. Aim of this paper is to give state of art for a passive detection technique i.e. JPEG double compression. Its forensics, anti-forensics and counter anti-forensics is presented with a review of technologies that exist so far.

Keywords--- JPEG Double compression, anti-forensics, counter anti-forensics.

I. INTRODUCTION

The technology nowadays comes with its side effects. At one end, we have information technology which is making our life and work simple and at the other end, it is misused by many. These day researchers have to work for innovative new technologies as well as on simultaneously to overcome its side effects and misuse. Due to the advancement in information technology and image processing software, the manipulation of the images has increased considerably from past few decades. Retouching or tampering of the images has been so prevalent that nowadays one can hardly believe their authenticity. Retouching is usually done for enhancement purpose by keeping the contents of the image intact and tampering is usually done for creating forged images by intentionally altering the contents. Moreover the availability of various free image processing software has made the scenario worst. Even an amateur can create forged images with ease.

Image forgery detection methods are broadly classified as active and passive methods. Active methods are preventive whereas passive methods are reactive. Active methods use precautionary measures to prevent forgery of images by using digital signatures or watermarks. One can check the authenticity of the image anytime by checking the watermark or signatures like date present on it. It’s usually followed for official images to protect them from forgery. Usually a code is embedded in the image which can be checked later for ensuring its authenticity. But this method requires either hardware or software so it is not possible to use them for each and every image clicked. Moreover the cost involved may also be high. But such images are equally prone to forgeries and need special methods to detect the traces of manipulations.

These techniques look for the basic inherent features of the imaging to detect the presence of tampering and come under passive methods. This area of study has fascinated many researchers by last one and half decade and hence it is quiet a mature discipline now. The number of publications has increased enormously in this field. But no single technique can be useful enough to reveal the tampering of images as forgers never use the same methods again. Due to this reason the discipline has also grown breadth wise covering a lot of techniques. A broad classification of these techniques may be done as [1]

• Source based detection
• Tampering operation based detecting
• Statistical irregularities based detection
• JPEG compression based detection

This paper aims at presenting the state of art about jpeg forensics, anti-forensics and its counter anti-forensics. Next section introduces the JPEG compression process. Further, double compression artifacts are discussed. Then the JPEG forensics, anti-forensics, and counter-forensics are discussed in following sections.

I. JPEG single and double compression

JPEG is the most popular file format used for sharing image information due to its size versus quality characteristics. As a result, it is the most common prey of image tampering. A number of various tampering operations possible and then there detecting technique have been proposed.

JPEG lossy compression is a Discrete Cosine Transform (DCT) based process. Firstly, the image is divided into many non-overlapped 8 x 8 blocks. And then 2-D DCT is performed on each 8 x 8 block. These 64 values within each block in frequency domain are known as DCT coefficients while the same position within those blocks is known as a mode. Then those DCT coefficients are quantized based on a certain quantization table, which is also sized 8 x 8. Within this quantization table, there are totally 64 values to be further processed on each mode, which is referred to as quantization steps. Most of the quantization steps within each quantization table are different from each other. A standard quantization table affects the compression rate and thus JPEG quality. Lastly entropy coding is applied. In order to decompress an image, entropy decoding, de-quantization and inverse DCT are consecutively applied. The block diagram of JPEG compression is as:

¹Research Scholar, I. K. Gujral Punjab Technical University, Jalandhar.
II. JPEG compression detection Forensics:

Mainly all the forensic techniques using JPEG characteristics aim at detecting whether the image is single or doubly compressed. If double compression in JPEG image is detected, the chances of it being tampered increases. Some methods may also localize the tampering area. These techniques for detecting forgery are based on either DCT or quantisation artifacts present due to double compression. Compressing an image with JPEG generates two peculiar footprints: the comb-like shape of the Discrete Cosine Transform (DCT) coefficient histogram, which contains empty bins caused by the quantisation stage; and the blocking artifacts in the spatial domain caused by the block-based coding approach. Forensic analysis leverages on such artifacts to infer information on the history or on the source of JPEG images. Features extracted from DCT or quantization artifact are then used for classifying the image as original or tampered.

First such technique based on quantization artifact is extracting the Blocking Artifact Characteristic Matrix. A significant work in this direction has been reported by Fan and Queiroz in 2003[2]. The author proposed a method to estimate the JPEG quantisation step. This work aims at identifying whether the image is previously compressed or not and which quantiser table is utilized for compression. The detection of compression is based on consistent discontinuities across block boundaries. Author computed a Blocking Artifact Characteristic Matrix (BACM) in the pixel domain to measure the symmetric property of blocking artifact, absence of which reveals the double compression. Further a maximum likelihood estimation model is presented to detect the quantiser table used.

Further, Luo et al. in [3] (2007) used BACM to determine cropping and double compression of JPEG images. Author discussed that BACM for original jpeg image exhibits a regular symmetrical shape, where as for images which are cropped from another JPEG image and re-saved as JPEG images, the regular symmetrical property of the BACM is destroyed. These features from the BACM are extracted to train a support vector machine (SVM) classifier for recognizing whether an image is an original JPEG image or it has been cropped from another JPEG image and re-saved as a JPEG image. A good accuracy rate is obtained for different quality factor images. Then Chen and Hsu in [4] 2008 extended the work done in [3] and again investigated the periodic property of blocking artifact by using two different set of features, based on which image classification is performed using SVM . Their technique outperforms the previous one.

Later some researchers worked on the techniques based on Edge information. Pan et al. [5] reported in 2004 that edge direction information can be utilized for detecting blocking artifacts. Author presented a novel unreferenced approach which is irrespective of the exact location of block boundary and therefore invariant to translation, scaling and rotation of the images. Author claimed it to be a new distortion metric for various types of images and video sequence. Then, Perra et al. in [6] (2005) had presented a novel blockiness index using Sobel operator. This index is based on luminance variation of boundary and other remaining pixels. In this method first the convolution of image and sobel mask is taken. Then boundary block edges and inner block edges are measured and a global blockiness measure is defined using both. The algorithm achieved good results with low complexity.

Tralic et al. in (2012) in their paper [7] proposed a method to detect jpeg re-compression using Blocking Artifact Grid extraction. Author highlighted that the process of breaking an image into blocks introduces horizontal and vertical breaks into image, which are called blocking artifact grid (BAG). Analysis of grid mismatches is performed using the map of local minimal values. The processing procedure was based on the assumption that BAG of copied area must be mismatched when compared to the grid of the initial image. The aim is to detect a new, shifted grid that belongs to the copied area. The search was performed among the remaining local minimal value points. Every copied area is assumed to have at least one such segment with 4 local minimum points that form vertices of a square with a side length of 8 pixels. Algorithm presents promising results.

Another category of anti-forensics using JPEG cover the techniques based on features extracted from the DCT and DWT Histogram. First work is done by Popescu 2004[8] in his thesis. He detected the presence of double JPEG compression by the presence of periodic artifacts in the DCT coefficients histogram. But the performance of the algorithm lacks the completeness. Later Chen et al. 2008[9] improved the algorithm given by popescu in [8]. He pointed that according to [8] if the ratio of second to first quantisation step is not an integer, then the JPEG mode histogram of double compressed image would have periodic artifacts. At the other end if the ratio is integer then the single and double JPEG modes would have same histogram and hence the effect of double compression is undetectable. But experimentally, the method fails most of the times when first quantisation QF1 is equal to or more than 95 and QF2 is less than 85. The author used Transition Probability Matrix to improve [8] and a SVM classifier is used to perform the double JPEG detection. Zhang et al. in their paper in [10] (2008) proposed a technique in which the difference between the sub-band DWT coefficient histograms between single and double JPEG compression is calculated. Author mentioned that double compression introduces specific artifacts which are visible in the histograms of these coefficients. A quantitative measure
for these artifacts is devised, and used to discriminate between single and double JPEG compressed images. Thing et al. in [11] (2012) tried to improve the accuracy of JPEG image tampering detection by considering the characteristics of the random distribution of high value bins in the DCT histograms. Author used CASIA authentic and tampered image data set of 9501 JPEG images.

Garg et al. 2008[12] discussed a technique for detecting different types of manipulations using average distortion which is calculated for each block in the image as a function of the remainders of the DCT coefficients with respect to the quantization matrix (Q matrix) used. Various types of forgery methods like rotation, copy-paste, cropping, and brightness are investigated. But the method was tested for only one type of forgery per image and that too on grayscale images.

Some researchers as in [13,14] also localized the tampered area in doubly compressed images. Barni et al. in 2010[13] worked on localizing the tampering by statistically analyze the image block wise and then region wise. The authors detected double compression by studying coding artifacts. Bianchi and Piva in [14] 2010 categorized the double JPEG compression as either aligned are non-aligned. Their method is capable of localizing the tampering. The approach first analyzes the probability models of DCT coefficients and then characterize the artifact as aligned or non-aligned. The Bayesian approach is followed to localize the tampering. Huang et al. in 2010[15] discussed different quantization matrices used for primary and secondary compressions. Author proposed a technique which can detect double JPEG compression with the same quantization matrix. Author pointed that JPEG image when recompressed with the same quantization matrix shows a sequential decrease in the quantized DCT coefficients. In this algorithm a proper ratio of the JPEG coefficient of recompressed image is calculated.

Although a good contribution has been made by the researchers in forensics of JPEG images but still a complete machine learning tool which can localize each type tampering type and its location has not been possible. Only fontani et al. in [16] has made some effort to design a tool merging different algorithms for splice detection in JPEG images. The proposed tool allows exploiting the capabilities of existing forensic algorithms, and moreover provides a decision fusion framework that can automatically interprets the outputs and can help in decision making. Furthermore, the tool can exploit localization capabilities of forensic algorithms to show a probability map to identify suspect regions. But much work is still required in this direction as the researchers are almost always assuming that the image is not processed by anti-forensic tools.

III. JPEG compression Anti-forensics

The anti-forensic means the tool designed to combat the forensics of JPEG images. In this stream, the researchers design the techniques to hide the tampering after effects so that its detection becomes impossible. It makes the forensics more meaningful, challenging and complete so that no stone left unturned. This section gives the state-of-the-art on anti-forensics to review the tools that exist to hide the artifacts arisen due to tampering especially double compression in the case of JPEG images. In the past few years, several anti-forensic schemes have been developed to hide traces of compression. Some of these attacks inspired new forensic detectors, which in turn inspired new attacks.

The first attempts to make JPEG footprints forensically undetectable on the basis of DCT artifacts are the techniques introduced by stamm et al. in their papers in[17,18]. In the first paper, quantisation gaps in the DCT histogram are reduced by spreading the coefficients with an additive noise called anti-forensic dither. The distribution of this noise depends on the value of DCT coefficient that is being modified, on the quantisation step and on the estimation of DCT coefficient distribution prior to compression. As a result, the DCT coefficient distribution in the attacked image approximates as closely as possible the distribution of the unquantised coefficient. In second paper, the traces of blocking artifacts are hidden by means of smoothing based on median filtering, followed by the addition of a Gaussian noise whose variance depends on the JPEG quality factor of the manipulated image. Author demonstrated the effectiveness of the technique. Understanding whether an image has been JPEG compressed multiple times can be useful for a number of forensic applications, including the detection of image splicing. In this scenario, a typical detector looks for a mismatch between the number of compressions of manipulated regions with respect to the rest of the image. Expectedly, counter-forensic schemes attempt to hide the manipulation by uniforming the number of compressions, as in Chunhui et al. [19] in 2012, where double quantisation artifacts are removed. The idea underlying the scheme in Milani et al. in 2013 [20] is similar. This tool attacks detectors based on Benford’s law of first digit (FD), like the one in Milani et al. in 2012 [21], by altering the FD’s probability mass function to match that of a single compressed image.

Qian & Qiao in [22] 2013, introduced a method to conceal clues of JPEG double compression of comb like DCT histogram and blocking artifacts by image enhancement and filtering. Compared with Stamm’s method of introducing noise into the targeting image, the proposed method preserves better quality of image. The technique can fool quantization table estimation, MSE distortion analysis and global histogram analysis. Bohme and kirchner [23] in 2013 framed a categorization of forensic methods and pointed out that stamm’s anti forensic has not been tested against median filtering forensic detectors so is also evident. Recently, Fan et al. in their paper [24] proposed an improved method of JPEG anti-forensics, with a higher visual quality of images. They employed variation based minimization for de-blocking to fool forensic detectors. Method ensures better trade-off between forensic undetectability and visual quality.

The Anti-forensics algorithm has given a new direction to the JPEG forensics. It helped in making the forensic algorithms more robust and is acting as benchmarks to test their applicability.

IV. JPEG compression Counter Anti-forensics

Counter Anti-forensics is the name given to the study for fighting the anti-forensic techniques. It means to design a tool to detect tampering even if an anti-forensic method is used to hide the affects of tampering. Valenzise et al. [25, 26] claimed that the dithering signal [17] degraded the image
quality. A forgery detector is therefore designed by measuring the noisiness of the re-compressed image, employing the TV of the image (the L1 norm of the spatial first-order derivatives). For a given image, the detector re-compresses it using different quality factors q, as a function of which, TV(q) is computed. Lai and Bohme [27] proposed another calibration-based detector to counter Stamm et al.’s JPEG anti-forensic method [17, 18]. They borrowed the idea of calibration from steganalysis [2]. Author defined a high frequency subband as subband that lies below the anti-diagonal of the 8 × 8 matrix of DCT subbands and used these 28 high frequency subbands characteristic of high rate of zero coefficients. The rate R of zero coefficients in high frequency subbands when compared against a threshold (R ≤ T) is used to categorize the image as either unsuspicous or undergone compression and counter-forensic. Li and Liu in [28] 2012 in their paper found that the dithering operation will destroy the statistical correlations among the 8 × 8 intrablock and interblock within an image. They employed the transition probability matrix of the DCT coefficients to measure such modifications for identifying the forged images from those original JPEG decompressed images and uncompressed ones and obtained detection accuracy as high as 99% on the image database of UCID. Qian and Zhang in [29] proposed to use the decimal histogram of the coefficients to distinguish the never-compressed images from the previously compressed or anti-forensically processed. This method is designed to combat Stamm’s anti-forensics method.

Counter Anti-forensics has proved that the JPEG image forensics is not impossible even if a forger has used an anti-forensic tool. These algorithms has highlighted that every forensic algorithm must have capabilities to survive against the anti-forensics algorithms only then they could be actually useful.

II. CONCLUSION

Image forensics is an application oriented domain. Due to the contribution of many research groups the field has actually matured as a subject. The main issue with the subject is its breadth. When a particular solution is proposed it has its own side effects and vulnerabilities. Moreover the solution is only applicable to only a subset of problem domain. Many variations of problems as well solution does exist due to which no single tool are good enough. Many considerations like file format, tampering type, type of analysis required are to be taken care of. To make complete machine learning system with such considerations and complexities doesn’t seems possible in near future. Human interference and governance can’t be neglected. To cover the entire domain of problem it is very important that simultaneously many researchers must work on different perspectives of the same problem, if one works on forensics, another work on its anti-forensics to highlight the limitations and further another work on counter anti-forensics to make the solutions robust, complete and actually employable, which is very important as it highlights the vulnerability concerned. Attacks against a lack of robustness can be warded off by demanding higher image quality standards. Fixing the security weaknesses fundamentally requires better image models. While it is generally hard to find good image models, finding models that are ‘good enough’ to withstand simple counter-forensics seems more much feasible. As a starting point, single-criterion detectors can be replaced with detectors that use image models with multiple (but not many) dimensions. This makes it considerably harder for the counterfeiter to move an image into the right detection region in each dimension at the same time. If the number of dimensions grows unmanageable, machine-learning techniques may be used as discrimination functions. Researchers should try to attack their schemes and argue or demonstrate how effective these attacks can be. This way, the field will develop completely.

REFERENCES
[7] D. Tralic, J. Petrovic & S. Grjic, “JPEG image tampering detection using blocking artifacts”. In Systems, Signals and Image Processing (IWSSIP), 2012 19th International Conference on (pp. 5-8). IEEE. http://dx.doi.org/10.1109/IWSSIP.2012.6245016


http://dx.doi.org/10.1109/ISISE.2012.41

http://dx.doi.org/10.1109/icassp.2013.6638219

http://dx.doi.org/10.1109/icassp.2012.6288362

http://dx.doi.org/10.4304/jcp.8.10.2483-2488

http://dx.doi.org/10.1007/978-1-4614-0757-7_12

http://dx.doi.org/10.1109/icassp.2013.6638220

http://dx.doi.org/10.1109/iccp.2011.6115854

http://dx.doi.org/10.1109/icassp.2011.5946874

http://dx.doi.org/10.1007/978-3-642-24178-9_20

http://dx.doi.org/10.1109/icip.2012.6466840