Double compressed doctored image anti-forensics with statistical forensics analysis

A research proposal submitted for the degree of

Doctor of Philosophy

Submitted By:

GURINDER SINGH

Registration No.: 901406015

Under the Supervision of

DR. KULBIR SINGH

PROFESSOR, ECED

THAPAR UNIVERSITY

PATIALA (PUNJAB)

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING
THAPAR UNIVERSITY, PATIALA-147004
# TABLE OF CONTENTS

1. Introduction..................................................................................................................1

2. Literature Survey..........................................................................................................3

3. Gaps in Literature Survey..............................................................................................11

4. Objectives.....................................................................................................................12

5. Methodology................................................................................................................13

References.........................................................................................................................14
1. Introduction

In this modern age, it is hard to imagine a crime that does not have a digital dimension. Criminals take the aid of technology to facilitate their offenses in order to avoid suspicion. This facilitation further creates new challenges for attorneys, judges, law enforcement agents, forensic examiners, and corporate security professionals as well as common people [1].

The term ‘forensic’ denotes the application of scientific methods to the investigation and prosecution of a crime. Digital forensics is a branch of forensic science concerned with the use of digital information produced, stored and transmitted by computers as source of evidence in investigations and legal proceedings [2]. Digital forensics is used for the purpose of reconstruction of events found to be criminal. It uses the scientifically derived and proven methods toward the preservation, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources [1], [2].

The reliability of images has a key part in numerous fields, including scientific examination, criminal examination, observation frameworks, knowledge administrations, medicinal imaging and news coverage. In today's computerized age, it is conceivable to effectively change or tamper the data or information of an image and make it bona fide. Digital image forensics is a promising field of exploration that can rely on thorough formalizations to gather information on the history of an image [3]. This information is related to its origin, authenticity and the processing steps that it has experienced. The forensic analysis of digital images refers to the reconstruction of the generation process of a given doctored digital image, where the main focus lies on inference about the image authenticity.

The Joint Photographic Experts Group (JPEG) format is widely used as one of the most popular lossy image compression formats today. Thus, it is adopted by various digital cameras and image editing/processing software tools. In an advanced examination that incorporates JPEG images utilized by the majority of cameras as evidences, the classes of issues that are need to manage, are basically two. The former concerns the legitimacy of the visual document under examination. If one has the capacity to prove that it is not unique or original and it has been changed with the
insertion or removal of some information. Then, one should recognize where the non-original parts are located. The latter is related to the retrieval of the device that generated the image under analysis [4]. The device or camera compresses the image once during shooting and if this image is further decompressed and resaved with different compression quality. Then the resultant image becomes double compressed. Therefore, the detection and analysis of double compression helps in the forgery investigation.

Anti-forensic techniques are actions whose objective is to prevent the process of forensic investigation or make it much harder. For the anti-forensic techniques, one can include activities such as deliberate erasure of information by overwriting with new information and protection tools against forensics analysis [5]. Anti-forensic techniques can be utilized to increase security, deleting and overwriting information with the goal that it cannot be read by unapproved persons. These techniques can however be misused by culprits of computer crimes with a specific goal to protect against disclosure of their actions [6]. The users of anti-forensic tools can also remove evidence of criminal activities, such as hackers, terrorists, etc.

The objective is to develop an anti-forensic technique for double compressed JPEG images, to fool the forensic detectors by removing the artifacts left by JPEG compression. There is a need to achieve a better tradeoff between the JPEG forensic undetectability and the visual quality of processed images. JPEG anti-forensic method aims to remove the footprints left by JPEG compression in a given image, in both the spatial domain and discrete cosine transform (DCT) domain. The various forensic detectors [7] as shown in Fig. 1 are used as attacks to identify the traces of the image JPEG compression history or JPEG anti-forensic processing.

![Fig. 1 JPEG compression detectors](image-url)
The previous forensic techniques for the detection of double compressed doctored JPEG images are easily circumvented by adopting anti-forensic attacks. In the literature, most of the forensic analysis for the detection of double compressed doctored JPEG images is based on the study of first-order statistics derived from image histogram. So, a higher order statistics analysis can be performed on double compressed JPEG doctored images.

Applications

The multimedia social networks provide network tools and applications such as Facebook, Flickr, Instagram, Youtube, etc. for sharing of digital image, audio and video, and other multimedia contents. The multimedia social network security becomes the primary concern due to the unethical use of multimedia. To check this unethical use of fake images, the digital image forensics can be used [8], [9].

In tracing the history of an image, identifying the device used for its acquisition is the primary interest. In a court of law, the origin of a particular image can represent crucial evidence. The validity of this evidence might be compromised by the reasonable doubt that the image has not been captured from the supposed acquired device. Helpful clues on the source imaging device might be simply found in the file’s header (EXIF) [9].

One can easily manipulate or tamper the digital images with the help of digital imaging and photo-editing software. In digital imaging both the acquisition process and the tampering techniques, are likely to leave subtle traces. The task of forensics experts is to expose these traces by exploiting existing knowledge on digital imaging mechanisms [9].

2. Literature Survey

This section presents the literature survey based on the existing forensics and anti-forensics techniques for double compressed doctored JPEG images.
Battiato et al. [8] analyzed the performances of existing approaches of forgery estimation. The effectiveness is evaluated by using different input datasets with respect to resolution size, compression ratio and just considering different kind of forgeries. A post-processing technique is also presented able to manipulate the forged image just to reduce the performance of the current state-of-art solution.

Redi et al. [9] studied that digital image forensics is a brand new research field which aims at validating the authenticity of images by recovering information about their history. Two main problems are addressed: the identification of the imaging device that captured the image, and the detection of traces of forgeries. This survey is designed for scholars and IT professionals approaching this field, reviewing existing tools and providing a view on the past, the present and the future of digital image forensics.

Popescu et al. [10] reported that a digitally altered photograph, often leaving no visual clues of having been tampered with, can be indistinguishable from an authentic photograph. As a result, photographs no longer hold the unique stature as a definitive recording of events. Therefore a statistical technique is described based on the statistical correlations for detecting traces of digital tampering in the absence of any digital watermark or signature.

Lukas et al. [11] studied that by checking the related histogram, it is conceivable to figure out if the image was doubly JPEG compressed. To recover the first quantization matrix, few thoughts are exposed taking into account the conduct of normalized histograms. It is also explained in this paper, how double compression detection techniques and primary quantization matrix estimators can be used in steganalysis of JPEG files and in digital forensic analysis for detection of digital forgeries.

He et al. [12] analyzed that a Bayesian methodology computes the probability of each block of the image of being subjected to double quantization. The proposed approach can detect doctored JPEG images and further locate the doctored parts, by examining the double quantization effect hidden among the DCT coefficients. Experiments show that the proposed method is effective for JPEG images, especially when the compression quality is high.
Chen et al. [13] utilized a Markov random process to display the differences between the images. Markov random process is applied to modeling difference 2-D arrays so as to utilize the second-order statistics. In addition, a thresholding technique is used to reduce the size of the transition probability matrices, which characterize the Markov random processes.

Thing et al. [14] proposed that the altering identification technique depends on periodic function detection strategy. The experimental results show that JPEG image forensics method can support reliable large-scale digital image evidence authenticity verification with consistent good accuracy.

Huang et al. [15] recommended a strategy that survey whether an image has been compressed twice with the same quantization table. The proposed algorithm is based on the observation that in the process of recompressing a JPEG image with the same quantization matrix over and over again. The numbers of different JPEG coefficients, i.e., the quantized discrete cosine transform coefficients between the sequential two versions will monotonically decreases.

Liu [16] found out that the recompression with the same quantization table is distinguished in the case of a duplicate operation. It is also observed that in this situation there is a significant probability that the grid of the pasted part is not aligned with the existing one. Recovering some even not all segments of the first quantization matrix, permit to search for the model of devices utilizing the same quantization tables identified before.

Wang et al. [17] studied that with help of Expectation Maximization (EM) algorithm, the probability of an 8 × 8 block being tampered can be estimated; and then, a sophisticated image segmentation method, graph cut, is applied to determine the tampered region. Extensive experimental results on large scale databases prove the effectiveness of the proposed method which is suitable for different tampered region sizes at all levels including pixel, region and image level.

Bianchi et al. [18] estimated the first quantization step, but only to find falsifications and without giving exhaustive results related to its estimation. The strategy investigates two types of traces
left by altering in doubly-compressed JPEG images: aligned and non-aligned. These two situations emerge depending if the DCT grid of the segment of the image pasted in a splicing or cloning operation is or not aligned with one of the original image.

Farid [19] opined a technique based on JPEG ghost detection that has the capacity to localize which parts of an image underwent double compression. A likelihood map is constructed to discover the regions that have experienced double JPEG compression. This approach is applicable to images of high and low quality and resolution.

Fan et al. [20] proposed a technique to detect the JPEG compression that if there is no compression, the pixel differences across blocks should be similar to those within blocks. After detecting a compression signature, this technique also estimated the compression parameters. Specifically, a method is developed for the maximum likelihood estimation of JPEG quantization steps.

Westfeld et al. [21] suggested a blockiness measures which is aware of gradients along block borders seem promising as well. It can be used to remove watermarks and simultaneously create a high peak signal to noise ratio. The gradient aware blockiness uses four instead of only two adjacent pixel values across block borders to measure the artifacts.

Lai et al. [22] established a calibration detector by utilizing the ratio of the variance of high frequency subbands. Vulnerability is point out in this scheme when a maximum likelihood estimator has no solution. A targeted detector is constructed against it, and presents an improved scheme which uses imputation to deal with cases that lack in estimation.

Lin et al. [23] exploited the impacts of successive quantizations took after by dequantizations and do not consider the error introduced by several operations, such as color conversions, rounding and truncation of the values to eight bit integers, etc. This simplification permits to effortlessly manipulate the included mathematical equations, however neglecting this source of error significantly degrades the performances.
Bianchi et al. [24] opined a reliable algorithm to detect the presence of nonaligned double JPEG compression in compressed images. The DCT is computed according to the grid of the previous JPEG compression. Then this method evaluates a single feature based on the integer periodicity of the block wise DCT coefficients.

Wang et al. [25] studied that the probability distributions of DCT coefficients will be disturbed by tampering operation. The tampered region and the unchanged region have different distributions, which is an important clue for locating tampering. The estimation of the above distributions and the size of the tampered region are based on the assumption of Laplacian distribution of unquantized AC DCT coefficients. Thus, the probability of each DCT block being tampered is obtained.

Popescu et al. [26] quantified the specific correlations introduced by color filter array (CFA) interpolation, and describes how these correlations can be automatically detected in any portion of an image. The results show the efficacy of this approach in revealing traces of digital tampering in lossless and lossy compressed color images interpolated with several different CFA algorithms.

Johnson et al. [27] opined a technique for exposing the digital forgeries by detecting inconsistencies in lighting. It is also depicted that, how to approximate complex lighting environments with a low-dimensional model and how to estimate the model’s parameters from a single image. Inconsistencies in the lighting model are then used as evidence of tampering.

Swaminathan et al. [28] introduced a new methodology based on the observation that the processing operations inside and outside acquisition devices leave distinct intrinsic traces on the digital images. These fingerprints can be identified and employed to verify the integrity of digital data. Any change or inconsistencies among the estimated camera-imposed fingerprints, or the presence of new types of fingerprints shows that the image has undergone some kind of tampering.
Lin et al. [29] investigated that the intrinsic fingerprint of many popular image source encoders, including transform-based coding, subband coding, differential coding, and also block processing as the traces of evidence. Based on the intrinsic fingerprint of image source encoders, the constructed image source coding forensic detector identifies that which source encoder is applied.

Luo et al. [30] studied the main errors of JPEG include quantization, rounding, and truncation errors. By analyzing the effects of these errors on single and double JPEG compression, three novel schemes are developed for image forensics. These include identifying whether a bitmap image has previously been JPEG compressed, estimating the quantization steps of a JPEG image, and detecting the quantization table of a JPEG image.

Stamm et al. [31] presented a set of anti-forensic techniques designed to remove forensically significant indicators of compression from an image. A technique is proposed to remove statistical traces of the blocking artifacts left by image compression techniques that divide an image into segments during processing.

Yuan [32] proposed a novel approach for detecting median filtering in digital images. This approach can accurately detect median filtering in arbitrary images, low-resolution and JPEG compressed images. It is also reliable to detect tampering when part of a median-filtered image is inserted into a nonmedian-filtered image, or vice versa.

Sun et al. [33] presented an anti-forensic steganography method that can embed and extract messages from images. The pixel differencing in the proposed adaptive exploiting modification direction (AdEMD) method is used to evaluate whether the pixel located in the edge area can tolerate a larger change than that of the pixel location in a smooth area.

Stamm et al. [34] studied the interaction between a forger and a forensic investigator by examining the problem of authenticating digital videos. An anti-forensic technique is proposed to fool video forensic techniques. Also a game theoretic framework is developed for analyzing the interplay between a forensic investigator and a forger.
Cao et al. [35] proposed two novel algorithms to detect the contrast enhancement involved manipulations in digital images. The histogram peak/gap artifacts incurred because of the JPEG compression and pixel value mappings are analyzed theoretically. Secondly to identify the composite image created by enforcing contrast adjustment on either one or both source regions.

Galvan et al. [36] proposed a novel algorithm to estimate first quantization matrix from double compressed JPEG images. The proposed approach copes with the case when the second quantization step is lower than the first one, exploiting the effects of successive quantizations followed by dequantizations.

Yang et al. [37] proposed an effective error-based statistical feature extraction scheme to detect the double JPEG compression with the same quantization matrix. Two classes of blocks in the error image, namely, rounding error block and truncation error block, are analyzed. Then, a set of features is proposed to characterize the statistical differences of the error blocks between single and double JPEG compressions.

Stamm et al. [38] analyzed the work of JPEG anti-forensics and trying to fill the gaps in the comb-like distribution of DCT coefficients in each sub-band. The proper addition of noise to an image discrete cosine transform coefficients can sufficiently remove quantization artifacts which can act as indicators of JPEG compression.

Stamm et al. [39] proposed a deblocking operation based on median filtering after the DCT histogram smoothing. The proposed anti-forensic operation is capable of removing blocking artifacts from a previously JPEG compressed image and able to fool forensic methods designed to detect evidence of JPEG compression.

Valenzise et al. [40] detected the footprints left by JPEG anti-forensic processing in [38]. Another disadvantage of the method in [38] is to noticeably degrade the image visual quality. When tested on a large set of images, the proposed method was able to correctly detect forged images in 97% of the cases.
Valenzise et al. [41] analyzed the cost of technique in terms of introduced distortion and loss of image quality. This paper characterized the dependency of the distortion on the image statistics in the DCT domain and on the quantization step used in JPEG compression.

Li et al. [42] analyzed that the dithering operation will inevitably destroy the statistical correlations among the $8 \times 8$ intrablock and interblock within an image. The transition probability matrix of the DCT coefficients is employed to measure such modifications for identifying the forged images from those original JPEG decompressed images and uncompressed ones.

Chen et al. [43] presented an effective Markov process (MP) based JPEG steganalysis scheme, which utilizes both the intrablock and interblock correlations among JPEG coefficients. The transition probability matrix is also computed for each difference JPEG 2-D array to utilize the intrablock correlation. Then average transition probability matrix is computed for difference mode 2-D arrays to utilize the interblock correlation.

Fan et al. [44] proposed an approach to JPEG anti-forensics in order to fool some existing JPEG forensic detectors as well as to keep a high visual quality of the processed image. This technique attempts to remove the blocking artifacts in the spatial domain of the image through a variational energy minimization.

Sutthiwan et al. [45] noticed that some relative work can also be adopted for JPEG anti-forensics, e.g., the double JPEG compression anti-forensic method. The efficacy of the proposed scheme has been evaluated on two prominent double JPEG detection techniques and the outcome reveals that the proposed scheme is mostly effective.

Lu et al. [46] studied that the statistical feature selection is a key issue affecting the performance of steganalytic methods. A performance comparison method for different types of image steganalytic features was proposed based on the changing rates. Then a study is performed on JPEG steganalytic features: Co-occurrence matrix vs. Markov transition probability matrix.
Rosa et al. [47] studied that the image forensic analysis for the detection of contrast enhancement and other histogram-based processing usually relies on the study of first-order statistics derived from image histogram. Methods based on such an approach, though, are easily circumvented by adopting some counter-forensic attacks. To overcome such a problem, a novel forensic technique is proposed based on the study of second-order statistics derived from the co-occurrence matrix.

3. Gaps in Literature Survey

From the above mentioned literature review following gaps is obtained.

- Various techniques are being used for the detection of double compressed doctored JPEG images and to estimate its first quantization steps/matrix which helps in digital investigation to find the authenticity of an image. Most of these techniques ignore the effect of the error introduced by color conversions (YCbCr to RGB and vice versa), rounding and truncation of the values to eight bit integers, etc. Here Y is the luma component and Cb and Cr are the blue and red chroma components. RGB stands for the three primary colors of light i.e. Red, Green, and Blue. So, there is a scope to deal with effects of this error properly.

- All the techniques in the literature are based on the concept to estimate the first quantization steps/matrix from double compressed JPEG images. There is a scope to estimate the first quantization steps/matrix from the partial double compressed JPEG images.

- In the previous JPEG anti-forensic work, most of the techniques are focused on removing JPEG blocking artifacts in the spatial domain. So, there is a scope to optimize the anti-forensic technique by removing the compression artifacts efficiently in DCT domain.

- There is a scope to improve the robustness of the anti-forensic technique against various forensic detectors.
• Most of the anti-forensic techniques are unable to achieve a good tradeoff between the JPEG forensic undetectability and the visual quality of processed images. So there is a scope to achieve a better tradeoff.

• Most of the forensic analysis for the detection of double compressed doctored JPEG images and other histogram-based processing usually relies on the study of first-order statistics derived from image histogram. So, there is a scope to conduct a higher order statistics analysis of double compressed JPEG doctored images.

• The previous forensic techniques for the detection of double compressed doctored JPEG images are easily circumvented by adopting counter-forensic attacks. So, there is a scope to improve the detection technique.

4. Research Objectives

Based on the initial studies, literature survey (as reported) and the understanding established the following objectives are proposed:

1. To study and analyze the existing forensics and anti-forensics techniques for double compressed doctored JPEG images.

2. To propose the anti-forensic technique for double compression in DCT domain by removing the compression artifacts in order to fool the existing JPEG forensic detectors.

3. To evaluate the robustness of the proposed technique against different types of forensic attacks.

4. To conduct a statistical analysis of double compressed JPEG doctored images to cope with double compression anti-forensics.
5. Methodology

The existing JPEG anti-forensic techniques for double compression would be analyzed and then an anti-forensic technique is proposed for double compression by removing the compression artifacts in both spatial and DCT domain. The analysis would be carried out by considering histogram of DCT coefficients obtained from the given image. The histogram analysis provides the information of the compression artifacts and these artifacts would be removed by using various techniques such as histogram smoothing, filtering and by filling the histogram gaps. Then the performance of the scheme would be evaluated against various forensic attacks. A higher order statistical forensic analysis would be performed based on the co-occurrence matrix and Markov transition matrix on the JPEG image processed through existing anti-forensic techniques. All simulations and analysis would be done using simulation tools, like MATLAB, Mathematica, etc.
References


