ISSN:0975-9646

Survey on Anti-forensics Operations in Image Forensics

Pranita D. Pandit , Monika Rajput

[#] *P.R.Pote Collage of Engineering ,Amravati*
SGBA University ,Amravati

***Abstract*— Nowadays, digital photos have been widely used as historical records and as evidences of real happenings in applications from journalist reporting, police investigation, law enforcement, insurance, medical and dental examination, military, and museum to consumer photography. While digital photos are conveniently used, their credibility has been severely challenged due to numerous fraudulent cases involving image forgeries. Image Forensics (IF) is an important part of many investigations. The numerous low-cost yet powerful digital tools have enabled easy image creation, modification and distribution, which make fraudulent image forgeries easier than ever. To restore the public trust towards digital photos, passive image forensics has become a booming research area to mainly address photo-authentication related challenges, such as source identification, tampering discovery and steganalysis. Increasingly organizations encounter data that cannot be analyzed with recent tools because of format incompatibilities, encryption, or simply a lack of training. Even data that can be analyzed can wait weeks or months before review because of data management issues. This paper explains about the how Image forensics is big challenge to young researcher and what are the complexities in Image Forensics .The forensic performances depend on both the image regularity types and the appropriateness of the detection methods.**

Keywords: Anti-forensics, Image Compression

I. INTRODUCTION

Due to the widespread availability of digital cameras and the rise of the Internet as a means of communication, digital images have become an important method of conveying visual information. Unfortunately, the ease with which digital images can be manipulated by photo editing software has created an environment where the authenticity of digital images is often in doubt. To prevent digital image forgeries from being passed off as unaltered originals, researchers have developed a variety of digital image forensic techniques. Image compression fingerprints are of particular forensic significance due the fact that most digital images are subjected to compression either by the camera used to capture them, during image storage, or for the purposes of digital transmission over the Internet. Techniques have been developed to determine if an image saved in a lossless format has ever undergone JPEG compression [6],or other types of image compression including wavelet-based techniques If evidence of JPEG compression is detected, the quantization table used during compression can be estimated [6]. Because most digital cameras and image editing software use proprietary JPEG quantization tables when compressing an image, an image's origin can be identified by matching the quantization tables used to compress the image with those in a database of quantization table and camera or software pairings [2]. If the quantization tables are matched with those used by image editing software, the authenticity of the image can be called into question. Recompressing an image which has previously been JPEG compressed, also known as double JPEG compression, can be detected [5],and the quantization table used during the initial application of JPEG compression can be estimated. Localized evidence of double JPEG compression can be used to identify image forgeries [1] as well as localized mismatches in an image's JPEG block artifact grid.

Though many existing forensic techniques are capable of detecting a variety of standard image manipulations, they do not account for the possibility that anti-forensic operations may be designed and used to hide image manipulation fingerprints. This is particularly important because it calls into question the validity of forensic results indicating the absence of image tampering. It may be possible for an image forger familiar with signal processing to secretly develop anti-forensic operations and use them to create undetectable image forgeries. As a result, several existing forensic techniques may contain unknown vulnerabilities. At present, very little anti-forensics research has been published. To the best of our knowledge, the only prior work studying digital image anti-forensics are techniques to remove traces of image resizing and rotation [3], forge the photo response non uniformity noise fingerprint left in an image by a digital camera's electronic sensor [4], and to artificially synthesize color filter array artifacts .

II. LITERATURE REVIEW

Proposed method derives a new, maximum likelihood estimate of the Laplacian parameter using the quantized coefficients available at the decoder. The benefits of biased reconstruction can be quantified through extensive simulations. It's demonstrated that such improvements are very close to the best possible resulting from centroid reconstruction. Assuming a Laplacian distribution for the unquantized, AC DCT coefficients, derive the ML estimate of the Laplacian parameter using only the quantized coefficients available to the decoder. This estimate gives modest improvements in PSNR.

Proposed a passive way to detect digital image forgery by measuring its quality inconsistency based on JPEG blocking artifacts. A new quantization table estimation based on power spectrum of the histogram of the DCT

coefficients is firstly introduced, and blocking artifact measure is calculated based on the estimated table. The inconsistencies of the JPEG blocking artifacts are then checked as a trace of image forgery. This approach is able to detect spliced image forgeries using different quantization table, or forgeries which would result in the blocking artifact inconsistencies in the whole images, such as block mismatching and object retouching.

A method was developed for the reliable estimation of the JPEG compression history of a bitmapped image. Not only an efficient method was presented to detect previous JPEG compression but also a very reliable MLE method was devised to estimate the quantized table used. The detection method. can trace JPEG images which are visually undistinguishable from the original and is extremely reliable for higher compression ratios, which is the range of interest. Detection can be made with QF as high as 95. It is likely that there will be no need for further processing the image for high QF, so that it is more important to accurately identify the high-compression cases. Our method has not failed yet in those circumstances.

It's possible that image manipulators can be done undetectably using anti-forensics counter measure. it's possible two represent a previously JPEG compressed image as never compressed, hide evidence of double JPEG compression, and falsify image's origin. Simple anti -forensics methods have been developed to render JPEG blocking artifact both visually and statistically undetectable without resulting in forensically detectable changes to an image. This technique can be used to fool forensic algorithm designed to detect evidence of prior application of JPEG compression within uncompressed image, determine an image/s origin, detect multiple application of JPEG compression, and identify cut and paste type image forgeries.

Propose an anti-forensics operation capable of disguising key evidence of JPEG compression. It operates by removing the discrete cosine transform (DCT) coefficient quantization artifacts indicative of JPEG compression. The resulting anti -forensically modified image can then be re-compressed using a different quantization table to hide evidence of tampering or to falsify the images origin. Alternatively, further processing can be performed to remove blocking artifacts and the image can be passed off as never-compressed. This is accomplished by adding noise to the set of quantized DCT coefficients from a JPEG compressed image so that the distribution of anti -forensically modified coefficients matches an estimate of the distribution of unquantized DCT coefficients.

Propose anti-forensics methods to removing the artifacts which wavelet -based compression schemes introduce into an image's wavelet coefficient histograms. After anti -forensics operation is applied, an image can be passed off as never compressed, thereby allowing forensic investigators to be misled about an image's origin and processing history. This technique operates by adding anti-forensics dither to the wavelet coefficients of a compressed image so that the distribution of anti-forensically modified coefficients matches a model of the coefficients before compression.

III. ANTI-FORENSICS OPERATION

A. *Anti-Forensics of Digital Image Compression*

Virtually all modern lossy image compression techniques are sub band coders, which are themselves a subset of transform coders. Transform coders operate by applying a mathematical transform to a signal, then compressing the transform coefficients. Sub band coders are transform coders that decompose the signal into different frequency bands or subbands of transform coefficients. Typical lossy image compression techniques operate by applying a two-dimensional invertible transform, such as the DCT or discrete wavelet transform (DWT), to an image as a whole, or to each set of pixels within an image that has been segmented into a series of disjoint sets. As a result, the image or set of pixels is mapped into multiple sub bands of transform coefficients, where each transform coefficient is denoted . Once obtained, each transform coefficients must be mapped to a binary value both for storage and to achieve lossy compression. This is achieved through the process of quantization, in which the binary representation of the transform coefficient is assigned the value according to the equation

$$X = x \quad \text{if } b_k \leq X \leq b_{k-1} \qquad (1)$$

where and denote the boundaries of the quantization interval over which maps to the value . Because some sub-bands of transform coefficients are less perceptually important than others, and thus can accommodate greater loss during the quantization process, the set of quantization interval boundaries is chosen differently for each sub band. After each transform co-efficient is given a binary representation, the binary values are reordered into a single bit stream which is often subjected to lossless compression. When the image is decompressed, the binary bit stream is first rearranged into its original two-dimensional form. Each decompressed transform coefficient is assigned a value through dequantization. During this process, each binary value is mapped to a quantized transform coefficient value be-longing to the discrete set.Each dequantized transform coefficient value can be directly related to its corresponding original transform coefficient value by the equation

$$Y=q_k \quad \text{If } bk \leq X \leq bk\text{-}1 \quad \ldots\ldots\ldots\ldots \qquad (2)$$

IV. CAUSES OF ANTI- FORENSICS

This section describes the landscape of recent computer forensic research activities and various challenges for forensics expert.

A. *Evidence-oriented design*

There are two fundamental problems with the design of recent computer forensic tools:

1. Recent tools were designed to help examiners find specific pieces of evidence, not to assist in investigations.
2. Recent tools were created for solving crimes committed against people where the evidence resides on a computer;

they were not created to assist in solving typical crimes committed with computers or against computers. Put crudely, recent tools were creating for solving child

pornography cases, not computer hacking cases. They were created for finding evidence where the possession of evidence is the crime itself. As a result of this bias, recent tools are poorly suited to finding information that is out-of-the-ordinary, out-of-place, or subtly modified. Recent tools can (sometimes) work with a case that contains several terabytes of data, but they cannot assemble terabytes of data into a concise report. It is difficult to use these tools to reconstruct a unified timeline of past events or the actions of a perpetrator. Such tasks are instead performed more-or-less manually when forensic tools are used for investigations, incident response, e-discovery, and other purposes.

B. ***The visibility, filter and report model***

Most of recent DF tools implement the same conceptual model for finding and displaying information. This approach may be terms the "Visibility, Filter and Report" model .

1. Data to be analyzed is viewed as a tree, with the root of the tree being a critical data structure from which all other data can be reached. Examples of roots include the partition table of a disk; the root directory of a file system; a critical structure in the kernel memory; or a directory holding evidence files.
2. Starting at the root, metadata is recursively examined to locate all data objects. Examples of data objects include files, network streams, and application memory maps.
3. Information regarding each data object is stored I a database. Some tools use in-memory databases, while others use external SQL database.

C. The difficulty of reverse engineering

Many of recent DF engineering resources are dedicated to reverse engineering hardware and software artifacts that have been developed by the global IT economy and sold without restrictions into the marketplace. But despite the resources being expended, researchers lack a systematic approach to reverse engineering. There is no standard set of tools or procedure. There is little automation. As a result, each project is a stand-alone endeavor, and the results of one project generally cannot exchange data or high-level processing with other tools in recent forensic kit.

D. Monolithic applications

There is a strong incentive among a few specific vendors to deploy their research results within the context of all-in-one digital investigation forensic suites or applications. These vendors largely eschew the tools-based philosophy of Unix and have instead opted to create applications that resembles Microsoft Office. This approach may simplify user training and promote product lock-in, but it also increases costs for the field as a whole. Support for file systems, data formats, and cryptographic schemes is a competitive advantage for vendors and development teams. But when these capabilities are bundled into a single application it is not possible for end-users to easily mix-and-match these capabilities as operational requirements dictate

E. ***Wavelet Decomposition of Images***

Wavelets are mathematical functions that decompose data or image into different frequency bands or components, and then study each component with a resolution matched to its scale. Wavelets have advantages over Fourier transform, wavelet applicable in where the signal contains discontinuities and sharp spikes. In past wavelets are used for in the fields of mathematics, physics and electrical and instrumentation engineering. But now the wavelet transform have new application the field of digital image processing, turbulence, human vision, radar, and some natural calamities prediction.

The wavelet transformation is a mathematical tool for decomposition of an image**.** The wavelet transform is a hierarchical system identical to sub band filtering system, in which sub bands are logarithmically spaced in frequency domain. The basic idea of the DWT for a two-dimensional image is explained as follows.

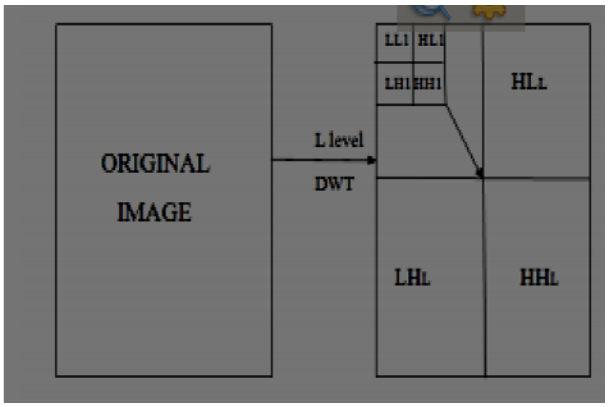

Figure 1: Decomposition of Image[8]

An image is first decomposed into four parts based on frequency sub bands, by sub sampling horizontal and vertical components using sub band filters and named as Low-Low (LL), Low-High (LH), High- Low (HL), and High- High (HH) sub bands as shown in figure 1. To obtain the next set of scaled wavelet coefficients, second level decompositions are needed. In second level decomposition the first sub band LL is further decomposed and critically sub sampled. This process is repeated several times in order to get different sub bands. The block diagram of this image decomposition is shown m in figure 1. Each level has various m sub bands information such as low– low, low–high, high–low, and high–high frequency bands. From these DWT coefficients, the original image can be reconstructed. This process is called the inverse DWT (IDWT).

V. CONCLUSION

This paper predicts an impending crisis in digital forensics given a continuation of current trends that have been identified by many observers. But whereas other papers looking at the future of forensics have focused on specific tactical capabilities that need to be developed, this paper discusses the need to make digital forensics research more efficient through the creation of new abstractions for data

representation forensic processing. Image is compressed using anti forensics method. Two forensic methods for detecting image compression, histogram of the DCT coefficients and blocking artifact measure have been calculated to determine whether the image has been compressed or not. Both the histogram and blocking artifact value are same as the uncompressed image. Hence it's not detected as compressed image. These are the loopholes in the existing forensic method. Hence the forensic methods have to be improved.

REFERENCES

[1] C. Stamm, S.K. Tjoa,W. S. Lin, and K. J. R. Liu, "Anti-forensics of Digital image compression," in Proc. IEEE Int. trans. Information forensics and security, Vol.6,No.3,Sep.2011, pp. 1694–169

[2] M. C. Stamm, S.K. Tjoa,W. S. Lin, and K. J. R. Liu, "Anti-forensics of JPEG compression," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process., Mar. 2010, pp. 1694–1697.

[3] M. C. Stamm and K. J. R. Liu, "Wavelet-based image compression anti-forensics," in Proc. IEEE Int. Conf. Image Process., Sept. 2010,pp. 1737–1740

[4] Z.Fan and R de queiroz,"Identification of bitmap compression histogram:JPEG detection and quantizer estimation" IEEE rans.Image process,vol.12,no.2,pp 230-235,Feb.2003

[5] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti -forensics," in Proc.IEEE Int. Conf. Image Process., Sep. 2010, pp. 2109–2112.

[6] J.He,Z Lin,L.Wang and X.Tang,"Detecting digital image forgeries by measuring inconsistancies of blocking artifacts," in Proc.IEEE Int.Conf.Multimedia Expo.2007,pp.12-15

[7] J.R. Price and M.Rabbani,"Biased reconstruction for JPEG decoding"IEEE signal process. vol.6, no.12,pp.297-299,Dec 1999

[8] Abhitha.E,V.J Arul Karthick "Forensic Technique for Detecting Tamper in Digital Image Compression" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2013