ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Tampering Detection For Jpeg Images Without Preserving using Fourier Domain.

Sachine Kumar Rajput*, and Parthipan V[2].

Department of Computer Science Engineering, Saveetha School of Engineering, Saveetha university, Tamil Nadu, India.

ABSTRACT

The wide availability of high-quality image editing software, general users can now easily edit or enhance digital image content in many ways. However, these easy-to-use image editing techniques also pose new challenges in digital forensics. Many passive or nonintrusive methods have been developed for detecting tampering in digital images. Some methods rely on detecting traces resulting from image acquisition or tampering operations, such as re sampling, color filter array interpolation, camera sensor noise pattern, and scanner sensor noise. Other methods attempt to analyze the inconsistencies in lighting direction or statistical properties of natural images. Unfortunately, most existing methods are effective only for uncompressed raw images and are very vulnerable to JPEG compression. Since the JPEG image format has now been adopted in digital cameras and image processing software, it is vital to account for compression issues in tampering detection methods. Tampering in JPEG images often involves recompression and thus changes the original compression characteristics. Most existing tampering detection methods for JPEG images attempt to detect inconsistency in compression characteristics. Some rely on detecting inconsistency of JPEG quantization tables. Others use the compression artifacts, either in spatial or frequency domain, as an inherent signature for JPEG images. Although these approaches adopt different compression characteristics, different methods have their restrictions and drawbacks. In the following subsection, we briefly summarize these approaches and their restrictions.

Keywords: Jpeg, Fourier domain, detection.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

In a JPEG encoder, all 8x8 discrete cosine transform (DCT) blocks are quantized by the same quantization table before entropy encoding. Once a JPEG image is tampered with (for example, using the copy-move forgery), the tampered image may inherit the characteristics of quantization tables from different sources and thusmay result in inconsistencies. In the quantization table is estimated by quantization errorminimization; in and the maximum likelihood estimation method and the MAP approach are proposed to estimate the JPEG quantization steps. Also, in, the authors pointed out that histogram of DCT coefficients concentrate only on multiples of quantization step and proposed to analyze the power spectrum of

DCT coefficients for quantization table estimation. With the estimated quantization table, it is possible to detect block in consistency and locate the tampered blocks. However, these methods tend to obtain a poor estimate of the primary quantization table from the recompressed image once ecompression is applied after tampering.*B. Abnormality of Compression Artifacts* When a tampered JPEG image is recompressed and again saved in JPEG format, the compression artifacts in the final image may differ from that of singly compressed images. These compression artifact abnormalities, either in spatial or frequency domain, have been used to detect recompression in JPEG images. Luo *et al.*proposed a spatial domain method to detect changes in the symmetric property of blocking artifacts forspatially shifted and recompressed images. Our earlier work analyzed the blocking artifacts from their periodicity and proposed a blocking periodicity model to detect whether an DCT coefficients histogram: (a) 2nd ac term with quantization step size and (b) 12th ac term with quantization step size .image has been cropped and recompressed. However, these spatial domain methods, which rely on detecting abnormality in blocking artifacts, are unable to detect recompression when there involves no spatially shift or cropping with misaligned block boundaries from the original JPEG image. In frequency domain analysis, Benford's law has been used to model the statistical change in DCT coefficients caused by recompression.

In a method via DCT coefficient analysis is proposed to detect and locate doubly compressed regions. However, although these frequency domain methods try to detect abnormality in DCT distributions, they usually fail to detect recompression with misaligned block boundaries. As is clear from the previous discussion no approach has been proposed for JPEG recompression detection that tackles both aligned and misaligned block boundaries. Considering that quantization table estimation completely relies on analysis of DCT coefficients, one would fail to measure the primary quantization table from recompressed images once there involves spatial shift with misaligned block boundaries. On the other hand, the spatial domain methods for detecting the abnormality of blocking artifacts would fail when the recompression includes no shifted or misaligned block boundaries. To the contrary, when the block boundaries in the recompressed images are misaligned from the original JPEG image, frequency domain methods usually fail to detect the abnormalities on DCT distributions.

In this paper, we assume the authentic images are originally in JPEG format and all tampering operations involve recompression. We propose a new compression characteristic that should be insensitive to either block aligned or misaligned cases, and then detect recompression in JPEG images using this proposed characteristic. In Section II, we describe the periodic characteristic of JPEG compressed images in mathematic formulation.

EXISTING SYSTEM

- JPEG is popular as an image compression standard that has ability to detect tampering in JPEG images.
- An image can be easily tampered with image editing tools.
- Hence the detection of tampering operations is of great importance..

PROPOSED SYSTEM

- M A technique to detect image tampering using two different methods.
- The first method is based on the Bayer interpolation process.
- The second method uses artifacts of the JPEG compression and more particularly in the JPEG frame is observable in the Fourier domain.

ISSN: 0975-8585

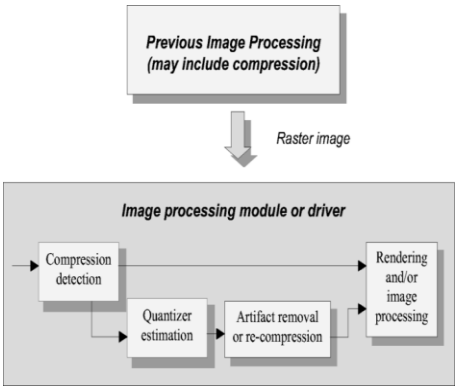

Fig:1 system architecture

SYSTEM FLOW DIAGRAM

SENDER

Sender selects a sample JPEG image as an input. The selected JPEG image finds a local IP as its host. An automatic unique key has been generated for that particular image. Using detect compression, the sender will detect whether the JPEG image is compressed or not. If the image is compressed then it will be send to the receiver. The sender didn't know whether the image gets tampered or not. If it is a JPEG image then there is a possibility for tampering occurrence. And for some other images like GIF, BITMAP tampering may or may not occur.

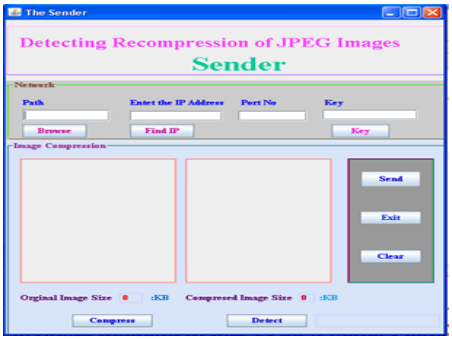

Fig.3 Sender form

RECEIVER

The receiver checks that the generated key is valid or not. If the key is valid the file is received to the receiver and the decompression of the image will take place or else it will exit. The detected tampered image is converted into the original image by using the techniques Bayer Interpolation Process and Fourier Domain. The output image is a tamper less image.

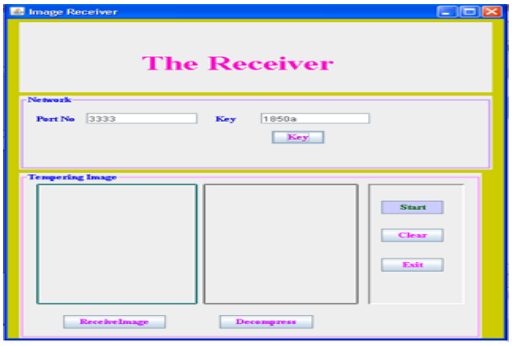

Fig.2 Receiver form

ISSN: 0975-8585

MODULES

a) Image Compression And Detecting Recompression
b) Bayer interpolation process
c) Fourier domain.
d) Automatic and Unique Key generate

IMAGE COMPRESSION AND DETECTING RECOMPRESSION

Image Compression and Detecting Recompression using compress the images and then recompress the images with the data using on the Fourier domain. In this type of image forgery the source may or may not be JPEG compressed. A region from the source image is cropped and pasted on target JPEG image without preserving the grid alignment (DCNGA).

$$f(a,b) = \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} F(k,l)\, e^{\iota 2\pi(\frac{ka}{N} + \frac{lb}{N})} \qquad F(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i,j)\, e^{-\iota 2\pi(\frac{ki}{N} + \frac{lj}{N})}$$

demosaicing method for colour interpolation of images captured from a single CCD using a Bayer colour filter array.

BAYER INTERPOLATION PROCESS

Bayer interpolation process this process can use for interpolation process using for the process then using the formulation of the compressing process. Instead of using a constant or near-constant hue approach like the methods described above, we propose the use of the following criterion: edges have much stronger luminance than chrominance components. Thus, when we look at interpolation of a green value at a red pixel location, for example, we don't discard the red value at that location – it is valuable information! Rather, we compare that red value to its estimate for a bilinear interpolation for the nearest red samples.

FOURIER DOMAIN

Fourier domain algorithms using compressing the images then converts the compressing images and then recompress the images then extract the images.

The DFT is the sampled Fourier Transform and therefore does not contain all frequencies forming an image, but only a set of samples which is large enough to fully describe the spatial domain image. The number of frequencies corresponds to the number of pixels in the spatial domain image, i.e. the image in the spatial and Fourier domain are of the same size.

Automatic and Unique Key Generate

A technique to detect image tampering using two different methods. The first method is based on the Bayer interpolation process. The second method uses artifacts of the JPEG compression and more particularly in the JPEG frame is observable in the Fourier domain.

CONCLUSION

In this study, we considered tampering in JPEG images as a problem of detecting recompression. The main contributions of our work include: 1) we used mathematical formulation and theoretical proof to show that the periodicity of compression artifacts would change once a JPEG image is recompressed; 2) using this property, we further proposed a novel and robust approach for detecting recompression; and 3) combining the periodic features in both spatial and frequency domains, our method can detect recompression with either aligned or misaligned block boundaries. Experimental results show that the proposed method outperforms existing approaches in most quality factor settings.

ISSN: 0975-8585

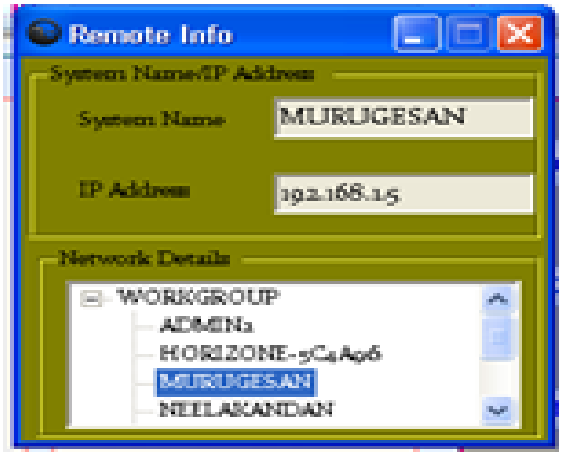

Fig:4 Remote information

FUTURE SCOPE

In future evaluation of tampering and security over image transmission becomes more important in data storage and transmission. Due to increasing use of images in different feeds security over the image also plays a vital role. It is essential to protect the confidence image data from unauthorized access. It is more secure to use image technique tools for compression and decompression of the image. Thus the future evaluation is secure against all different attacks.

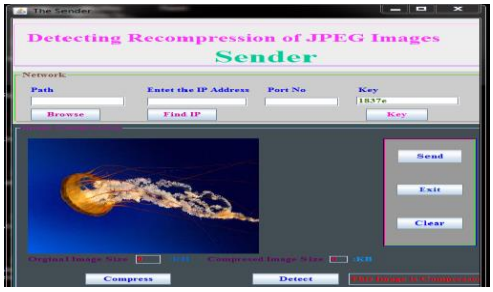

Fig:5 Sender image

Fig:6 Receiver image

REFERENCES

[1] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in the Proceedings of IEEE Conference on Privacy and Security, 1996, pp. 164–173.

[2] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, "The keynote trust-management system, version 2," in RFC 2704, September 1999.

[3] G. Karjoth, "The authorization service of tivoli policy director," in the Proceedings of the 17th Computer Security Applications Conference (ACSAC), December 2001, p. 319.

[4] T. Woo and S. Lam, "A framework for distributed authorization," in the Proceedings of the 1st ACM Conference on Computer and Communications Security, November 1993, pp. 112–118.

[5] S. Ioannidis, A. Keromytis, S. Bellovin, and J. Smith, "Implementing a distributed firewall," in the Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2000, pp. 190–199.

[6] T. Phan, Z. He, and T. D. Nguyen, "Using firewalls to enforce enterprisewide policies over standard client-server interactions," in Journal of Computers (JCP), April 2006, vol. 1, no. 1, pp. 1–12.

[7] S. Capkun, J. Hubaux, and L. utty´an, "Mobility helps security in ad hoc networks," in the Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), June 2003, pp. 46–56.

[8] N. Minsky and V. Ungureanu, "Unified support for heterogeneous security policies in distributed systems," in the Proceedings of 7th USENIX Security Symposium, January 1998.