Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

# APPLICATION OF IMAGE EDITING SOFTWARE FOR FORENSIC DETECTION OF IMAGE

N. Emami

Department of Computer Science, Kosar University of Bojnord, Iran

Published online: 05 June 2016

## ABSTRACT

The image editing software's available today is apt for creating visually compelling and sophisticated fake images, which causes major issues to the reliability of digital contents as a right representation of reality. Authenticity is the main problem in most digital image communication. Various forensic techniques have been developed for the verification of image integrity, authentication, and tampering detection. Digital image forensics aims at finding the authenticity of images by recovering history of the image. Image manipulations occur at the time of compression, which means changing the DCT coefficients. Forensic technique is capable of detecting chains of operators that is applied to an image. Here the union of Joint Photographic Experts Group compression and full-frame linear filtering were studied and derived an accurate mathematical framework for fully characterizing the probabilistic distributions of the discrete cosine transform (DCT) coefficients of the image, which gets quantized and filtered. This statistical model is used for deriving a set of significant features from the DCT histogram of the input image; these features were fed to a effective classifier which effectively classifies different combinations of linear filtering and compression.

**Keywords:** Full- frame linear filtering, JPEG compression, Linear classifier, image forensics.

Author Correspondence, e-mail: Nasibeh.emami@kub.ac.ir

doi: http://dx.doi.org/10.4314/jfas.v8i2s.277

## I. INTRODUCTION

As the image processing technology grows faster, it is easy to tamper the digital images without leaving any obvious visual hints. Now whatever we see with our eyes are no longer believable. Image forgery can cause serious harm to society as like other illegal issues . Thus the verification of the authenticity of images becomes very important issue.

As a solution to digital image authentication, proposed method was Digital watermarks and signatures. But these methods need insertion of an imperceptible watermark or want to attach a signature at the time of the data creation in order to facilitate with the tampering detection. Hence this can be called as active methods. Now, passive method has evolved quickly. This method assumes that the original data has some features which is inherent, that are introduced by different imaging devices. And by the process of analyzing how the data is acquired and processed, from where the data is coming, is easily understandable, is it an original one or not, and what all are the tampering operations that had been done previously. By comparing with active methods, this method does not depend on any extra data such as a watermark or a signature. An image is a collection of pixels. Where each pixel represents a three-dimensional (3-D) color vector for a color image. The Joint Photographic Experts Group (JPEG) is a standard used to compress the digital color images. JPEG compression process is by quantizing the discrete cosine transform (DCT) coefficients of the images. The linear image processing, such as filtering, is often applied to the entire image (full-frame) as post processing for image enhancement, but possibly also for forensic footprints removal, may alter the characteristic artifacts introduced by the JPEG compression scheme. By the knowledge of the compression quantization step and a effective forensic tool which is able to jointly detect the filter kernel and the quality factor of the JPEG compression that have been applied to an image, and hence retrieve the entire processing history of the content. Then it can extract a set of significant features of the DCT distributions of the compressed and filtered image and build a linear classifier able to effectively discriminate different combinations of filtering and compressions. And it represents an approach to jointly disclose traces of chain processing operators such as JPEG compression and full-frame linear filtering.

## II. LITERATURE SURVEY

## III. IMPLEMENTATION DETAILS

In paper [1], Image forensics is used for the detection of history of the digital image. the union of JPEG compression and linear filtering has been studied here and then analyzed the impact of this combination on the statistical distribution of the discrete cosine transform (DCT) coefficients of the image. And thus from the DCT distributions, the characteristic features have been extracted and build an effective classifier that is capable of disclosing the applied compression quality factor and filter kernel jointly.

In paper [2], the unions of JPEG compression and linear filtering have been studied and analyzed the impact of these combinations on the images statistical properties. Then derived a mathematical model, which allows for characterizing the probabilistic distribution of the DCT coefficients of the quantized and filtered images. And thus these knowledge's were exploited for the estimation of filter kernel. Here, to analyze the processing accurately, the relationship between the DCT coefficients is expressed before and after the filtering.

In paper [3], a method was proposed which finds image editing's since many editing software's are available today. That is forensic detection of image was done. Here together with JPEG compression, linear filtering was done and derived a model mathematically that characterizes the probability distribution of DCT coefficients of the image that gets quantized and filtered. Then some set of features were defined using this. Then trained an classifier that is able to disclose both the quality factor and filter kernel jointly.

In paper [4], Anti- forensic method is proposed in this paper for image compression. The traces left in the image after image compression can be removed by using this anti-forensic method. Also it is capable of removing blocking artifact traces of an image. Thus this method is mainly used to remove the fingerprints left by JPEG compression. An image is segmented into series of 88 blocks when the image is JPEG compressed. Then the DCT of each image is block is calculated, hence then compression is achieved by the quantization of each DCT coefficients. The division of each DCT coefficients by its corresponding quantization matrix yields the quantization. Then these quantized values are rearranged in a zigzag order. The sequences of these quantized values are rearranged into original order for the decompression process. Then by multiplying each quantized DCT coefficients with its corresponding quantization matrix yields the dequantization. Now for each of the DCT blocks, inverse DCT (IDCT) is applied, a value will be resulted, and this pixel value will be rounded to nearest integer value. For the removal of compression artifact, here anti- forensic dither is added to each of the DCT coefficients.

The field of computer graphics is getting advanced day by day. And hence the images are susceptible for manipulation. Now various tools are available for such manipulations which may affect the images in positive as well as in a negative way. The manipulated image is difficult to identify from the original image. Hence it affect the authenticity of image. Thus the images transmitted can be easily attacked by the hacker and can manipulate them and can make a fake image. This may adversely affect in different fields like military, medical field, court etc. The loss of authenticity of an image can cause loss of a human life. So it is such an issue that should be solved properly.

The image forensics hence evolved as a solution for the image manipulation. This field aims at finding the history information's that the image has undergone. That it is based on a fact that any hints will be leaved out by the personalities who manipulate the images. And the history of an image can be justified without any original image. Watermark is also a solution, but it needs insertion of data at the time of processing which delays the time and special tools are needed to insert that data or image into it for authentication. That is hence the image authentication method is termed into two active method and passive method. Active method is a method which needs information, image or anything embedded into it. Example foe such a method is watermarking. Next method is the passive method in which no need of embedding into the image. Also this method is called as blind since it doesn't need original image for the verification of its authenticity.

Image compression is a process that reduces the data amount that is needed to represent an image. This compression process is done by the removal of all unnecessary or redundant data's. There are two types of compression; they are lossless compression and loss compression. Lossless compression preserves the image without any loss of information, while the loss compression only produces the original image with less perfection. But the advantage behind loss compression is that it requires less amount of information and can achieve greater levels of compression.

Linear filtering is an filtering technique which enhances or modifies an image. Filtering an image means it will take some features or will remove some other features of the image.

Here in this paper we use both compression and linear filtering. The compression used is loss compression that is JPEG compression is used here together with the filtering process. Filtering is done as a post- processing because it enhances the compressed image.

Let us look up into the figure 1 which illustrates the block diagram for the process.

The variation of the histograms when processing through

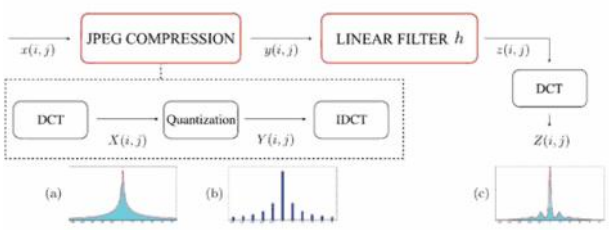


**Fig.1.** Shows the block diagram of the considered system.

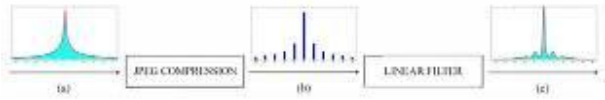

**Fig.2.** Shows the block scheme of the considered system.

Panel (a) shows the original DCT histogram for uncompressed images together with its curve fitting. In panel (b), the same distribution of the coefficients after JPEG quantization is shown. Panel (c) shows the distribution when an linear average filter of size 3 x 3 is applied to the image, along with the derived model for such distribution. Each block is shown in figure 2.

Fig 1. simply shows the block diagram. In this block diagram it includes compression and filtering. Initially the input image gets compressed by the JPEG compression. The JPEG compression includes three steps here, they are DCT, Quantization and IDCT. That is the input image pixels are converted into blocks of equal sizes say; 8 x 8. And they are converted to DCT coefficients by the DCT transformation. These DCT coefficients are now quantized by the quantization process with the aid of quantization table. After that IDCT is applied to that quantized coefficients to convert the frequency domain back to spatial domain. That is to recover the image for the purpose of filtering. Now filtering is applied to the output of IDCT, which also enhances the image. The convolution the quantized image with the filter kernel produces the filter output. The weighted sum of some number of neighboring pixels produces the filtered image pixels. And DCT transformation is again applied so that it is easy to understand the history form the histogram of DCT coefficients than from that of pixels.

Fig 2 illustrates the histograms. It shows the variations in the histogram when it is processed through each block. The fig 2.(a) represents the histogram of the original image. This is given to JPEG compression block. A new histogram arrives. From this histogram we can see that there is quantization artifacts introduced by JPEG compression. These quantization artifacts introduced by the JPEG compression is perturb by the filter that in the DCT distribution. And in the histogram obtained after filtering has some new patterns.

The algorithm for JPEG compression is straightforward and the following steps explains them:

An image is taken and dividing it into 8-pixel by 8-pixel blocks. If the division of image into 8-by-8 blocks is not possible, then pad zeros in empty pixels around the edges of the image.

For each of these 8-by-8 block, get the data of image such that there is values for the representing the color at each of the pixel.

Then take the Discrete Cosine Transform (DCT) of each of the 8-by-8 block.

After taking the DCT, multiply the block by a mask, that is matrix multiplication this will make some values of the DCT matrix zero.

At last for getting the data for the compressed image, take the inverse for each DCT block, that is take IDCT for each block. Then all blocks are combined back into an image as the original image of the same size.

Now obtained the decompress image. This image is passed through a filter, which is a linear filter which enhances the image. The filter can be any linear filter with filter kernels. Now the filter convolutes its input image with its filter kernel and produces the filtered image. That is the obtained image is quantized and compressed image. This quantized and compressed image is now in the form like that of the original image. DCT is then applied to the image obtained.

SVM classifier is a linear classifier that defines the decision boundaries based on the concept of decision planes. The decision plane separates different class members as different set of objects. For separating such classes a complex line is required between the sets of objects. Lines between different sets make them easier. SVM classifier (a linear classifier) is a classifier that separates these different classes of objects with a optimal line. This makes the separation easier.

The quantized and filtered DCT coefficients are now used for the detection purpose. The changes occurred in this image is not understandable by the naked eye. This is given to the SVM classifier for discriminating the image.

SVM classifier is not able to detect the forensics without any training. So initially the SVM

classifier needs to be trained with sufficient images. Here it is trained according to the needs here required. So when SVM classifier is trained they have the images with the details of changes occurred in the image. Hence they can be used for discrimination.

The quantized and filtered output is now giving to the SVM classifier as input. The classifier discriminates the input with the trained data. Classifies them according to the trained data available within them, by classification the SVM classifier is able to detect the changes that is happened to the input image. It identifies the changes occurred, that is it will find out the forgeries happened to the input image. And hence can identify the forgery caused to the input image which cannot be identified by the naked eye. Thus due to this the classifier is used in many occasions like in court etc for the purpose of forensic detection.

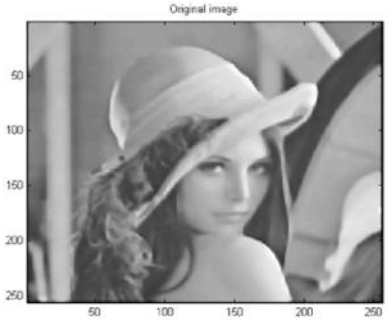


**Fig.3.** Original image.

**Fig.5.** Filtered image

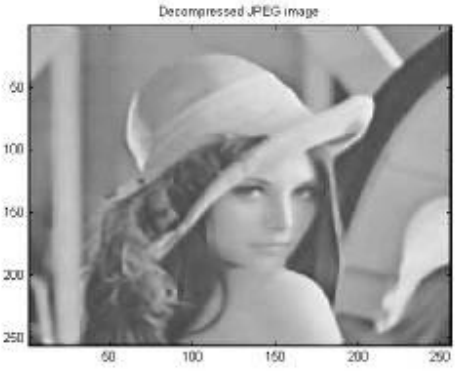


**Fig.4.** Decompressed image. **Fig.6.** Disclosing the quality factor and filter kernel of the image

This image is given to an linear classifier, which effectively classifies its input with the trained data and found out the changes happen to the image.

## IV. RESULT

MATLAB is the simulation tool used. Forensic detection was the solution for detecting faked image. Many software's are available now detecting forgery is a difficult task. Here with the help of an SVM classifier the image get forged is detected. The input image, its corresponding histogram and the image at each stage is shown below.

## V. CONCLUSION

Due to the rapid increase of technology, many software's that can edit the images are available today. These editions make the image susceptible to manipulations. These manipulations may adversely affect the human. The available can be used in both ways that is in a positive as well as in a negative way. The negative way may sometimes affect the human life. The detection of these forged images is not possible with the human eye. The input image gets JPEG compressed

## REFERENCES

[1]V. Conotter, P. Comesafia, F. Perez-Gonzalez,"Joint detection of full-frame linear filtering and JPEG compression in digital images". in Proc. IEEE Int. Workshop Inf. Forensics Secure., Guangzhou, China, 2013, pp. 156161, Nov.

[2]V. Conotter, P. Comesafia, F. Perez-Gonzalez, and K. Hugl, "Forensic analysis of full-frame linearly filtered JPEG images," International Con-ference on Image Processing (ICIP) , 2013.

[3]V. Conotter, P. Comesafia, F. Perez-Gonzalez, "Forensic Detection of Processing Operator Chains: Recovering the History of Filtered JPEG Images," in in IEEE transactions on information forensics and security, 2015, 10 (11), november.

[4]M. S. Sreelakshmi and D. Venkataraman, "Image compression using anti-forensics method," in Proc. IEEE Transactions, Dec.

[5]Gregory K. Wallace, "The JPEG Still Picture Compression Standard," in IEEE Transactions on Consumer Electronics,, Dec. 1991

**How to cite this article**:
Emami N. Application of image editing software for forensic detection of image. J. Fundam. Appl. Sci., 2016, 8(3S), 1300-1307.