Improving JPEG Image Anti-forensics

Priya M. Shelke
Vishwakarma Institute of Information Technology
Pune, India
priya.shelke@viit.ac.in

Dr. Rajesh S. Prasad
N.B.N. Sinhgad school of Engineering
Pune, India
rajesh.prasad@sinhgad.edu

ABSTRACT

This paper proposes a forensic method for identifying whether an image was previously compressed by JPEG and also proposes an improved anti-forensics method to enhance the quality of noise added image. Stamm and Liu's anti-forensics method disable the detection capabilities of various forensics methods proposed in the literature, used for identifying the compressed images. However, it also degrades the quality of the image. First, we analyze the anti-forensics method and then use the decimal histogram of the coefficients to distinguish the never compressed images from the previously compressed; even the compressed image processed anti-forensically. After analyzing the noise distribution in the AF image, we propose a method to remove the Gaussian noise caused by image dithering which in turn enhances the image quality. The paper is organized in the following manner: Section I is the introduction, containing previous literature. Section II briefs Anti-forensic method proposed by Stamm et al. In section III, we have proposed a forensic approach and section IV comprises of improved anti-forensic approach. Section V covers details of experimentation followed by the conclusion.

Keywords

Anti-forensics; Forensics; JPEG compression; Image Enhancement; AF (Anti forensically processed) image.

1. INTRODUCTION

With the development of computer technologies, digital images can easily be processed by editing software and spreading via the internet. Hence, it becomes necessary to find out if the image is original or tampered (fake) [1] [2].As a result, researchers have developed many forensics schemes to detect the probable forgeries in digital images. As human vision alone is not capable of perceiving the forgeries, features extracted from the image can be used to expose the tampering fact [3].

At present, virtually all existing digital image forensic techniques assume that no anti-forensic methods are employed by an image forger to disguise evidence of image tampering or alter other forensically significant image properties. To account for this possibility, anti-forensic image processing operations must be developed and studied so that weaknesses in existing image forensic techniques can be made known to researchers.

This will allow researchers to know when forensic results can be trusted and to assist them in the development of improved digital forensic techniques. At times, defects emerge inside the anti-forensically processed images. E.g quality of anti-forensically processed images degrades due to noise. So, improved anti-forensic methods can also be developed. It creates a game theoretic framework.

JPEG is the most widely used tool for image compression .In order to conceal the JPEG compression history Stamm et al. [4][6] pioneered the work of JPEG compression anti-forensics. Stamm et al. have proposed an anti-forensic de-blocking[5] operation capable of reliably removing statistical traces of JPEG blocking artifacts in images previously compressed using a quality factor of 30 or higher.

A research paper by Wei Fan et al [7] makes a contribution to improving the un-delectability of JPEG anti-forensics with a higher visual quality of processed images.

The paper by Zhenxing Qian, Xinpeng Zhang [8] proposes an improved anti-forensics method for JPEG compression. After analyzing the noise distribution, they propose a de-noising algorithm to remove the grainy noise caused by image dithering, and a de-blocking algorithm to combat Fans forensics method [9] against blocking artifacts.

The paper by Wei Fan et al [10] proposes a JPEG anti-forensic method, which aims at removing from a given image the footprints left by JPEG compression, in both the spatial domain and DCT domain.

Anti-forensics is compressive for assessing the forensics methods and is helpful for improving their reliability [11].

Lai et al[12]detect counter-forensics of JPEG compression, which only modifies DCT coefficients to smooth the marginal distributions of AC sub bands based on Lam and Goodman's model[18] and calibration from Steganalysis.

After analyzing the anti-forensics method, Zhenxing et al [13] propose to use the decimal histogram of the coefficients to distinguish the never-compressed images from the previously compressed; even the compressed image is anti-forensically processed.

Valenzise et al [14] analyzed the cost of the technique proposed in [4] in terms of introduced distortion and loss of image quality. Valenzise et al [15] proposed a detector of anti-forensically

ICTCS '16, March 04-05, 2016, Udaipur, India
© 2016 ACM. ISBN 978-1-4503-3962-9/16/03…$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905134

attacked images, which also estimates the original JPEG quality factor Q. The core of the proposed detector by Valenzise et al [16] is based on the Recompress and Observe paradigm. This work extends previous work [15] to the general and challenging scenario in which quantization template matrix is unknown. Authors measure the noisiness of recompressed images by means of Total Variation i.e the l1 norm of the spatial first order derivatives [17].

We propose a system to distinguish the never compressed images from the previously compressed; even the compressed images anti-forensically compressed, using decimal histogram analysis [13].At times, defects emerge inside the anti-forensically processed images. So we implement a method to improve the noise distributions in the resulting images.

2. JPEG ANTIFORENSICS

Stamm et al. have shown that the statistical footprints of JPEG compression can be removed by adding a properly designed dithering noise signal to the quantized DCT coefficients of a JPEG-compressed image. The distribution of the dithering noise signal is such that the resulting coefficients are approximately distributed as those of the uncompressed original image. Using this technique, the authors have also demonstrated that many of the forensic techniques based on JPEG footprints can be fooled.

Stamm first estimated the distribution of the un-quantized DCT coefficients. He modeled the un-quantized DCT coefficients as being distributed according to the Laplacian distribution [18]. By assuming that the quantization table is known, he calculated maximum likelihood estimate λ_{ML} of Laplacian parameter, $\lambda_{(i,j)}$ for each DCT sub band. Next, to alter the comb-like histograms caused by the discreteness of Laplacian distribution, he proposed the image dithering algorithm. Noise is added to the AC coefficients to approximately reconstruct the histogram of each sub band, using,

$$Z = Y + N \qquad \text{…………. (1)}$$

Where N is the additive noise. The distribution of noise is conditionally dependent upon the coefficient value to which it is added. Assuming that the model distribution is accurate and that $\lambda_{ML} = \lambda$, this choice of conditional noise distributions ensures that the distribution of anti-forensically modified DCT coefficients will exactly match the model distribution of unmodified DCT coefficients. The results of this method are as follows:

3. COUNTERING JPEG ANTIFORENSICS

The key idea of Stamm and Liu's method is to pad the gaps appear in the histogram of each sub-band for AC components. However, when analyzing the decimal values of the DCT coefficients, we find they are not distributed as Laplacian distribution in each sub band for never compressed images. As a result, we propose to use the distribution feature of decimal values in the image to verify whether the image was compressed or anti-forensically processed.

For a test image X, first divide the image into 8×8 blocks, and turn each block into a coefficient block by discrete cosine transform (DCT). Let the coefficient at $(i, j)^{th}$ position of the k^{th} block be $C_k^{i,j}$. Generate the histogram of coefficients corresponding to the $(i, j)^{th}$ position of all the blocks,

$$H_{i,j} = hist(C_k^{i,j}) \qquad \text{…………. (2)}$$

Where hist(•) is the histogram function. The artifact of comb-like histogram should appear if the image was previously compressed. However, if the image had been processed by Stamm and Liu.'s anti-forensics method, we are unable to find this evidence. In order to decide whether the image was processed by anti-forensics method, we round $C_k^{i,j}$ to the first decimal,

$$D_k^{i,j} = \text{round}(10 * C_k^{i,j})/10 \qquad \text{……….. (3)}$$

And calculate the difference of $D_k^{i,j}$ with its nearest integer.

$$E_k^{i,j} = \text{sgn}(C_k^{i,j}).(D_k^{i,j} - round(D_k^{i,j})) \qquad \text{……….. (4)}$$

The range for $E_k^{i,j}$ is from –0.5 to 0.4. Generate the histogram of $E_k^{i,j}$,

$$H'_{i,j} = hist(E_k^{i,j}) \qquad \text{………. (5)}$$

Call this histogram the "decimal histogram".

Because the calculation of DCT randomly produces decimal numbers, values of $H'_{i,j}$ are uniformly distributed for the never-compressed images. If the image was previously compressed by JPEG, coefficients were quantized and thus decimal values concentrate around zero. Even Stamm and Liu.'s anti-forensics method is unable to conceal the evidence.

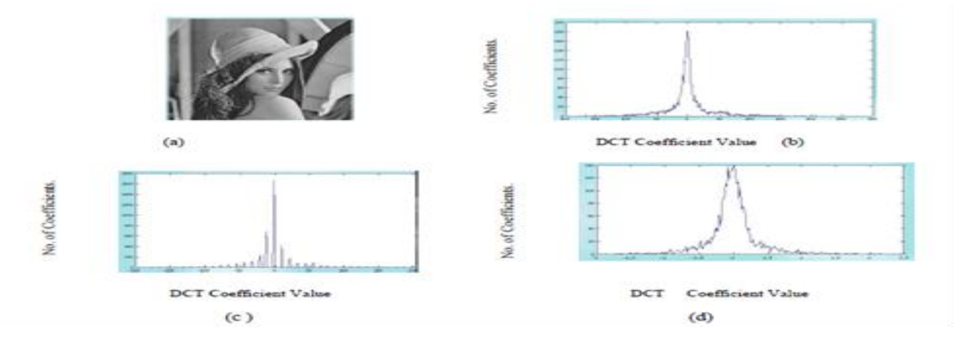

Figure 1. Results of anti-forensic by Stamm (a) the original never-compressed image, (b) histogram of the coefficients at subband (1, 2), (c) histogram of the coefficients corresponding to the compressed image, (d) histogram of the coefficients after processing the compressed image by Stamm et al's anti-forensics method.

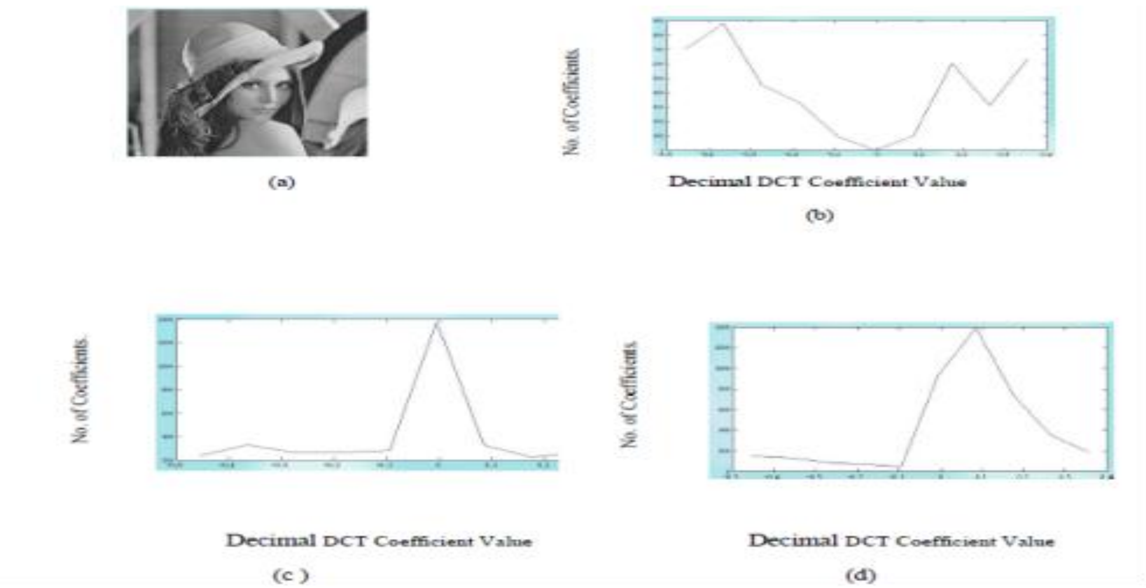

Figure 2. Result of Forensic method by Zhenxing (a) a never-compressed image, (b) decimal histogram of (a) at the sub - band (1, 2), (c) decimal histogram at the sub-band (1, 2) of the compressed image with quality factor 80, (d) decimal histogram corresponding to the image processed by anti-forensics

Zhenxing Qian et al [8] have used a threshold value to determine whether the image is original, compressed or dithered.

We contribute the observation that the shape of the decimal histogram of the never compressed image follows either a nearby flat shape or the shape of trough through zero, whereas decimal histogram of compressed and dithered (AF) image takes the shape of crest rising at or after zero.

4. IMPROVING JPEG ANTIFORENSICS

The noise distribution of AF image is different from that of uncompressed image. To reveal the noise abnormalities in the resulting image, we use a low-pass filter with the kernel H,

$$H = 1/9 \begin{bmatrix} 111 \\ 111 \\ 111 \end{bmatrix} \ldots\ldots\ldots\ldots(6)$$

Convolute the image I with H to generate a filtered image I'.

I'= I *H ………… (7)

where, * stands for the convolution operation. Based on Stamm and Lius method, we propose a new anti-forensics method, aims at improving the quality of the AF images, removing the fingerprints of JPEG compression and eliminating the noise abnormalities.

This method includes three parts, first median filtering and later applying histogram equalization and then Wiener filter. Median filtering removes the Gaussian noise; histogram equalization improves the sharpness while wiener filter improves the brightness of the dithered image.

5. EXPERIMENTATION

To determine the efficiency of proposed forensic method, we have used normally available UCID image database. We randomly use 400 images from the UCID database and turn them into gray images. Each image is compressed by JPEG using quality factor 20, 50 and 80, respectively. These images are then forged by Stamm and Liu’s anti-forensics method. The decimal histogram analysis is carried out. Experimental results show that more than 90% of the never-compressed images are truly determined and all the previously compressed images that were further processed by Stamm and Liu’s method are truly determined. Detection results show that the proposed scheme has a good forensic capability.

Similarly for proposed improved anti-forensic method, we used AF images created from Stamm’s method as input. We can see from fig.1.3 that histogram of proposed method is quite similar to original image histogram as compared to the histogram of AF image by Stamm’s method.

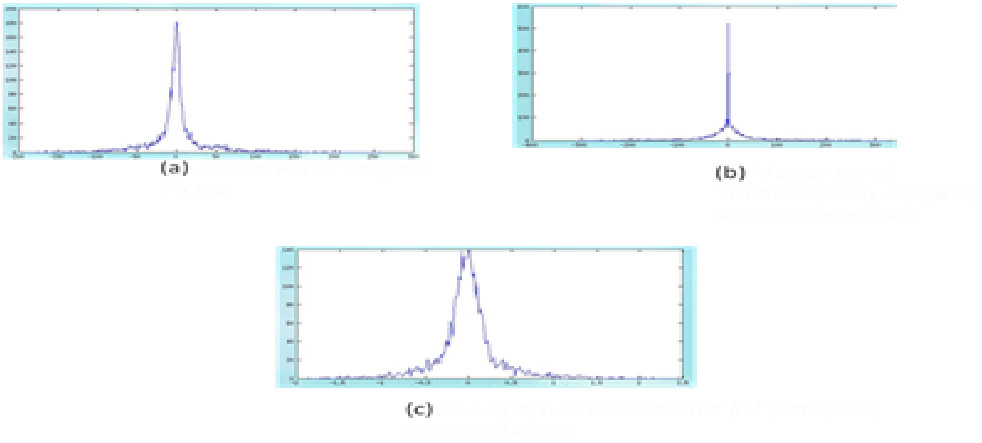

Figure 3. Result of Improved Anti-Forensic method by proposed method (a) Histogram of never-compressed image, (b) histogram of enhanced AF image at the sub-band (1, 2) by proposed method, (c) Histogram of AF image by Stamm's method

6. CONCLUSION

We have proposed a forensics method for identifying whether an image was previously compressed. This method is designed to combat Stamm and Liu's anti-forensics method. By analyzing the decimal values of the DCT coefficients, we have found that the distributions in the decimal histogram are different for never compressed images and previously compressed images, even if the compressed traces are hidden by the anti-forensics processing.

We have also proposed a new anti-forensics method for jpeg compressed images. We first analyzed the defects of Stamm and Liu's method, including the new fingerprint caused by anti-forensics and the poor quality of the resulting image. Accordingly, we defined a forensic approach for identifying whether an anti-forensically processed image is abnormal on the aspect of noise distribution. A new approach for improving Stamm and Liu's method was proposed. By estimating the noise of the dithered image, we presented a method for removing the Gaussian noise.

7. REFERENCES

[1] Farid, H. (2009). Image forgery detection. Signal Processing Magazine, IEEE, 26(2), 16-25.

[2] Gloe, T., Kirchner, M., Winkler, A., & Böhme, R. (2007, September). Can we trust digital image forensics? In Proceedings of the 15th international conference on Multimedia (pp. 78-86). ACM.

[3] Popescu, A. C., & Farid, H. (2004, May). Statistical tools for digital forensics. In Information Hiding (pp. 128-147). Springer Berlin Heidelberg.

[4] Stamm, M. C., Tjoa, S. K., Lin, W. S., & Liu, K. R. (2010, March). Anti-forensics of JPEG compression. In Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on (pp. 1694-1697). IEEE.

[5] Stamm, M. C., Tjoa, S. K., Lin, W. S., & Liu, K. J. (2010, September). Undetectable image tampering through JPEG compression anti-forensics. In Image Processing (ICIP), 2010 17th IEEE International Conference on (pp. 2109-2112). IEEE.

[6] Stamm, M. C., & Liu, K. J. (2011). Anti-forensics of digital image compression. Information Forensics and Security, IEEE Transactions on, 6(3), 1050-1065.

[7] Fan, W., Wang, K., Cayre, F., & Xiong, Z. (2013, May). A variational approach to JPEG anti-forensics. In Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on (pp. 3058-3062). IEEE.

[8] Qian, Z., & Zhang, X. (2014). Improved anti-forensics of JPEG compression. Journal of Systems and Software, 91, 100-108.

[9] Fan, Z., & De Queiroz, R. L. (2003). Identification of bitmap compression history: JPEG detection and quantizer estimation. Image Processing, IEEE Transactions on, 12(2), 230-235.

[10] Fan, W., Wang, K., Cayre, F., & Xiong, Z. (2014). JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality. Information Forensics and Security, IEEE Transactions on, 9(8), 1211-1226.

[11] Kirchner, M., & Böhme, R. (2008). Hiding traces of resampling in digital images. Information Forensics and Security, IEEE Transactions on, 3(4), 582-592.

[12] Lai, S., & Böhme, R. (2011, May). Countering counter-forensics: the case of JPEG compression. In Information hiding (pp. 285-298). Springer Berlin Heidelberg.

[13] Qian, Z., & Zhang, X. (2012). Combating Anti-forensics of Jpeg Compression.

[14] Valenzise, G., Tagliasacchi, M., & Tubaro, S. (2011, May). The cost of JPEG compression anti-forensics. In Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on (pp. 1884-1887). IEEE.

[15] Valenzise, G., Nobile, V., Tagliasacchi, M., & Tubaro, S. (2011, September). Countering JPEG anti-forensics. In Image Processing (ICIP), 2011 18th IEEE International Conference on (pp. 1949-1952). IEEE.

[16] Valenzise, G., Tagliasacchi, M., & Tubaro, S. (2013). Revealing the traces of JPEG compression anti-forensics. Information Forensics and Security, IEEE Transactions on, 8(2), 335-349.

[17] Rudin, L. I., Osher, S., & Fatemi, E. (1992). Nonlinear total variation based noise removal algorithms. Physica D: Nonlinear Phenomena, 60(1), 259-268.

[18] Lam, E. Y., & Goodman, J. W. (2000). A mathematical analysis of the DCT coefficient distributions for images. Image Processing, IEEE Transactions on, 9(10), 1661-1666.

[19] Schaefer, G., & Stich, M. (2003, December). UCID: an uncompressed color image database. In Electronic Imaging 2004 (pp. 472-480). International Society for Optics and Photonics.