Combating Anti-forensics of Jpeg Compression

Zhenxing Qian[1], Xinpeng Zhang[2]

[1]School of Communication & Information Engineering, Shanghai University, Shanghai, China

ABSTRACT

This paper proposes a forensic method for identifying whether an image was previously compressed by JPEG. Though some methods have already been proposed for this purpose, Stamm and Liu's anti-forensic method disables the detection capabilities of these methods. After analyzing the anti-forensics method, we 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. Experimental results show that this method has a good forensic capability.

Keywords: *Digital Forensics, Anti-forensics, JPEG Compression*

1. Introduction

With the development of computer technologies, digital images can easily be processed by editing software and spread via internet. This provides forgers opportunities for manipulating original images into fakes [1]. As a result, researchers have developed many forensics schemes to detect the probable forgeries in digital images. Though most forgeries may not be perceived by human vision, features extracted from the image can be used to reveal the tampering fact [2, 3].

A particular type of forensics is the operation of JPEG compression, which is a very popular method for image compression. With the method proposed in [4], an image's origin can be identified by analyzing the quantization steps of JPEG compression and compare them with a database containing kinds of camera models and editing software. If the parameters match, decisions of manipulations can be made. Some schemes have also been proposed for identifying whether an image in uncompressed format was previously compressed by JPEG. Fan and Queiroz proposed a method able to estimate the quantization steps by analyzing the DCT coefficients of the image [5]. Some other methods such as [6] and [7] are proposed to detect the existence of double JPEG compression.

However, these forensic methods can be defeated by anti-forensic methods hiding the features of tampering operations. In [8] and [9], Stamm and Liu proposed to hide the JPEG compression history by adding noise into the DCT coefficients. During compression, the Laplacian distribution of coefficients' histograms changes to discrete form, which is an obvious evidence of JPEG compression. After adding noise into the coefficients, the discrete gaps of the histograms are efficiently padded.

Anti-forensics is compressive for assessing the forensics methods and is helpful for improving their reliability [10, 11]. In this paper, we propose a forensics method to combat Stamm and Liu's anti-forensics to images that are previously compressed by JPEG. We find the distribution for decimal values of the coefficients of a never-compressed image is different to that of the previously compressed image, and also different to that of the anti-forensically processed image.

2. Related Work

Previously, Stamm and Liu proposed an effective anti-forensics method of hiding traces of JPEG compression in

[8] and [9]. According to [12], coefficients for AC components corresponding to the same subband of a never-compressed image follow Laplacian distribution. Let *X* be the DCT coefficient at the block position (*i*, *j*) for a never-compressed image,

$$P(X=x)=\frac{\lambda}{2}e^{-\lambda|x|} \tag{1}$$

where λ is a Laplacian parameter.

If the image was previously compressed by JPEG, AC coefficients of each subband are distributed as discrete Laplacian distribution because of the quantization and the reverse. For the the coefficients at the (*i*, *j*)-*th* position, if we use the quantization step $Q_{i,j}$, the distribution would be

$$P(Y=y)=\begin{cases} 1-e^{-\frac{\lambda Q_{i,j}}{2}} & \text{if } y=0 \\ e^{-\lambda|y|}\sin\left(\frac{\lambda Q_{i,j}}{2}\right) & \text{if } y=kQ_{i,j} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

Where $Y=Q_{i,j}\cdot round(X/Q_{i,j})$, and the parameter λ can be generated by maximum likelihood estimation

$$\lambda_{ML}=-\frac{2}{Q_{i,j}}\ln\left(\frac{-N_0Q_{i,j}+\sqrt{N_0^2Q_{i,j}^2-(2N_1Q_{i,j}-4S)(2N_1Q_{i,j}+4S)}}{2NQ_{i,j}+4S}\right) \tag{3}$$

Where $S=\sum_{k=1}^{N}|y_k|$, *N* is the total number of coefficients at the (*i*, *j*)-th position, N_0 represents the number of coefficients taking zero values, and N_1 the number of nonzero coefficients.

The discreteness of Laplacian distribution causes comblike histograms as many gaps appear. To hide the compression evidence, Stamm and Liu introduce noises into the AC coefficients to approximately restore the histogram of each subband, by

$$Z=Y+N \tag{4}$$

Where *N* is the additive noise. For the coefficient *Y* of zeros value at the (*i*, *j*)-*th* position, the noise distribution is given by

$$P(N=n\,|\,Y=0)=\begin{cases} \frac{1}{c_0}e^{-\lambda_{ML}|n|} & \text{if } \frac{-Q_{i,j}}{2}\le n<\frac{Q_{i,j}}{2} \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

Where $c_0=1-e^{-\lambda_{ML}Q_{i,j}/2}$; and for the nonzero values

$$P(N=n\,|\,Y=y)=$$

$$\begin{cases} \frac{1}{c_1}e^{-sgn(y)\lambda_{ML}(n+q/2)} & \text{if } \frac{-Q_{i,j}}{2}\le n<\frac{Q_{i,j}}{2} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

Where $c_1=\frac{1}{\lambda_{ML}}\left(1-e^{-\lambda_{ML}Q_{i,j}}\right)$.

3. Countering Anti-Forensics

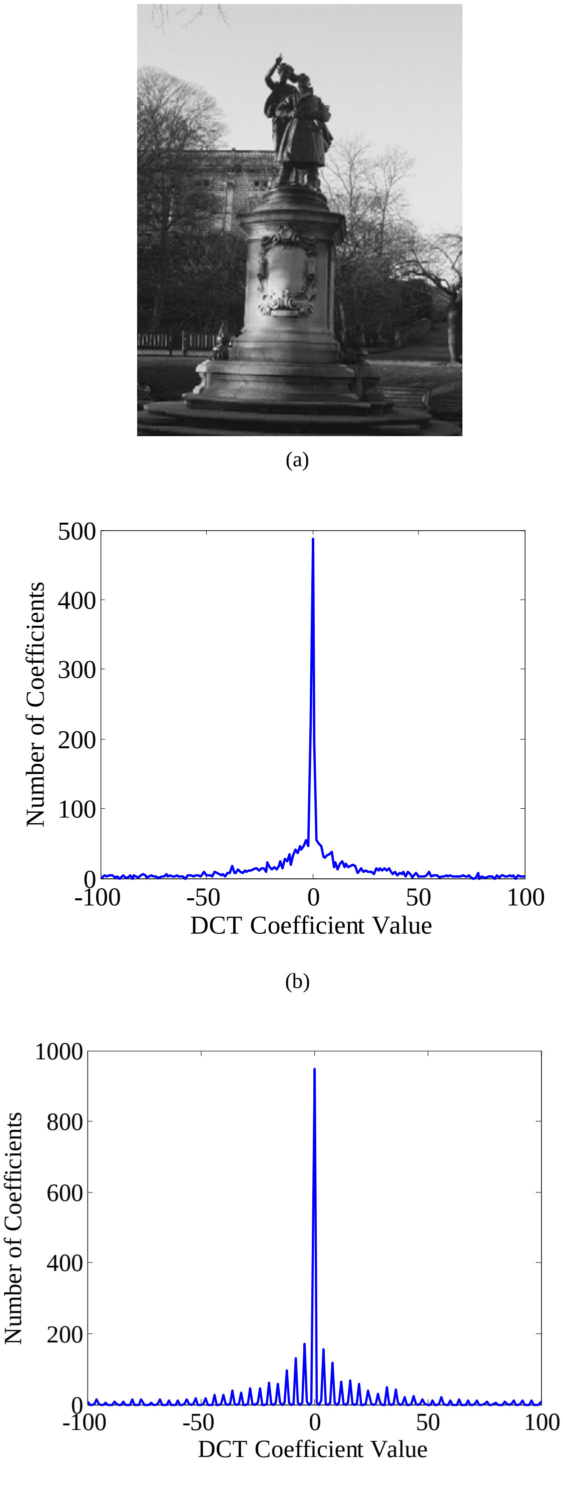
The key idea of Stamm and Liu's method is to pad the gaps appear in the histogram of each subband for AC components. However, when analyzing the decimal values of the DCT coefficients, we find they are not distributed as Laplacian distribution in each subband for never-compressed images. As a result, 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,

$$H_{i,j}=hist(C_k^{i,j}) \tag{7}$$

Where *hist*(·) is the histogram function. The artifact of comblike 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.

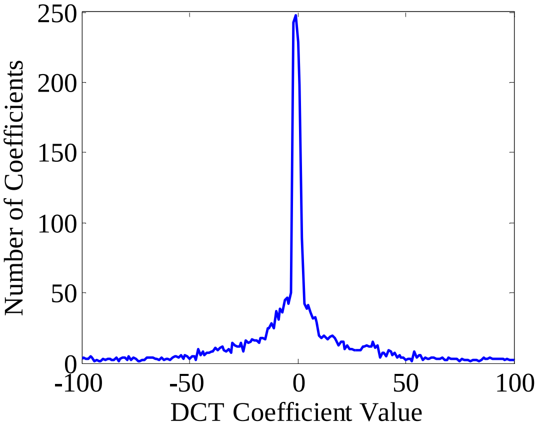
An example is shown in Figure 1, in which (a) is a never-compressed image, and the histogram of coefficients at position (1, 2) is shown in (b). If the image is compressed with quality factor 80, histogram of coefficients at the subband (1, 2) is changed into (c) that a comblike histogram with many gaps. After using Stamm and Liu.'s method, the gaps disappear, and again the histogram is approximately turned into a Laplacian distributed form, which is shown in (d).



(a)

(b)

(c)



(d)

Figure 1 (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.

In order to decide whether the image was processed by anti-forensics method, we round $C_k^{i,j}$ to the first decimal,

$$D_k^{i,j} = round(10 \cdot C_k^{i,j})/10 \qquad (8)$$

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

$$E_k^{i,j} = sgn(C_k^{i,j}) \cdot (D_k^{i,j} - round(D_k^{i,j})) \qquad (9)$$

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

$$H'_{i,j} = hist(E_k^{i,j}) \qquad (10)$$

We 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. Thus, we further define a function for identifying whether the image was compressed,

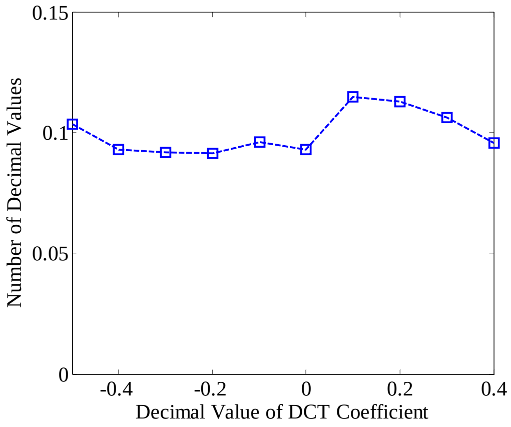
$$DIF_{i,j} = \max(H'_{i,j}) - \min(H'_{i,j}) \qquad (11)$$

and compare $DIF_{i,j}$ with a threshold *T*. The threshold we used here is 0.05, which comes from the training results shown in the following section. Finally, we can make a decision that the image was previously compressed if $DIF_{i,j} > T$; otherwise, it is uncompressed.

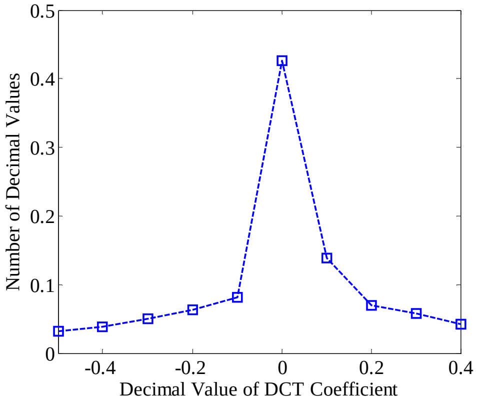
4. Experimental Results

To verify the proposed method, we choose the commonly used UCID database [13]. A group of decimal histograms are shown in Figure 2, in which (a) is the original never-compressed image, (b) the decimal histograms of (a). After JPEG encoding and decoding using quality factor 80, the decimal histogram corresponding to subband (1, 2) is shown in (c). Then we use Stamm and Liu's anti-forensics method to forge an uncompressed image, decimal histogram of which is shown in (d). The decimal histogram of the never-compressed image is near flat, while the other two histograms have clear peaks on zero.

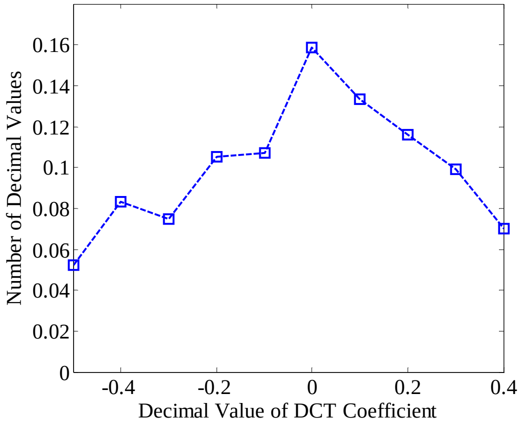
(a)



(b)



(c)



(d)

Figure 2 (a) a never-compressed image, (b) decimal histogram of (a) at the subband (1, 2), (c) decimal histogram at the subband (1, 2) of the compressed image with quality factor 80, (d) decimal histogram corresponding to the image processed by anti-forensics

To determine the threshold, we randomly use 200 images from the UCID database and turn them into grey 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. Figure 3 shows the values of $DIF_{1,2}$ for all images, which are used to determine the threshold for identifying whether an image was compressed or processed by anti-forensics. According to the results shown in Figure 3, we choose T=0.05.

We further use 400 never-compressed images for testing the proposed scheme. Experimental results are shown in Table 1. With the predefined threshold 0.05, 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.

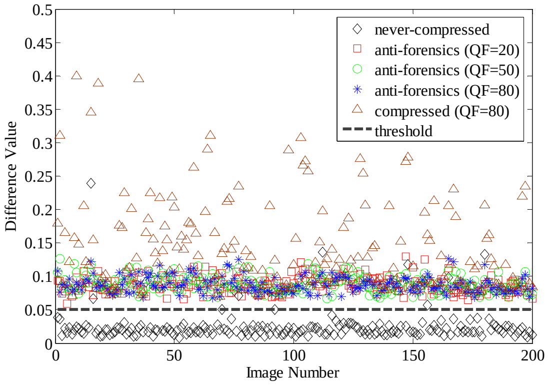


Figure 3 Threshold training using 200 images from UCID

Table 1 Detection Results

Decision	Never-Compressed	Stamm et al.'s Anti-forensics Processed		
		QF=80	QF=50	QF=20
True	91%	100%	100%	100%
False	9%	0	0	0

5. Conclusion

In this paper, 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. Experimental results show that with proper threshold high detection rates are achieved.

Acknowledgement

This work was supported by the Natural Science Foundation of China (Grant 61103181), the Natural Science Foundation of Shanghai (Grant 11ZR1413200), and the Innovation Program of Shanghai Municipal Education Commission (Grant 11YZ10).

References

[1] H. Farid, "Image forgery detection," *IEEE Signal Processing Magazine,* vol. 26, no. 2, pp. 16–25, Mar. 2009.

[2] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *6th International Workshop on Information Hiding*, Toronto, Canada, 2004.

[3] M. Kirchner and R. Böhme, "Synthesis of color filter array pattern in digital images," in *Proc. SPIE-IS&T Electronic Imaging: Media Forensics and Security*, Feb. 2009, vol. 7254.

[4] H. Farid, "Digital image ballistics from JPEG quantization," Tech. Rep. TR2006-583, Dept. of Computer Science, Dartmouth College, 2006.

[5] Z. Fan and R. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Trans. on Image Processing*, vol. 12, no. 2, pp. 230–235, Feb 2003.

[6] T. Pevny and J. Fridrich, "Detection of double-compression in JPEG images for applications in steganography," *IEEE Trans. on Information Forensics and Security*, vol. 3, no. 2, pp. 247–258, June 2008.

[7] J. He, Z. Lin, L. Wang, and X. Tang, "Detecting doctored JPEG images via DCT coefficient nalysis," in *Proc. of ECCV*, 2006, vol. 3593, pp. 423–435.

[8] M. Stamm, S. Tjoa, W. Lin, K. Liu, Anti-forensics of JPEG compression. In: IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP 2010), pp. 1694–1697. IEEE Press, Los Alamitos (2010)

[9] M. Stamm and K. Liu, "Anti-forensics of digital image compression," *IEEE Trans. Information Forensics and Security*, vol. 6, no. 3, pp. 1050 –1065, Sep. 2011.

[10] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we

trust digital image forensics?," in *15th Int. Conf. Multimedia*, 2007, pp. 78–86.

[11] M. Kirchner and R. Böhme, "Hiding traces of resampling in digital images," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 4, pp. 582–592, Dec. 2008.

[12] E. Y. Lam and J. W. Goodman, "A mathematical analysis of the DCT coefficient distributions for images," *IEEE Trans. Image Processing*, vol. 9, no. 10, pp. 1661–1666, Oct 2000.

[13] G. Schaefer and M. Stich, "UCID: an uncompressed color image database," in *Proc. SPIE: Storage and Retrieval Methods and Applications for Multimedia*, 2003, vol. 5307, pp. 472–480.

Zhenxing Qian received the B.S. degree in 2003 and the Ph.D. degree in 2007 from University of Science & Technology of China (USTC). Since 2009, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University. He is now an associate professor. His research interests include data hiding, image processing, and digital forensics.

Xinpeng Zhang received the B.S. degree in computational mathematics from Jilin University, China, in 1995, and the M.E. and Ph.D. degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently a Professor. His research interests include information hiding, image processing and digital forensics.