International Journal of Research Studies in Science, Engineering and Technology
Volume 1, Issue 6, September 2014, PP 8-13
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

Total Variation Based Forensics for JPEG Compression

P.M.Shelke

Assistant Professor
Department of Information Technology, VIIT
Pune, Maharashtra, India
kharade.priya@gmail.com

Bhavesh Kabra

Department of Information Technology, VIIT
Pune, Maharashtra, India
kabrabhavesh12@gmail.com

Amey Deole

Department of Information Technology, VIIT
Pune, Maharashtra, India
amey.deole@gmail.com

Abstract: *Compression is the fastest way to reduce redundancy of the image data to be able to store or transmit data in an efficient way. In the case of JPEG lossless compression the image can be reconstructed but in case of lossy compression nature of transform coding introduces characteristics traces in the compressed images. A forensic analyst can reveal these traces by analyzing discrete cosine transform (D.C.T) coefficients and exploit to identify copy-move forgery, local tampering. It has been recently shown that adversary can conceal traces of JPEG compression by adding noise signal in DCT domain, in order to restore the histogram of the original image. We take perspective of forensic expert and show how we show to counter anti-forensic method by using same Quantization matrix used.*

Keywords: *Forensic; JPEG compression*

1. Introduction

Due to availability of digital camera it is easy to take digital images. Images forms as a popular means of conveying information. The graphical editing software has allowed images to be easily manipulated producing an photo-realistic forgeries of original content has become a simpler task, even for non professional users in some cases the forged image can be used for malicious purpose. As a result number of researchers has developed computer based forensic algorithm to detect digital forgeries when they are visually convincing. [5][7][10] Forensic technique analyse the image content in order to find traces left by specific coding or editing operation.

JPEG image format is the most popular form of Image format used to represent Digital Images. JPEG is capable of producing very high-quality compressed images that are still far smaller than the original uncompressed data. JPEG was designed specifically to discard information that the human eye cannot easily see. JPEG was designed to compress color or gray-scale continuous-tone images of real-world subjects: photographs, video stills, or any complex graphics that resemble natural subjects.

The footprint left by JPEG compression plays an important role in detecting possible forgeries. The JPEG encoder quantizes each discrete cosine transform (D.C.T) of an image to multiples of quantization step size. Since the image is divided into blocks and each block is processed separately, it introduces compression footprints around the edges. The forensic expert can analyze the distribution of D.C.T. to reveal these traces.

When the image is decoded the distribution of reconstructed D.C.T coefficient differs from original. When an image is compress, the quantization steps quantize D.C.T value around similar values. Thus the D.C.T. coefficient exhibits characteristic comb-like shape using which we can detect quantization matrix. JPEG compression footprints can be concealed by adding a properly designed dithering noise signal by a knowledgeable adversary. It has been shown that adding noise signal to quantized D.C.T. coefficient can remove statistical footprint of JPEG compression.[2]

The core of proposed detector is recompress the questioned image by varying coding condition and analyze the amount of granny noise left by adversary. We design a anti-forensic detector which only needs to change at each compression round ,a pair of properly selected D.C.T. coefficient. This re-compress and observe paradigm is inspired to exploit idem potency property of quantization.

2. BACKGROUND

In this section we explain the basics of JPEG Compression and Corresponding footprints.

2.1 The JPEG Compression and its Footprints

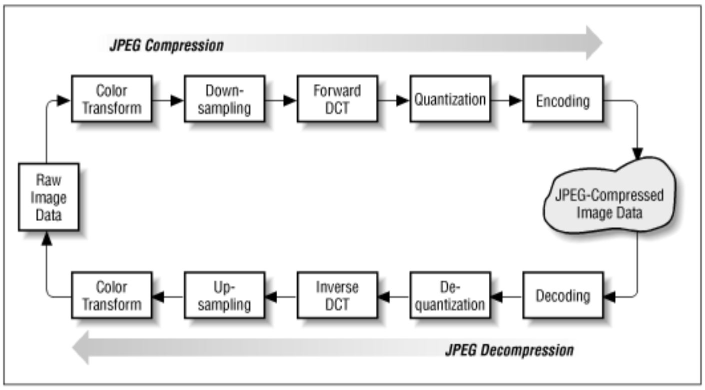

Fig 1. *Jpeg Compression process*

JPEG itself encodes each component in a colour model separately, and it is completely independent of any colour-space model, such as RGB, HSI, or CMY. The best compression ratios result if a luminance/chrominance colour space, such as YUV or YCbCr, is used. The luminance describes the brightness of the pixel while the chrominance carries information about its hue. These three quantities are typically less correlated than the (*R*, *G*, *B*) components. Furthermore, psycho-visual experiments demonstrate that the human eye is more sensitive to luminance than chrominance, which means that we may neglect larger changes in the chrominance without affecting our perception of the image.

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \begin{bmatrix} 0.29900 & 0.58700 & 0.11400 \\ -0.16874 & -0.33126 & 0.50000 \\ 0.50000 & -0.41869 & -0.08131 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}.$$

Fig 2. *RCB to YC_rC_b Conversion*

Since this transformation is invertible, we will be able to recover the *(R,G,B)* vector from the *(Y,C_b,C_r)* vector. This is important when we wish to reconstruct the image. (To be precise, we usually add 128 to the chrominance components so that they are represented as numbers between 0 and 255.). When we apply this transformation to each pixel in our block. We obtain three new blocks, one corresponding to each component. These are shown below where brighter pixels correspond to larger values. The image is then divided into 8 by 8 blocks of pixels. each 8×8 block of each component (Y, Cb, Cr) is converted to a frequency-domain representation, using a normalized, two-dimensional type-II discrete cosine transform (DCT)

$$G_{u,v} = \frac{1}{4}\alpha(u)\alpha(v)\sum_{x=0}^{7}\sum_{y=0}^{7} g_{x,y}\cos\left[\frac{(2x+1)u\pi}{16}\right]\cos\left[\frac{(2y+1)v\pi}{16}\right]$$

Fig 3. *Discrete Cosine Transform equation*

When a gray scale image undergoes JPEG compression, it inserts segmented into a series of 8×8pixel blocks, then the DCT of each block is computed. Next, each DCT coefficient is quantized by dividing it by its corresponding entry in a quantization matrix Q, such that a DCT coefficient X at the block position (i, j) is quantized to the value $\dot{X}$= round(X/$Q_{i,j}$). Finally, the quantized DCT coefficients are rearranged using the zigzag scan order and losslessly encoded.

To decompress the image, the sequence of quantized DCT coefficients is losslessly decoded then rearranged into its original ordering. De-quantization is performed by multiplying each quantized coefficient by its corresponding entry in the quantization matrix, resulting in the de-quantized coefficient Y=$Q_{i,j}$* X. Finally, the inverse DCT (IDCT) of each block of DCT coefficients is computed and the resulting pixel values are rounded to the nearest integer. Pixel values greater that 255 or less than 0 are truncated to 255 or 0 respectively, yielding the decompressed image.

Due to quantization process the de-quantized coefficient can only assume values that are integer multiples of quantization step size. Thus histogram of de-quantized coefficient of the ith sub-band appears to be comb shape with peaks spaces apart by quantization step size. We refer this characteristic comb shape of D.C.T. coefficient histogram as JPEG compression footprints. This process reveals two details, the first is that quantization process has occurred earlier and second is the original quantization step size can be revealed which was used.[1]

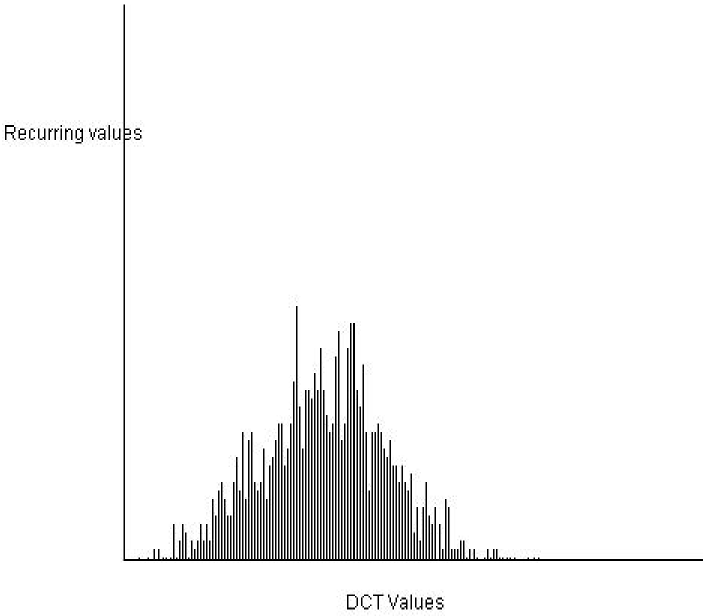

Fig 4. *Original Image Histogram*

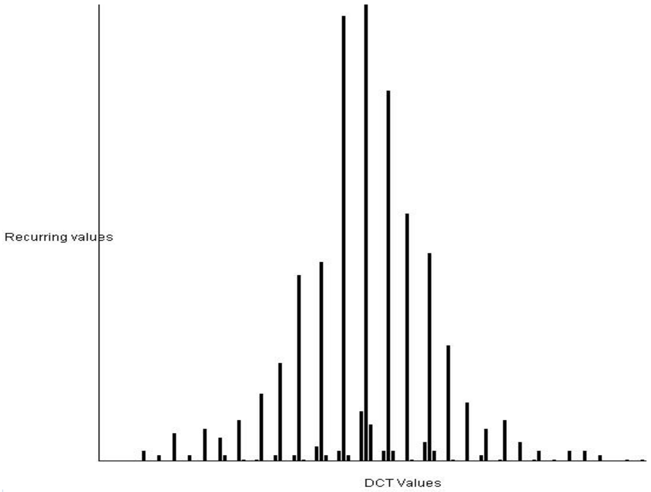

Fig 5. *Compressed Image Histogram*

2.2 JPEG compression Anti-Forensics

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.[2][3] 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. By assuming that the quantization table is known, he calculated maximum likelihood estimate ($\lambda_{ML)}$ of Laplacian parameter, $\lambda(i,j)$ for each DCT sub band. Next, to alter the comblike histograms caused by the discreteness of Laplacian distribution, he proposed the image dithering algorithm. [2][3][6].Noise is added into the AC coefficients to approximately reconstruct the histogram of each sub band, using,

$$Z = Y + N \tag{1}$$

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 λML = λ, 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.

3. Detection of JPEG Compression in Presence of Anti-Forensic

In practice we do not have access to the original JPEG compressed image in order to compute the M.S.E (Mean Square Error) distortion after re-quantization. [1][4][9] We observe that dithering signal can be detected using blind noisiness metric. We adopt the Total variation (TV) metric which is defined as L1 norm of spatial first order derivative. [8] Total Variation is more sensitive to small & frequent variation in pixel domain due to noise than abrupt changes in edges. It is widely adopted as part of objective function of optimizing algorithm used for de-noising. Other metric can also be used for de-noising.

We consider that we have the original JPEG coding is available i.e. quantization matrix belongs to family of quantization matrices corresponding to certain JPEG implementation. In many JPEG implementation and commercial photo editing software it is customary to use predetermined JPEG quantization matrix. The specification matrix is implicitly identified when user select target quality factor Q.

Forensic analyst may use the specific JPEG implementation that was originally used to encode the image he can readily generate 8x8 quantisation matrices given scalar quality factor QA. That is

$$\mathbf{Q}_{\mathbf{A}} = \mathbf{Q}_{\mathbf{A}}\,(Q_A) \tag{2}$$

where subscript A refers to quality factor used by analyst. He can then recompress the doubted image using different QA i.e. using different qualities for each compression of doubted image. For each compression is calculated.

$$TV(\mathbf{Q}_{\mathbf{A}}) = TV(\mathbf{Q}_{\mathbf{A}}\,(Q_A)) \tag{3}$$

The total variation increases smoothly when QA increases. As we approach to original quality at which image was compressed and added noise, there is sudden increase in the total variation value of an image for subsequent quality. This is due to effect that noise become visible as quality Q_A approaches to the quality Q at which compression occurred earlier. Thus we propose to analyse the total variation curve in order to devise detector that identifies when the traces of JPEG compression have been concealed by adversary. We can also determine quality factor Q.

In order to decide whether an image has been attacked we consider first order backward difference signal $\Delta TV(Q_A)$ obtained from the curve as

$$\Delta TV(Q_A) = TV(Q_A) - \Delta TV(Q_A-1) \tag{4}$$

$$\tau < \max(Q_A)\ \ \Delta TV(Q_A) \tag{5}$$

Where τ is the threshold parameter that can be adjusted by detector. We estimate quality factor Q' of the JPEG compressed image as

$$Q = (\arg\max \Delta TV(Q_A)) - 1 \tag{6}$$

Where -1 is used to compensate for the bias introduced by approximation by first order derivation

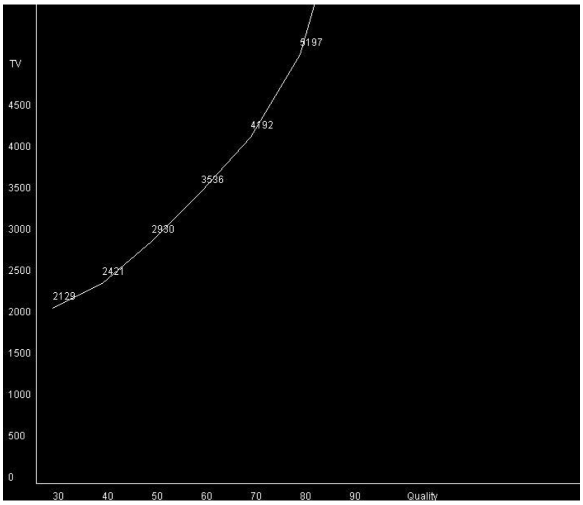

Fig 6. *Original Image*

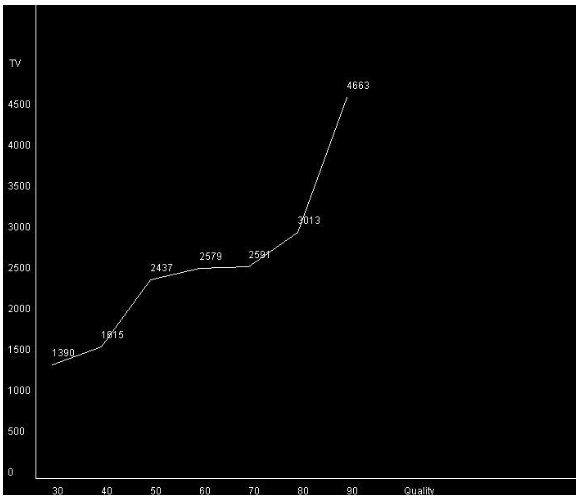

Fig 7. *Dithered Image*

4. Experiment

We gathered 90 images from various reliable sources . All the pictures in our dataset have a resolution of 320x240. We considered the luminance component only. We split the dataset in sets of equal size. The first half contained images that were JPEG-compressed at a random quality factor using the IJG implementation. More specifically, the quality factor is uniformly sampled in the set {30, 40, 50, 60, 70, 80, 90, 95} with probability 1/8. In order to restore the original statistics of the DCT coefficients, we added an anti-forensic dithering signal. The remaining half contained uncompressed original images.

Fig 6 and Fig 7 shows the graph of TV against quality factors. From Fig. 7, as shown in it if graph contains drastic changes in slope we can conclude that the image was previously compressed with that quality factor.

We were still able to detect the originality of image with a good accuracy.

5. Conclusion

JPEG compression leaves characteristics footprints which even on adding the noise the forensic analyst can detect the image originality. The paper investigates the problem of JPEG-compression anti-forensics, by showing how the forensic analyst can effectively counter the anti forensic method. Our analysis proves that removing traces of JPEG compression is quite possible in case of known quantization matrics. Removing the traces of JPEG compression, in case of unknown quantization matrics is left for future work.

REFERENCES

[1] Revealing the Traces of JPEG Compression Anti-Forensics" in IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 2, FEBRUARY 2013

[2] M. C. Stamm, S.K. Tjoa,W. S. Lin, and K. J. R. Liu, Anti-forensics of JPEG compression, in Proc. Int. Conf. Acoustics, Speech, and Signal Processing, Dallas, TX, Apr. 2010.

[3] M. C. Stamm and K. J. R. Liu, Forensic detection of image manipulation using statistical intrinsic fingerprints, IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492506, Sep. 2010.

[4] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, Countering JPEG anti-forensics, in Proc. Int. Conf. on Image Process., Bruxelles, Belgium, Sep. 2011.

[5] H. Farid, Image forgery detection, IEEE Signal Process. Mag., vol. 26, no. 2, pp. 1625, Mar. 2009

[6] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, Undetectable image tampering through JPEG compression anti-forensics, in Proc. Int. Conf. Image Process., Hong Kong, Sep. 2010, pp. 21092112.

[7] S. Y. Lai and R. Bohme, Countering counter-forensics: The case of JPEG compression, in Information Hiding. New York: Springer, 2011, pp. 285298.

[8] L. I. Rudin, S. Osher, and E. Fatemi, Nonlinear total variation based noise removal algorithms, Physica D: Nonlinear Phenomena, vol. 60, no. 14, pp. 259268, 1992

[9] G. Valenzise, M. Tagliasacchi, and S. Tubaro, The cost of JPEG compression anti forensics, in Proc. Int. Conf. Acoustics, Speech, and Signal Processing, Prague, Czech Republic, May 2011.

[10] F. Huang, J. Huang, and Y. Q. Shi, Detecting double JPEG compression with the same quantization matrix, IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 848856, Dec. 2010.