Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 4, April -2016

Graph Generation and Total Variation Forensics For JPEG Compression

P. S. Gaikwad, Gayatri Nanoti, Prajakta Wagh

Assistant Professor, Department of Computer Engineering, AISSMSIOIT, PUNE, Maharashtra, India
Department of Computer Engineering, AISSMSIOIT, PUNE, Maharashtra, India
Department of Computer Engineering, AISSMSIOIT, PUNE, Maharashtra, India

ABSTRACT -*The widespread availability of photo editing software has made it easy to create visuallyconvincing digital image forgeries. The field of anti-forensics seeks to developa set of techniques designed to fool current forensic methodologies. There exists atechnique for disguising an images JPEG compression history. An image's JPEGcompression history can be used to provide evidence of image manipulation, supplyinformation about the camera used to generate an image, and identify forged regionswithin an image. The technique includes proper addition of noise to an imagesdiscrete cosine transform coefficients which can sufficiently remove quantization artifacts,acts as indicators of JPEG compression while introducing an acceptable levelof distortion. A forensic analyst is able to counter above technique by using totalvariation concept of signal.*

Keywords*– JPEG Compression, Anti-forensic, DCT, Forensic, Histogram, Total Variation*

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. Forensic technique analyze the image content in order to find traces left by specific coding or editing operation.

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.

The core of proposed detector is recompress the questioned image by varying coding condition and analyze the amount of granny noise left by adversary. Systems designed, 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

2.1 THE JPEG COMPRESSION

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 thebrightness 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 wemay neglect larger changes in the chrominance without affecting our perception of the image.

$$\begin{vmatrix} Y \\ Cb \\ Cr \end{vmatrix} = \begin{vmatrix} 0.29900 & 0.58700 & 0.11400 \\ 0.16874 & -0.33126 & 0.50000 \\ 0.50000 & -0.41869 & -0.08131 \end{vmatrix} \begin{vmatrix} R \\ G \\ B \end{vmatrix}$$

Fig 1. *RCB to YCrCb Conversion Matrix Equation*

System will be able to recover the *(R,G,B)* vector from the *(Y,Cb,Cr)* vector i.e From Fig 1. This is important when 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 apply this transformation to each pixel in our block. System 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)

$G_{u,v} = \frac{1}{4}\alpha(u)\alpha(v)\Sigma\Sigma g_{x,y}AB$

Where, $A = \cos[\frac{(2x+1)u\pi}{16}]$

$B = \cos[\frac{(2y+1)v\pi}{16}]$

Fig 2. *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. The quantized DCT coefficients are rearranged using the zigzag scan order and losslessly encoded. 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/Qi,j). De-quantization is performed by multiplying each quantized coefficient by its corresponding entry in the quantization matrix, resulting in the de-quantized coefficient Y=Qi,j* X to decompress the image.

The sequence of quantized DCT coefficients is losslessly decoded then rearranged into its original ordering. 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.

Histogram of de-quantized coefficient of the i^{th} sub-band appears to be comb shape with peaks spaces apart by quantization step size. Due to quantization process the de-quantized coefficient can only assume values that are integer multiples of quantization step size. Refer this size ,characteristic comb shape of D.C.T. coefficient histogram as JPEG compression footprints.

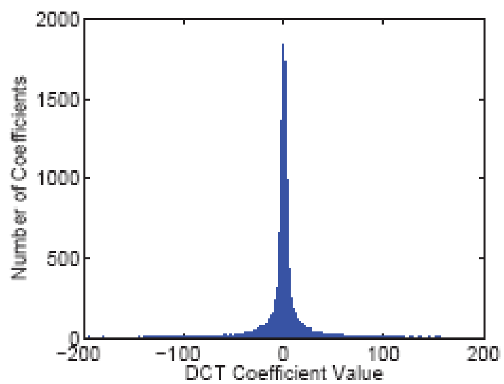

Fig 3.*Original Image Histogram*

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.

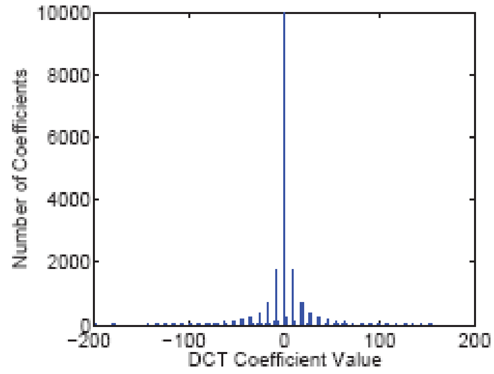

Fig 4. *Compressed Image Histogram*

2.2. ANTIFORENSIC APPROACH

First, estimated the distribution of the un-quantized DCT coefficients. According to the Laplace distribution un-quantized DCT coefficients as being distributed. By assuming that the quantization table is known, then calculated maximum likelihood estimate (λML) 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. Noise is added into the AC coefficients to approximately reconstruct the histogram of each sub band, using,

$$Z = Y + N \quad \text{--- (1)}$$

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.

3. DETECTION OF JPEG COMPRESSION

System adopt the Total variation (TV) metric which is defined as L1 norm of spatial first order derivative. 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. Observed that dithering signal can be detected using blind noisiness metric.

Assume, 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 used to encode the image he can readily generate 8x8 quantization matrices given scalar quality factor QA. That is

$$\mathbf{QA} = \mathbf{QA}(QA) \quad \text{--- (2)}$$

A refers to quality factor used by analyst. Recompress the doubted image using different QA

$$TV(\mathbf{QA}) = TV(\mathbf{QA}(QA)) \quad \text{--- (3)}$$

The total variation increases smoothly when QA increases. 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 QA approaches to the quality Q at which compression occurred earlier. In order to decide whether an image has been attacked we consider first order backward difference signal $\Delta TV(QA)$ obtained from the curve as

$$\Delta TV(QA) = TV(QA) - \Delta TV(QA-1) \quad \text{--- (4)}$$
$$\tau < \max(QA) \quad \Delta TV(QA) \quad \text{--- (5)}$$

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

$$Q = (\arg\max \Delta TV(QA)) - 1 \quad \text{--- (6)}$$

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

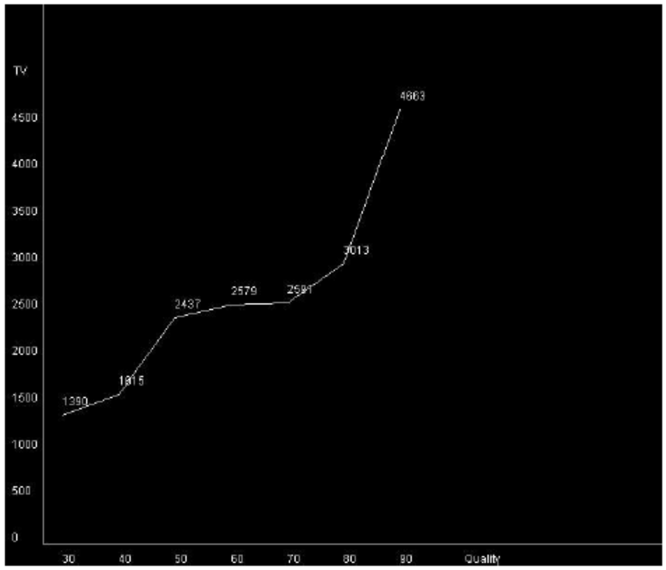

Fig 5. *Dithered Image Graph*

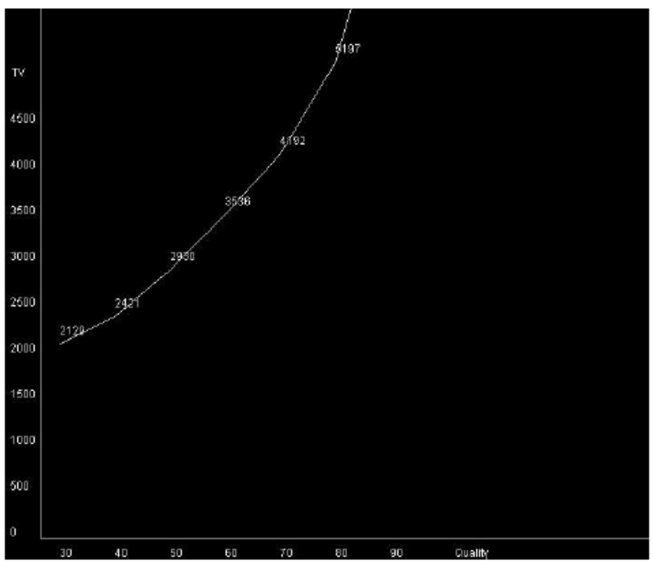

Fig 6. *Original Image Graph*

4. EXPERIMENTAL RESULT

From various reliable sources . All the pictures in our dataset have a resolution of 320x240. Split the dataset in sets of equal size. Considered the luminance component only. In first, JPEG-compressed at a random quality factor using the IJG implementation.

The quality factor is uniformly sampled in the set {30, 40, 50, 60, 70, 80, 90, 95} with probability 1/8. Then add an anti-forensic dithering signal, to restore the original statistics of the DCT coefficients. The second , contained uncompressed original images. Fig 5 and Fig 6 shows the graph of TV against quality factors. In the graph, if graph contains drastic changes in slope then can conclude that the image was previously compressed with that quality factor. System able to detect the originality of image with a good accuracy.

5. CONCLUSION

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

6. REFERENCES

[1] Giuseppe Valenzise, Marco Tagliasacchi and Stefano Tubaro “Revealing TheTraces of JPEG Compression Anti-Forensics in IEEE TRANSAC- TIONS ONINFORMATION FORENSICS AND SECURITY”, VOL. 8, NO. 2, FEBRUARY2013

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

[3] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting traces ofResampling”, IEEE Trans. Signal Process., vol. 53, no. 2, pp. 758767, Feb. 2005

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

[5] G. Valenzise, V. Nobile, M. Tagliasacchi, and S. Tubaro, “Countering JPEG antiforensics,in Proc. Int. Conf. on Image Process.”, Bruxelles, Belgium, Sep. 2011.

[6] J. Luk and J. Fridrich, “Estimation of primary quantization matrix in dou- blecompressed JPEG images”, in Proc. Digital Forensic Research Work- shop, 2003

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

[8] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, “Undetectable imagetampering through JPEG compression anti-forensics”, in Proc. Int. Conf. random quality factor using the IJG implementation. Image Process.,Hong Kong, Sep.2010, pp. 21092112.

[9] S. Y. Lai and R. Bhme, “Countering counter Forensics: The case ofJPEG compression”,in Information Hiding. New York: Springer, 2011, pp. 285298.

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