TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 5516-5522

Forgery Detection using Forward Quantization Noise method

Mr.Satish Pratapur
Research scholar
VTU regional office, Kalaburagi
Karnataka ,India
Contact No:9916464964
Email –Id: satish.pratapur@gmail.com

Shubangi D C
Professor
VTU regional office, Kalaburagi
Karnataka , India
Contact No:9886689209
Email –Id: drshubhangipatil1972@gmail.com

Article Info
Volume 83
Page Number: 5516 - 5522
Publication Issue:
May - June 2020

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *17 May 2020*

Abstract

In this work, the presence of forgery was detected using the forward quantization noise method. Required threshold to achieve maximum sensitivity, specificity and precision was derived for JPEG images. Seam carving dataset with a quality factor of 75% was used in order to demonstrate the method. The threshold was varied from 0.005 to 0.0005 and the corresponding maximum sensitivity, specificity and precision were estimated. It has been demonstrated that a threshold of 0.0005 yields that highest maximum sensitivity, specificity and precision.

Keywords: *Image forgery detection, JPEG, Forward quantization noise*

I. INTRODUCTION

Image forgery is becoming threat to the veracity of the image contents in a web portal or in the social media networks. There is a huge undesired growth in the image forgery of late leading to spread of false news there by creating false perception in the society. The forgery has been promoted by some anti social elements and there are special software tools being developed and used for this purpose. Forgery of an image basically deals with alteration of contents of the image. Image compression is one of the techniques used to forge an image. The image compression technique can be lossy or loss less. For example, JPEG is one of the popular techniques used in the image compression. The JPEG compression is lossy compression technique.

A forgery can be carried out to an image using JPEG compression methods. Usually, an image is altered and then it

is subjected to loss compression and then image is recovered back from compression. In such a scenario, when an image is regenerated back, it will be difficult to identify the tampered regions of the image. This problem can be addressed by analyzing the history of the JPEG compression [1, 2]. By studying the history in detail using mathematical tools, it is possible to determine to what extent the image was tampered. The extent of image compression can be assessed using mathematical methods [3, 4]. In fact it is also possible to determine if the image was compressed more than once. However, these methods are not sufficient to deal with the

detection of forgery as there is high quality compressions being performed by the professional hackers or manipulators.

Especially when images are decompressed of those images that were compressed with high quality JPEG, it becomes difficult, though not impossible to find if there was any forgery or tampering to the original image. When the compression is a high quality JPEG, the traces can be found only in few

May – June 2020
ISSN: 0193-4120 Page No. 5516-5522

high frequency discrete cosine transform coefficients. When an image is decompressed back into spatial domain, these traces can be observed. The traces can be observed easily when the DCT coefficients are plotted in histograms.

The DCT values can be utilized to verify if an image was compressed decompressed or uncompressed [4]. The DCT values in the range of -2 to 2 and its absolute value provides good information about the image compression. For example, Quantity of DCT values that lie between -2 to 2 can be used to determine if an image was uncompressed. In order to determine if an image was decompressed or uncompressed, the DCT values can be compared with a threshold and based on quantity or percentage of DCT coefficients beyond a threshold; it is possible to verify if an image was indeed decompressed or uncompressed. This method has a limitation. It considers only those DCT coefficients that are close to zero and the image is subjected to two quantization steps to verify.

An improvement over the method of comparing DCT coefficients [4] was made by computing the variance of the DCT coefficients [5, 6]. The basis for this method was, if the image was uncompressed, then the variance of high frequency DCT coefficients have smaller values and decompressed image will have values.

Other methods to verify if the image was decompressed or uncompressed was using JPEG grid position [7-11], quantization tables [12], following the steps of quantization [13-17] and other methods [18-23].

In the current research, the threshold for the variance of the DCT coefficients are derived to determine if the image has any tampered regions in it. Simulations are carried out on Seam carving dataset. The regions of the forgery has been identified and marked in the image. The threshold value has been varied for a quality factor of 75% and the accuracy metrics were analyzed.

In this paper, Sec I is dedicated for the introduction of the problem and important developments in the area of detecting forgery using DCT coefficients. Section II deals with the mathematical back ground of the solution. Section 3 mainly focuses on the simulations of the proposed model on the Seam carving dataset. This section also deals with the analysis of the metrics. Finally, important conclusions are drawn in Sec. IV.

II. JPEG COMPRESSION-FORGERY DETECTION IN AN IMAGE

Forward quantization method [24] is used in this work to verify if an image has any tampered region in it or not. Variation of DCT coefficients are compared with a threshold. The quality factor of the JPEG compression has an influence on the DCT coefficients. When quantization is applied on the DCT coefficients, it removes some information. When the image subjected to inverse DCT, the image obtained will have some loss of information. The loss of information can be used as measure to determine if the image has any tampered regions. In order to determine the tampered regions, the original image is treated as a combination of 8x8 blocks; and DCT, Quantization, dequantization and inverse DCT are applied on each of the 8x8 blocks.

In a DCT block, there are AC components and a DC component. The first element in the DCT block, that s DCT[1,1] is the DC component and it is the average of all the pixel intensities in the spatial domain. All other components in the DCT block other DCT[1,1] are AC components. Fig.1 shows the flow of the image in the forward quantization. Loss information is the main criteria to verify the decompressed or uncompressed images.

$$y = DCT_1 - DCT_2 \tag{1}$$

$$y = DCT_1 - \left[\frac{DCT_1}{QUANT75}\right] QUANT75, \quad QUANT75 \in N \tag{2}$$

where

y : Loss of information
DCT_1: First DCT matrix of coefficients
DCT_2: Second DCT matrix of coefficients
$QUANT75$: Quantization matrix for a quality factor of 75%

Quantization noise [24] has a distribution and may be expressed as

$$f_y = \sum_{k=-\infty}^{\infty} f_Y(k.QUANT75 + s), \quad and\ s \in \left[-\frac{QUANT75}{2}, \frac{QUANT75}{2}\right] \tag{3}$$

Where

May – June 2020
ISSN: 0193-4120 Page No. 5516-5522

f_y: Distribution of loss of information with Gaussian distribution
f_Y Distribution of DCT coefficients with Laplacian distribution
Forward quantization noise can be written as

$$Z = Y - [Y] \quad (4)$$

Since Y and [Y] have distribution, the Z has a variation. Hence variation of Z can be used to verify of the image was decompressed or uncompressed.

$$Z = \begin{cases} Uncomp, if\ \sigma^2 > Thsld \\ Decomp, if\ \sigma^2 \leq Thsld \end{cases} \quad (5)$$

In the present work, the experiments are conducted to determine the threshold value for the Seam carving dataset for the presence of forgery in the JPEG images.

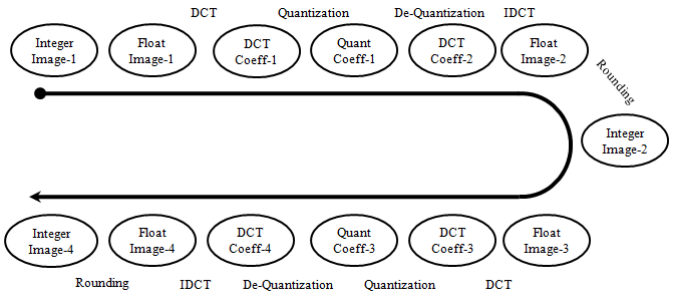

Figure 1: Flow diagram of tamper detection in JPEG

Algorithm:

Step 1: Read a JPEG image from the Seam Carving database.
Step 2: Define a quality factor and derive the quantization matrix using standard methods
Step 3: For first forward quantization, calculate the variance of the noise.
Step 4: For second forward quantization, calculate the variance of the noise.
Step 5: Define a threshold value. The threshold value is usually dependent on variances of first and second quantization noise.
Step 6: Compare the variance of the noise of first forward quantization with the threshold.
Step 7: Classify it as untampered, if it is less than or equal to the threshold. And if it is more than the threshold, then classify it as tampered.
Step 8: Read tampered JPEG images from the Seam Carving database.
Step 9: For first forward quantization, calculate the variance of the noise.
Step 10: For second forward quantization, calculate the variance of the noise.
Step 11: Define a threshold value. The threshold value is usually dependent on variances of first and second quantization noise.
Step 12: Compare the variance of the noise of first forward quantization with the threshold.
Step 13: Classify it as untampered, if it is less than or equal to the threshold. And if it is more than the threshold, then classify it as tampered.
Step 14: Mark the DCT blocks that are tampered.
Step 15: Mark the regions of all DCT blocks identified as tampered.
Step 16: Vary the threshold from 0.0005 to 0.005.
Step 16: Print the confusion matrix

III. Simulation Results

In this work, simulations are carried out for the Seam carving data base. One hundred images are taken from the database each from the tampered and untampered sets. The simulations are conducted to determine the percentage of forgery on the image. For the purpose of testing, an image is tested in both tampered and untampered conditions. Fig. 2 shows three samples of untampered and tampered images from the seam carving dataset. In each of figures 1a, 1b and 1c, left side image is the untampered image and right side image is the tampered image. The tampered portion in tampered image is highlighted with rectangular box after applying the proposed algorithm.

(a)

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 5516-5522

(b)

(c)

Figure 2: Three samples of untampered (left) and tampered images (right) from the Seam_Carving_Q75dataset

In the simulations, the untempered images were detected as untampared, which is true positives in 100% of the test cases. But the tampered images were detected as untampered in some cases. The percentage of forgery in the image is compared with a threshold in order to determine the optimal threshold that will ensure maximum specificity and precision. The threshold value is varied at 0.005, 0.002, 0.001, 0.0005 and 0.0001.

For a threshold value of 0.005, the confusion matrix is

	Actual		
Predicted	100 (TP)	52 (FP)	Total
	0 (FN)	48 (TN)	100
Total	100	100	100

True Negatives (TN)= 48
True Positives (TP) = 100
False Negatives = 0
False positives (FP) = 52
Total Positive class = 100 (Untampered)
Total Negative class = 100 (Tampered)

Sensitivity = (TP)/(TP+FN)
= 100 / (100+0)
= 100%

Specificity = (TN)/(TN+FP)
= 48/ (48+52)
= 48%

Precision = (TP)/(TP+FP)
= 100 / (100+52)
= 66%

From the above results, it can be observed that sensitivity is 100% which means all untampered images were detected by the model as untampered in all the cases. This is a very performance. In case of tampered images, only 48 out of 100 were detected as tampered and the remaining 52 were detected as untampered. Hence the specificity is 48% and precision is 66%.

For a threshold value of 0.002, the confusion matrix is

	Actual		
Predicted	100 (TP)	23 (FP)	Total
	0 (FN)	77 (TN)	100
Total	100	100	100

True Negatives (TN)= 77
True Positives (TP) = 100
False Negatives (FN) = 0
False positives (FP) = 23
Total Positive class = 100 (Untampered)
Total Negative class = 100 (Tampered)

Sensitivity = (TP)/(TP+FN)
= 100 / (100+0)
= 100%

May – June 2020
ISSN: 0193-4120 Page No. 5516-5522

Specificity = (TN)/(TN+FP)
= 77 / (77+23)
= 77%

Precision = (TP)/(TP+FP)
= 100 / (100+23)
= 81%

From the above results, it can be observed that sensitivity is again 100%. In case of tampered images, only 77 out of 100 were detected as tampered and the remaining 23 were detected as untampered. Hence the specificity is 77% and precision is 81%. When the threshold was decreased from 0.005 to 0.002, the specificity and precision increased significantly.

For a threshold value of 0.001, the confusion matrix is

	Actual		
Predicted	100 (TP)	8 (FP)	Total
	0 (FN)	92 (TN)	100
Total	100	100	100

True Negatives (TN)= 92
True Positives (TP) = 100
False Negatives (FN) = 0
False positives (FP) = 8
Total Positive class = 100 (Untampered)
Total Negative class = 100 (Tampered)

Sensitivity = (TP)/(TP+FN)
= 100 / (100+0)
= 100%

Specificity = (TN)/(TN+FP)
= 92 / (92+8)
= 92%

Precision = (TP)/(TP+FP)
= 100 / (100+8)
= 93%

For a threshold value of 0.0005, the confusion matrix is

	Actual		
Predicted	100 (TP)	1 (FP)	Total
	0 (FN)	99 (TN)	100
Total	100	100	100

True Negatives (TN)= 99
True Positives (TP) = 100
False Negatives (FN) = 0
False positives (FP) = 1
Total Positive class = 100 (Untampered)
Total Negative class = 100 (Tampered)

Sensitivity = (TP)/(TP+FN)
= 100 / (100+0)
= 100%

Specificity = (TN)/(TN+FP)
= 99 / (99+1)
= 99%

Precision = (TP)/(TP+FP)
= 100 / (100+1)
= 99%

For a threshold value of 0.0001, the confusion matrix is

	Actual		
Predicted	100 (TP)	1 (FP)	Total
	0 (FN)	99 (TN)	100
Total	100	100	100

True Negatives (TN)= 99
True Positives (TP) = 100
False Negatives (FN) = 0
False positives (FP) = 1
Total Positive class = 100 (Untampered)
Total Negative class = 100 (Tampered)

Sensitivity = (TP)/(TP+FN)
= 100 / (100+0)
= 100%

Specificity = (TN)/(TN+FP)
= 99 / (99+1)
= 99%

Precision = (TP)/(TP+FP)
= 100 / (100+1)
= 99%

When the threshold value decreased from 0.002 to 0.001, 0.0005 and 0.0001, the sensitivity remains at 100% for untampered images. In case of tampered images, finally 99 out of 100 were detected as tampered and the remaining 1 was detected as

untampered. Hence the specificity and precision increased to 99%. Any further decrease in the threshold did not improve the specificity and precision, which is evident when the threshold was reduced from 0.0005 to 0.0001. Hence the threshold can be fixed either at 0.0005 or 0.0001 for this dataset.

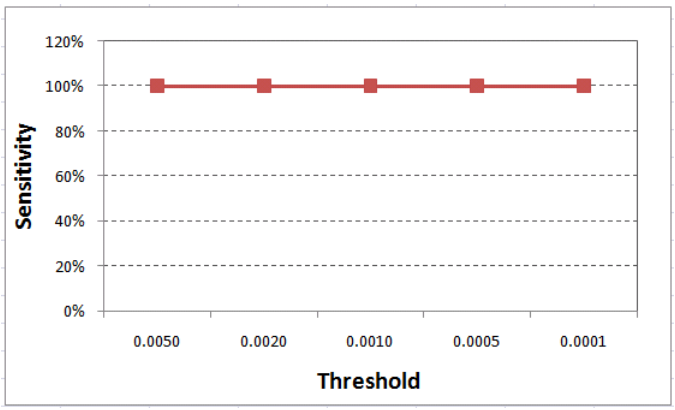

Figure 3: Sensitivity of the proposed method on Seam_Carving_Q75dataset

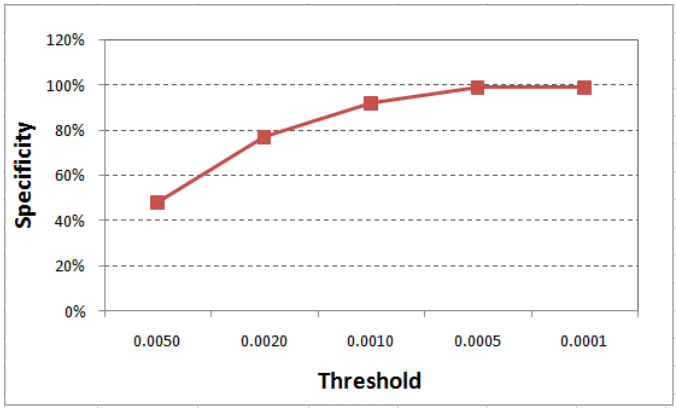

Figure 4: Specificity of the proposed method on Seam_Carving_Q75dataset

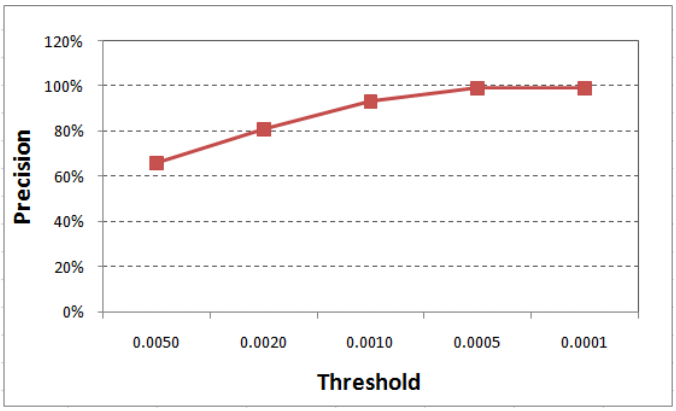

Figure 5: Precision of the proposed method on Seam_Carving_Q75dataset

Figs. 3, 4 and 5 show the change in sensitivity, specificity and precision for the 100 images of Seam carving Q75 dataset. It can be observed from Fig. 2 that sensitivity remain constant at 100% at all the thresholds. Specificity changes from 48% to 99% when the threshold was decreased from 0.005 to 0.0005 and to 0.0001. It becomes asymptotic thereafter. Similarly, the precision increases 66% to 99% when the threshold was decreased from 0.005 to 0.0005 and to 0.0001. It becomes asymptotic thereafter.

IV. CONCLUSIONS

In this work, the forward quantization noise technique [34] was enhanced and the same was applied to detect the tempered and untampered portions in the JPEG images. The method uses the quantization noise as a measure to determine if there is any forgery exists in the image. The feed forward noise was compared with a threshold to determine the forgery. To test the performance of the method, Seam carving dataset with a quality factor of 75% was used. The threshold was decreased from 0.005 to 0.0001. It has been observed that sensitivity remains at 100% in all the cases. But the specificity was very low at 48% when the threshold was set at 0.005. When the threshold was reduced in decrements to 0.0005, the specificity increased significantly to 99% and then by further reducing the threshold to 0.0001, the specificity remains at 99%. The precision also increased from 66% to 99% when the threshold was reduced in decrements from 0.005 to 0.0005 and no change observed thereafter. Hence it is concluded that for the Seam carving dataset, the threshold may be fixed at 0.0005 to obtain highest sensitivity, specificity and precision.

REFERENCES

[1] A. Piva, "An overview on image forensics," *ISRN Signal Process.*, vol. 2013, pp. 1–22, Nov. 2013.

[2] M. C. Stamm, M. Wu, and K. J. R. Liu, "Information forensics: An overview of the first decade," *IEEE Access*, vol. 1, pp. 167–200, May 2013.

[3] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and

May – June 2020
ISSN: 0193-4120 Page No. 5516-5522

quantizer estimation," *IEEE Trans. Image Process.*, vol. 12, no. 2, pp. 230–235, Feb. 2003.

[4] W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 480–491, Sep. 2010.

[5] S. Lai and R. Böhme, "Countering counter-forensics: The case of JPEG compression," in *Proc. 13th Int. Conf. Inf. Hiding Workshop* (Lecture Notes in Computer Science), vol. 6958, Prague, Czech Republic, 2011, pp. 285–298.

[6] J. Fridrich, "Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes," in *Proc. 6th Int. Workshop Inf. Hiding*, vol. LNCS 3200. 2005, pp. 67–81.

[7] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, vol. 2. Apr. 2007, pp. II-217–II-220.

[8] Z. Qu, W. Luo, and J. Huang, "A convolutive mixing model for shifted double JPEG compression with application to passive image authentication," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Las Vegas, NV, USA, Mar./Apr. 2008, pp. 1661–1664.

[9] Y.-L. Chen and C.-T. Hsu, "Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 396–406, Jun. 2011.

[10] Q. Liu, "Detection of misaligned cropping and recompression with the same quantization matrix and relevant forgery," in *Proc. 3rd ACM Int. Workshop Multimedia Forensics Intell.*, 2011, pp. 25–30.

[11] T. Bianchi, A. Piva, and F. Perez-Gonzalez, "Near optimal detection of quantized signals and application to JPEG forensics," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Guangzhou, China, Nov. 2013, pp. 168–173.

[12] D. Fu, Y. Q. Shi, and W. Su, "A generalized Benford's law for JPEG coefficients and its applications in image forensics," *Proc. SPIE, Secur., Steganogr., Watermarking Multimedia Contents IX*, vol. 6505, pp. 65051L-1–65051L-11, Feb. 2007.

[13] J. Fridrich, M. Goljan, and R. Du, "Steganalysis based on JPEG compatibility," *Proc. SPIE, Multimedia Syst. Appl. IV*, vol. 4518, pp. 275–280, Nov. 2001.

[14] R. N. Neelamani, R. de Queiroz, Z. Fan, S. Dash, and R. G. Baraniuk, "JPEG compression history estimation for color images," *IEEE Trans. Image Process.*, vol. 15, no. 6, pp. 1365–1378, Jun. 2006.

[15] S. Ye, Q. Sun, and E.-C. Chang, "Detecting digital image forgeries by measuring inconsistencies of blocking artifact," in *Proc. IEEE Int. Conf. Multimedia Expo*, Beijing, China, Jul. 2007, pp. 12–15.

[16] T. C.-I. Lin, M.-K. Chang, and Y.-L. Chen, "A passive-blind forgery detection scheme based on content-adaptive quantization table estimation," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 4, pp. 421–434, Apr. 2011.

[17] F. Galvan, G. Puglisi, A. R. Bruna, and S. Battiato, "First quantization matrix estimation from double compressed JPEG images," IEEE Trans. Inf. Forensics Security, vol. 9, no. 8, pp. 1299–1310, Aug. 2014.

[18] J. Seuffert, M. Stamminger, C. Riess, "Towards forensic exploitation of 3-D lighting environments in practice", *Proc. SICHERHEIT*, pp. 159-169, Apr. 2018.

[19] S. J. Nightingale, K. A. Wade, D. G. Watson, "Can people identify original and manipulated photos of real-world scenes?", *Cogn. Res. Princ. Implications*, vol. 2, no. 1, pp. 30, Jul. 2017.

[20] T. H. Thai, R. Cogranne, F. Retraint, T.-N.-C. Doan, "JPEG quantization step estimation and its applications to digital image forensics", *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 123-133, Jan. 2017.

[21] D. Cozzolino, G. Poggi, L. Verdoliva, "Splicebuster: A new blind image splicing detector", *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, pp. 1-6, Nov. 2015.

[22] M. Huh, A. Liu, A. Owens, A. A. Efros, "Fighting fake news: Image splice detection via learned self-consistency", *Proc. Eur. Conf. Comput. Vis. (ECCV)*, pp. 101-117, 2018.

[23] O. Mayer, M. C. Stamm, "Learned forensic source similarity for unknown camera models", *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, pp. 2012-2016, Apr. 2018.

[24] Bin Li, Tian-Tsong Ng, Xiaolong Li, Shunquan Tan, and Jiwu Huang, Revealing the Trace of High-Quality JPEG
Compression Through Quantization Noise Analysis, IEEE Transactions On Information Forensics And Security, vol. 10, No. 3, March 2015, pp 558-573.

Biography:

Mr. Satish Pratapur awarded BE degree in computer Science and Engineering from PDACE, Klb under VTU, Belgaum in the year 2008. M.Tech in the year 2012 from VTU, Belgaum and currently pursuing P.hD in Image processing from VTU, Belgaum and working as Asst.Prof in APPAIET, Klb. Sir has published 6 research papers in various conferences and journals.