Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 9; April-June, 2015 pp. 85-94

http://www.krishisanskriti.org/acsit.html

An Evaluation of Image Forgery Detection Methods using JPEG Compression Properties

Nilofar Zafar Siddiqui[1] and Manisha Dawra[2]

[1]M. Tech. Scholar Department of Computer Science and Engineering
Al-Falah School of Engineering and Technology Dhauj, Faridabad, Haryana, India
[2]Department of Computer Science and Engineering Al-Falah School of Engineering and Technology Dhauj, Faridabad, Haryana, India
E-mail: [1]nilofarzsiddiqui8@gmail.com, [2]manishadawra@gmail.com

Abstract—*Detection of forged images based on JPEG compression properties plays a very crucial role in image forensics. Nowadays, JPEG is the most commonly used compression standard. Most of the digital cameras in the market are mainly exporting JPEG file format. It is very important to identify whether an image has been previously JPEG compressed or not. Recently, few successful approaches have been presented, which, making use of the JPEG compression properties, give us various helpful details of the image under consideration. In this paper, we present an evaluation of image forgery detection methods(IFDM) using JPEG compression properties based on various parameters such as the method employed, the feature extracted, the classifier used, the detection accuracy achieved and the limitations identified. The objective of this paper is to identify the research gaps in IFDM.*

1. INTRODUCTION

Nowadays, with the advancement in digital computing, and better bandwidths available, images are being used as one of the primary sources of representing information in areas like print media, medical imaging, courtrooms and Internet [27]. Therefore, their authenticity is very crucial. Due to the ease and availability of image processing softwares, it has become very easy to manipulate the origin and content of digital images without leaving any obvious signs of tampering. Digital image forensics has come up with the intention of verifying the genuineness of images [2].

Techniques for detection of forged images can be classified as active or passive [2]. Active approaches such as digital watermarking and digital signatures require some pre-processing of the image and special hardware or software before the images are transmitted whereas the passive approaches do not[1, 2]. Passive techniques make use of the artifacts, and hence the inconsistencies introduced by digital forgeries to detect tampering in images [2]. The passive detection techniques can be based on tampering operations such as copy move, splicing, resampling, image processing operations or jpeg compression properties. A lot of research is going on in this field. In this paper, we analyze some of the major approaches of detecting forgery in digital images based on JPEG compression properties. We are considering both single and double compressions for our review.

Several approaches have been proposed in this direction recently. In [1], the methods for detection of forgeries based on copy move, splicing, retouching and lighting conditions have been compared but methods for detection of forgery using JPEG compression properties have not been discussed. Birajdar and Mankar in [2] presented a survey of digital image forgery detection using passive techniques. In this paper, they have also compared detection methods of few types of forgeries. As per our knowledge, there is no evaluation done on the IFDM using the JPEG compression properties on the basis of parameters such as method employed, features extracted, classifiers used, detection accuracy attained and the limitations identified. Therefore, it motivated us to evaluate the IFDM using JPEG compression properties on the basis of following parameters: method proposed, extracted feature, classifier, detection accuracy and limitations.

This paper is organised as follows: Section II presents the criteria for selection of parameters for evaluation of IFDM using JPEG compression properties. In section III, an evaluation of IFDM using JPEG compression properties is provided. Finally, conclusion and future work are given in Section IV.

2. CRITERIA

The main aim of passive detection techniques is to classify a given image as original or forged. Most of the existing passive forgery detection methods extract one or more features from the image, and based on these features extracted from training image sets, train the selected classifier to classify the image as authentic or not [2]. Our work of evaluating these passive techniques of detection of forged images using the JPEG compression properties is based on this structure of forgery detection and focuses on the features extracted and the classifier used.

3. AN EVALUATION OF THE FORGERY DETECTION METHODS USING JPEG COMPRESSION PROPERTIES

We have evaluated more than 25 proposed methods of detection of forged images using JPEG compression properties from the year 2003 to 2014. This evaluation is in the form of a comparative study of these methods on the basis of parameters of method proposed, extracted features, classifier and detection accuracy. Based on our analysis, the shortcomings or drawbacks of the given approaches are identified from the papers and expressed here. Our work can help the researchers in identifying new research areas to work on.

In 2003, Fan and Queiroz proposed a method using threshold detection to determine if an image has been JPEG compressed earlier and this detection could be made even when the QF was as high as 95. They also formulated a method to estimate compression parameters and quantization table used [3]. Three methods were proposed by Fridrich and Lukas in 2003 for primary quantization matrix estimation of which the one using neural network as classifier was the most accurate giving less than 1% of errors [2]. In 2008, Qu, Luo and Huang proposed a method to identify if the given JPEG image has ever been double compressed with inconsistent block segmentation. A total of 13 features of IVM were used with SVM as classifier to give more than 90% accuracy at QF of 95 [2]. In 2006, Junfeng et al. presented a method for detecting JPEG images which were doctored and also locating the doctored parts. This method is effective at a high compression quality [13]. In 2009, Mahidan and Saic used artifacts like double peaks and periodic zeros to detect double JPEG compression. SVM as classifier was used here giving a very less number of false positives [15]. Bianchi and Piva in 2012 gave an algorithm to detect non-aligned double JPEG compression in a digital image which was better in terms of accuracy as compared to other existing methods [21]. In 2014, Zhang and Rang-DingWang gave a method to detect an image's compression history automatically. Detectin accuracy was satisfactory [26]. Several other methods are given in Table 1.

4. CONCLUSION AND FUTURE WORK

Passive image forgery detection for verifying the integrity and authenticity of digital images is one of the rapidly growing topics in research field. In this paper, we evaluated IFDM using JPEG compression properties. Most of the algorithms are developed to detect image manipulation and few of them are also able to localize the forged areas. Based on our analysis, we have identified the research gaps in the field of image forgery detection. Future research agenda includes the following:

1. Automation of existing methods so that human interpretation is not needed to analyse the outputs.
2. Reduction of the size of databases in some of the methods as arge databases can be computationally demanding.
3. Extension of some of the methods used for monochrome images to color images.
4. Further extension of these research works to the areas of audio and video forgeries.
5. Establishment of benchmarks for evaluating the accuracy of the methods employed for detection.
6. Differentiation between malicious and innocent forgery depending upon the motive of the manipulator.
7. Further exploration of the uses of a source coder identification system.
8. Localization of tampered regions in an image is required but some of the methods only identify a tampered image but cannot localize the area of tampered region.
9. Reduction of high false positive rates in some cases.

We hope our work to be helpful to the researchers working in the area of digital image forgery detection in finding new and promising ideas and methods which can overcome the shortcomings of existing methods. Also, researchers can add to the parameters on the basis of which this evaluation table has been formulated and be more precise in describing the methods based on these parameters.

5. ACKNOWLEDGEMENTS

All authors thank Mohd. Sadiq at Jamia Millia Islamia for his generous help.

Table 1: Evaluation of IFDM using JPEG compression properties

Authors	Method	Extracted Feature	Classifier	Detection Accuracy	Limitations
Fan and Queiroz (2003)	A method to find if the image was JPEG compressed earlier and estimation of compression parameters and quantization table used [2].	Quantization Table [2]	Threshold Detection [3]	Detection is possible with QF as high as 95.	Results were presented for monochrome and not for color images. Also, it may fail to give an estimation at low bit rates. Its performance is also obstructed at very high bit rates [3]

Fridrich and Lukas (2003)	Three different approaches were proposed for primary quantization matrix estimation from a JPEG image which was double compressed of which the one using neural network as classifier was the most accurate [2].	Primary quantization matrix [2]	Neural Network [2]	Less than 1% of errors [2].	In order to get accurate results, satisfactorily large images are needed. Also, it is not possible to estimate quantization steps reliably for high-frequency coefficients due to inadequate statistics[2]
Popescu (2004)	Proposed a technique to detect whether an image in JPEG format was double compressed or not [2].	Histograms of the DCT coefficients [2]	Thresholding classification [5]	False positive rate = 0% . In general, the detection accuracies were nearly perfect. When first quality is 95, e.g., Q1 = 95 and Q2 = 80, the double quantization cannot be detected. For high first qualities and low second quality factors, e.g., Q1 = 90 and Q2 = 50, the detection accuracy is 50 % approximately [5].	It is hard to detect images that are first compressed using a high quality, and then using a significantly lower quality [2]. Method is open to attack too. Also, If we crop a manipulated JPEG image before re-saving it, the artifacts described, will be absent[5].
Neelamani et al. (2003)	Implemented a method to estimate image JPEG compression history components including the colour transformation, sub-sampling, and the quantization table employed during the previous JPEG operations [2].	DCT coefficients [2]	Not needed	Quantization step-size estimates, especially at the more important low DCT frequencies, is also accurate. The estimation errors for the L, a, and b color planes respectively are: 1.Quantization step-size estimation for the corresponding DCT frequency was not possible because all the DCT coefficients were quantized to zero during the compression. 2. The estimates for the a and the b planes suffer from seemingly large errors [4].	The dictionary-based CHEst approach would fail if an unknown proprietary color space was used to perform the JPEG compression [4].
Fu et al. (2007)	The generalized Benford's law can be used in the detection of JPEG compression for images in bitmap format, the estimation of JPEG compression Q factor for JPEG compressed bitmap image, and the detection of double compressed JPEG images [2].	Block-DCT and quantized JPEG coefficients [2]. For Detection of the JPEG compression for bitmap image: logarithmic function of the first digit distributions [7].	SVM[7]	For Detection of the JPEG compression for bitmap image, detection accuracy is 100% for Q factors- 99, 95, 90, 80, 70 and 60 [7]. For detecting double JPEG compression using the generalized Benford's law, the detection accuracy is only 30.91% by SSVM [9].	Estimation of the primary Q-factor in double compressed JPEG image is not given. Also, only 8-bit gray level images are considered in this work and not the color images [7].

Tjoa et al. (2007a)	To determine which transform was used during compression [2].	Histograms of coefficient subbands [22].	After calculating the relative entropy between the obtained histogram and the estimated original histogram for each subband, a final distance measure is obtained; if this measure is high, then the transform tested is classified as being the true transform used during compression. [22].	This method succeeds in classifying the transform used during compression among the six different transforms [22]. The three block transforms – DCT, Hadamard, and Slant and three wavelet transforms – 5/3, 9/7, and 17/11 were correctly determined [2].	Not many uses for a source coder identification system is apparent and needs to be explored further [22].
Tjoa et al. (2007b)[2]	To estimate the block size in digital images in a blind manner without making any assumptions on the block size or the nature of any previous processing [2].	Block artifacts that lossy coders leave behind [23].	Threshold detection [23].	Correctly classifies an image as block-processed with a probability of 95.0% and the probability of false alarm at 7.4% [2].	As block size increases, estimate is less accurate. Estimation for block sizes of 16, 32, and 64 fails for PSNR above 41.1 dB, 39.5 dB, and 38.6 dB, respectively. Furthermore, estimation accuracy is also data dependent, because high-frequency regions in an image can mask block artifacts [23].
Ye et al. (2007)	To detect digital forgeries by checking image quality inconsistencies. A blocking artifact measure is proposed based on the estimated quantization table using the power spectrum of the DCT coefficient histogram [2].	Based on blocking artifact caused by JPEG compression whose measure is based on the estimated quantization table using the power spectrum of the DCT coefficient histogram [2].	Classification is done based on blocking artifact inconsistencies [10].	Can successfully distinguish digital forgeries from original images [10].	Detect digital forgeries by checking image quality inconsistencies based on blocking artifacts caused by JPEG compression while it does not address other kinds of image quality inconsistency measures [10].
Zhang et al. (2009)	To detect and locate for the tampered areas in tampered images based on double JPEG2000 compression [2].	DWT coefficient histograms[2]	Threshold detection[9]	b1 is the bit rate when image is first JPEG2000 compressed and b2 when the image is second JPEG2000 compressed. The detection accuracies are good even in the case of b1= b2. The proposed approach can achieve an effective detection for double JPEG 2000 compression as well as accurate location for the tampered areas. [9]	If the ratio between the tampered part and the entire image is too high, the detection accuracy for double JPEG2000 compression will drop[9].

Luo et al. (2008)	For block size estimation based on morphological operation [2].	Block Artifacts[11]	To detect the block artifact boundaries introduced by compression schemes, a 2 × 2 cross-differential filter is used to eliminate the effect of the actual image contents, and then obtain a binary image from the filtered image in each dimension for subsequent block boundary detection. Erosion operation is employed to detect block artifact [11].	40% accuracy improvement compared with existing gradient-based method reported in Tjoa et al. (2007b)[2]. On average, this method can achieve 89.16% accuracy, while the gradient based method just has 50.01%.It is also observed that the larger the block sizes, the lower detection accuracy . Also, when the quality factor increases, the detection accuracy would decrease [11].	The potential applications of this method in image restoration and enhancement is not investigated[11].
Fridrich and Penvy (2008)	For detection of double compressed JPEG images and a maximum likelihood estimator of the primary quality factor. The algorithm not only detects cover images but also images processed using steganographic algorithms [2].	First order statistics of individual DCT modes of low frequency DCT coefficients [2].	Support vector machines [2].	Accuracy better than 90% [2]. The detection accuracies are about 97% for typical compression quality factors used in some steganographic algorithms, but drops sharply for some other quality factors [9].	In the case of Q1 = Q2, the double compression is undetectable, and the algorithm also needs much time to train the SSVM [9].
Qu et al. (2008)	For identifying if a given JPEG image has ever been compressed twice with inconsistent block segmentation [2].	Total of 13 features which represent the asymmetric characteristic of the independent value map [2].	SVM [2].	Accuracy of above 90% at QF of 95 [2].	The method did not address the color JPEG images and other blockwise compressed multimedia, such as JPEG2000 [12].
Chunhua et al. (2008)	To distinguish between double and single JPEG compressed images [2].	Markov process and transition probability matrix (TPM) applied to the difference JPEG 2-D arrays, which are of the second order statistics which detects the artifacts left with double JPEG compression [2].	SVM [24].	Improved Detection accuracy of 94% for some cases with high first quality factor and low second quality factor . When detecting the N/D case Q=70 vs. Q1/Q2=95/70, this proposed scheme can achieve the accuracy of 66.86%. .In another non-“N/D” case, Q=55 vs. Q1/Q2=70/55, this proposed scheme can achieve accuracy of 99.95%. [24].	When applying to the Shifted Double JPEG compression case, this method may be effective but its performance may degrade [24].

Junfeng et al. (2006)	To detect doctored JPEG images and locate the doctored Parts. The approach has several advantages like the ability to detect doctored images by different kinds of synthesizing methods , the ability to work without fully decompressing the JPEG images and the fast speed [2].	Double quantization effect hidden among the DCT coefficients [2].	SVM [13]	Method is effective for JPEG images, especially when the compression quality is high [13].	The method fails when the original image to contribute the undoctored part is not a JPEG image and in case of heavy compression after image forgery [2].
Farid (2009)	For detecting image composites created by different JPEG compression quality on low quality images and can detect relatively small regions that have been altered. The technique detects if part of an image was initially compressed at a lower quality than the rest of the image [2].	Spatially localized local minima in the difference between the image and its JPEG compressed counterpart. Under many situations, these minima,are termed JPEG ghosts [14].	Threshold detection [14]	Accuracy for images with no tampering is greater than 99% (i.e., a less than 1% false positive rate). Detection accuracy is above 90% for quality differences larger than 20 and for tampered regions larger than 100 × 100 pixels. The detection accuracy degrades with smaller quality differences and smaller tampered regions [14].	This technique is effective only when the tampered region is of lower quality than the image into which it was inserted [2].
Lin et al. (2009)	Constructed a fast, fully automatic method for detecting tampered images. The technique was insensitive to different kinds of forgery methods such as alpha matting and inpainting, in addition to simple image cut/ paste [2].	Double quantization effect hidden among the DCT coefficients [2].	SVM [2].	Effort is still needed to improve the accuracy. Some tampered images may not be detected and the detected tampered regions may not be 100% correct either. As the DQ effect breaks down when Q1 =Q2, the image level detection becomes random guess at Q2 = Q1. The average detection rates (averaged on Q2) are about 60% [8].	The method fails when the whole image is resized, rotated, or cropped[2].
Mahdian and Saic (2009)	Detection of double JPEG compressed image. The method exploits the fact that altering a JPEG image brings into the image specific artifacts like periodic zeros and double peaks [2].	Histograms of DCT coefficients [2].	SVM [2].	Almost–always when the image is double compressed and contains detectable artifacts, then both methods work well and detect the double compression. Nontheless, the method proposed in this paper produces a significantly less number of false positives [15].	The method produces high false positive to natural images with “nonperfect histograms” [2].

Huang et al. (2010)	Can detect double JPEG compression with the same quantization matrix. The method can also be extended to detect the triple JPEG compression, four times JPEG compression, and so on [2].	JPEG coefficients [2].	Threshold Detection[16]	If the QF is no less than 90, the final detection accuracy rates are constantly higher than 90% for UCID, NRCS, and OurLab image data set [2].	The key issue is the “proper” ratio of JPEG coefficients of the recompressed image that should be found [16].
Luo et al. (2010)	For image tamper detection including identifying whether a bitmap image has previously been JPEG compressed, quantization steps estimation and detecting the quantization table of a JPEG image [2].	By analyzing the effects of quantization, rounding and truncation errors [2].	Threshold Detection[17]	The method achieves accuracy of around 90% Eeven if the image size decreases to 8 × 8 and the quality factor is as high as 95 while identifying JPEG images, average accuracy is 81.97% for the images with size of 128 × 128 and with the quality factor 85 while estimating quantization steps, and the accuracy can achieve over 94.52% when the image size becomes larger than 64 × 64 while detecting quantization table [2].	Presented theoretical analysis and experimental results for gray-scale images, and not for color images [17].
Wang et al. (2010)	Can locate the tampered region in a lossless compressed tampered image when its unchanged region is output of JPEG decompressor [2].	PCA is employed to separate different spatial frequencies quantization noises, i.e. low, medium and high frequency quantization noise and extract high frequency quantization noise for tampered region localization [2].	Classification is done based on the presence of stronger high spatial frequency quantization noise in case of the tampered region as against the low frequency quantization noise in case of unchanged region.[18]	Effective algorithm but when the tampered region has little high frequency information, this method may fail [18].	Fails to detect forgery if the tampered region of a forged image has little high frequency information or the source image is saved in JPEG format with higher quality than the quality tampered image [2].
Bianchi and Piva (2011)	To detect the presence of non-aligned double JPEG compression (NA-JPEG) [2].	Single feature which depends on the integer periodicity of the DCTcoefficients when the DCT is computed according to the grid of the previous JPEG compression [2].	Threshold detector classifier [6]	The proposed detector achieves a higher detection accuracy than previously proposed methods and is able to analyze smaller images. Moreover, the proposed method is able to accurately estimate both the quantization step and the grid shift of the primary JPEG compression, which can be used to perform more advanced analyses [6].	Cannot identify NA-JPEG when the second compression uses the same quantization step as the primary compression. Also, cannot automatically localize tampered regions [6].

Chen and Hsu (2011)	To detect either block-aligned or misaligned recompression by formulating the periodic characteristics of JPEG images both in spatial and transform domains[2].	The periodicity of compression artifacts[19].	SVM [19]	Method works better with the smaller size of pasted patch. The detection rate does not always increase as increases when global operations such as additive white Gaussian noise or blurring are applied [19].	The approach is limited if a global operation such as additive white Gaussian noise or blurring are applied with a large distortion level before recompression [2].
Kee et al. (2011)	Extracts camera signature (9163 camera configurations) from a JPEG image to determine if an image has been modified in anyway [2].	Information about quantization tables, Huffman codes, thumbnails, and EXIF Format [2].	The signature and camera make and model are extracted From the EXIF metadata and compared against authentic image signatures extracted from the same camera make and model. To the extent that photo-editing software will employ JPEG parameters that are distinct from the camera's, any manipulation will alter the original signature, and can, therefore, be detected [20].	Although there is an ambiguity in some of the signatures, the signature still significantly constrains the identity of the camera make and model. Also, any photo-editing with Photoshop can be easily and unambiguously detected [20].	A determined forger could conceal their traces of tampering by extracting the signature of a camera, modifying the image, and then resaving the image with the appropriate EXIF format and all of the appropriate parameters in which case this method will fail. Also,vulnerable to a standard rebroadcast attack in which a digital image is manipulated, printed, and re-photographed. For large databases, this analysis can be computationally demanding [20].
Bianchi et al. (2011)	Applied a statistical test to differentiate between original and forged regions in JPEG images along with an estimation of the primary quantization factor in the case of double compression [2].	By computing probability models for the DCT coefficients of singly and doubly compressed regions [2].	Forgery detector is based on thresholding the probability map. After a thresholding step, a binary detection map is achieved, that locates which are the blocks detected as tampered. [25].	The new probability map has an improved accuracy that helps in discriminating forged and unchanged regions. The method is able to reveal tampering even if QF2 < QF1.[25]	Interpretation of the probability map is manual and not automatic. Also, there is a need to focus on the combination of such a result with the output of other multimedia forensics tools [25].
Bianchi and Piva (2012)	To detect into a digital image the presence of non-aligned double JPEG compression [2].	DCT coefficients [2].	Threshold Detector [21]	Improved accuracy with respect to existing methods and is able to accurately estimate the grid shift and the quantization step of the DC coefficient of the primary JPEG compression. Detector is from 5% to 15% more accurate for similar image sizes.[21].	Cannot automatically localize tampered regions [21].

Zhang and Rang-DingWang(2014)	To automatically detect the compression history of an image. This work aims at revealing the primary JPEG compression of a camera image especially when it has undergone an out-camera JPEG compression [26].	JPEG error between the given image and the recompressed version in the Y, Cb and Cr color channels [26].	In-camera and out-camera JPEG compression can be distinguished by comparing the dq curves of luminance and chrominance components. The in-camera compression is identified by examining whether the first minimum on the luminance dq curve is present on the chrominance curves [26].	Satisfactory detection accuracy, over 96 % accuracy rate for in-camera compression and no false positives with a block size of 512×512 [26].	1 1.Compressing an image at a lower quality factor than the previous compression will mask the earlier compression with a higher quality factor. 2 2.A difference between two compression qualities, i.e., the first and the second compression quality, is required. 3. This method may be attacked by misaligned JPEG compression [26].

REFERENCES

[1] Mushtaq, S., and Mir, A. H., "Digital Image Forgeries and Passive Image Authentication Techniques: A Survey", IJAST, Vol.73 (2014), pp.15-32.

[2] Birajdar, G. K., and Mankar, V. H., "Digital image forgery detection using passive techniques: A survey", Digital Investigation: The International Journal of Digital Forensics & Incident Response, Volume 10 Issue 3, October, (2013).

[3] Fan, Z., and Queiroz, R. L., "Identification of bitmap compression history: JPEG detection and quantizer estimation", IEEE Trans Image Process 2003; 12(2):230–5.

[4] Neelamani, R., Queiroz, R., Fan, Z., and Baraniuk, R., "Jpeg Compression History Estimation For Color Images", Proc. International conference on image processing, vol. 2. 2003. p. III–245–248.

[5] *Popescu, A. C., "Statistical* Tools for Digital Image Forensics", Thesis, Dartmouth College, Hanover, New Hampshire, December, (2004).

[6] Bianchi, T., and Piva, A., "Detection of non-aligned double JPEG compression with estimation of primary compression parameters", Proc. International conference on image processing 2011. p. 1929–32.

[7] Fu, D., Shi Y. Q., and Su. W., "A generalized Benford's law for JPEG coefficients and its applications in image forensics", Proc. SPIE electronic imaging: security, steganography, and watermarking of multimedia contents, vol. 6505. 2007. p. 65051L.

[8] Lin, Z., He, J., Tang, X., and Tang, C., "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis", Pattern Recognit 2009; 42(11): 2492–501.

[9] Zhang, J., Wang, H., and Su, Y., "Detection of Double-Compression in JPEG2000 Images for Application in Image Forensics", J Multimed 2009;4(6):379–88.

[10] Ye, S., Sun, Q., and Chang, E., "Detecting digital image forgeries by measuring inconsistencies of blocking artifact", Proc. IEEE International conference on multimedia and Expo (ICME) 2007. p. 12–5.

[11] Luo, W., Huang, J., and Qiu, *G.," A* Novel Method for Block Size Forensics Based on Morphological Operations", Proc. of International workshop on digital watermarking (IWDW) 2008. p. 229–39.

[12] Qu, Z., Luo, W., and Huang, J., "A convolutive mixing model for shifted double JPEG compression with application to passive image authentication", Proc. IEEE International conference on acoustics, speech and signal processing 2008. p. 1661–4.

[13] Junfeng, H., Zhouchen, L., Lifeng, W., and Xiaoou, T., "Detecting Doctored JPEG Images Via DCT Coefficient Analysis", Proc. of the 9th European conference on computer vision, vol. Part III. 2006. p. 423–35.

[14] *Farid, H., "* Exposing Digital Forgeries from JPEG Ghosts", IEEE Transactions on Information Forensics and Security, Volume 4 Issue 1, March 2009.

[15] Mahidan, B., and Saic, S., "Detecting Double Compressed JPEG Images", 3rd International Conference on Crime Detection and Prevention (ICDP 2009).

[16] Huang, F., Huang, J., and Shi, Y.Q., "Detecting double JPEG compression with the same quantization matrix", IEEE Trans Inf Forensics Security 2010; 5(4):848–56.

[17] Luo, W., Huang, J., and Qiu, G., "JPEG Error Analysis and Its Applications to Digital Image Forensics", IEEE Trans Inf Forensics Security 2010;5(3):480–91.

[18] Wang, W., Dong, J., and Tan, T., "Tampered Region Localization of Digital Color Images Based on JPEG Compression Noise", Proc. International workshop on digital watermarking 2010. p. 120–33.

[19] Chen, Y., and Hsu, C., "Detecting recompression of JPEG images via periodicity analysis of compression artifacts for tampering detection", IEEE Trans Inf Forensics Security 2011;6(2):396–406.

[20] Kee, E., Johnson, M.K., and Farid, H., "Digital Image Authentication From JPEG Headers", IEEE Trans Inf Forensics Security 2011;6(3):1066–75.

[21] Bianchi, T., and Piva, P., "Detection of non-aligned double JPEG compression based on integer periodicity maps", IEEE Trans Inf Forensics Security 2012;7(2):842–8.

[22] Tjoa, S., Lin, W.S., and Liu, K.J.R., "Transform Coder Classification For Digital Image Forensics", Proc. International conference on image processing (ICIP) 2007a. p. 105–8.

[23] Tjoa, S., Lin, W.S., Liu, K.J.R., and Zhao, H.V., "Block Size Forensic Analysis In Digital Images", Proc. IEEE International conference on acoustics, speech and signal processing 2007b. p. I-633–6.

[24] Chen, C., Shi, Y.Q., and Su, W., "A Machine Learning Based Scheme for Double JPEG Compression Detection", Proc. International conference on pattern recognition 2008. p. 1–4.

[25] Bianchi, T., Rosa, A.D., and Piva, A., "Improved Dct Coefficient Analysis For Forgery Localization in Jpeg Images", Proc. International conference on acoustics, speech and signal processing 2011. p. 2444–7.

[26] Zhang, R., and Wang, R., "In-camera JPEG compression detection for doubly compressed images", Multimed Tools Appl , Springer Science+Business Media New York (2014).

[27] Kusam, Abrol, P., and Devanand, "Digital Tampering Detection Techniques: A Review", BIJIT - BVICAM's International Journal of Information Technology, 2009.