Scientific Research Publishing

Journal of Computer and Communications, 2019, 7, 1-13
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

A Survey of Blind Forensics Techniques for JPEG Image Tampering

Xueling Chu, Haiming Li

College of Computer Science and Technology, Shanghai University of Electric Power, Shanghai, China
Email: chuxue0924@163.com

How to cite this paper: Chu, X.L. and Li, H.M. (2019) A Survey of Blind Forensics Techniques for JPEG Image Tampering. *Journal of Computer and Communications*, **7**, 1-13.
https://doi.org/10.4236/jcc.2019.710001

Received: August 19, 2019
Accepted: October 8, 2019
Published: October 11, 2019

Abstract

Blind forensics of JPEG image tampering as a kind of digital image blind forensics technology is gradually becoming a new research hotspot in the field of image security. Firstly, the main achievements of domestic and foreign scholars in the blind forensic technology of JPEG image tampering were briefly described. Then, according to the different methods of tampering and detection, the current detection was divided into two types: double JPEG compression detection and block effect inconsistency detection. This paper summarized the existing methods of JPEG image blind forensics detection, and analyzed the two methods. Finally, the existing problems and future research trends were analyzed and prospected to provide further theoretical support for the research of JPEG image blind forensics technology.

Keywords

Image Forensics, Tamper Detection, JPEG Image Forensics, JPEG Block Effect

1. Introduction

As a very important and effective information carrier in people's life, image describes objective objects in a simple, direct and vivid way. As image processing technology becomes more advanced, tampering technology becomes more and more complex, and the tampered and forged images are more and more difficult to be detected by the human eye. If image tampering occurs in important occasions such as military politics and courts, it will inevitably have an immeasurable and harmful impact on national security and stability as well as people's lives.

Active forensics and passive forensics are two main techniques of digital forensics. Active forensics technology refers to the technology of embedding fragile watermark or signature into digital image in advance and extracting watermark or signature for forensics. Digital image passive forensics technology,

namely blind forensics technology, is a kind of technology that verifies the authenticity and source of images without relying on pre-signature or pre-embedding information extraction [1]. Compared with active forensics, passive forensics has higher application and research value, but it is more difficult to obtain evidence than active forensics. JPEG, as one of the popular image formats at present, is also the image compression standard. Its advantage is that it can still obtain better image quality with relatively high compression rate and relatively fast processing speed. Therefore, the blind forensics research on JPEG tampered images has very important significance and application prospect. This paper briefly describes the main achievements in passive forensics of JPEG image tampering. Based on the different methods of tamper and detection, the current detection methods can be divided into dual JPEG compression detection method and JPEG block effect inconsistency detection method. The performance of representative methods of two kinds of detection methods is evaluated.

2. Double JPEG Detection

2.1. Double JPEG Image Compression Principle

The double compression of JPEG image means that after the JPEG image is decompressed, it is compressed with a new quantization table and stored again. When image software is used for image tampering, after the tampering is completed, the JPEG image may be compressed again with a quality factor different from the original image compression factor, that is, the dual JPEG image compression. It should be noted that when the first compression quality factor QF1 is equal to the second compression quality factor QF2, the characteristics of the image do not change significantly, in this case, the image is not called through JPEG compression. The image double compression process is shown in **Figure 1**: decompression of the original JPEG image is performed first, namely decoding and inverse quantization, followed by inverse DCT transformation, and the decompression image is finally compressed for a second time.

2.2. Double-JPEG Image Blind Forensics Algorithm

Researchers have developed many blind forensics algorithms for double-JPEG tampered images. The method of locating tampering areas by estimating the first compression quantization table of images [2] [3] [4] has been studied by many scholars. Farid uses different compression factors to re-compress the JPEG images

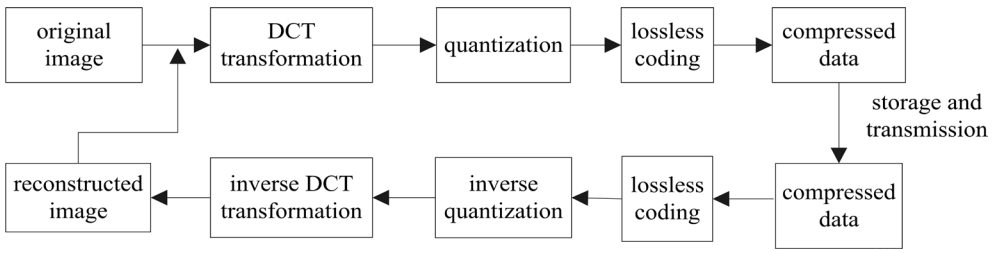

Figure 1. Double JPEG compression process.

to be detected. When the compression factor is equal to the compression factor of the tampered area, the statistical characteristics of the tampered area have little change in the degree of distortion, thus achieving the detection of the tampered area [5]. HE realized as a JPEG image tamper with the area of automatic detection and localization, this method can detect the different synthesis methods of image, without full decompression JPEG images can work, the speed, the experimental results show that the method of JPEG image compression effect is good, especially in the compression under the condition of high quality [6]. The estimated quantization step obtained by Fridrich *et al.* was extracted by estimating DCT coefficient and quantization step compatibility [7]. However, this method can only detect the image tampered with BMP format saved image, JPEG dual compression format is invalid.

The detection algorithm proposed above has relatively large limitations: literature [8] proposed an algorithm that can realize automatic detection of image tampering regions. The average probability density of histogram period is used to approximate the tampering region. Bayes theorem is used to calculate the posterior probability of a certain kind of image block. On the basis of literature [8], Duan Xintao *et al.* used particle swarm optimization algorithm to set an adaptive threshold to optimize the posterior probability density map, and classified and judged the threshold. Detection and separation of tampered areas were realized through the posterior probability density map [9]. Experimental results show that this method can automatically detect and extract the tampered areas quickly and accurately, and the detection results are significantly improved when the first quality factor is greater than the second quality factor.

Literature [10] [11] traverse all possible compression factors of the detected image, and try to carry out the third compression, and then analyze the degree of image distortion, which can detect the size of the original compression factor of the image to be detected. Smartphones are exploding in the market for imaging devices, with megapixels threatening traditional digital cameras. While smartphone images are widely distributed, images can be easily manipulated using a variety of photo editing tools. Therefore, smart phone image authentication and recognition after capture is an important content of digital forensics. Qingzhong Liu, *et al.* in order to improve the detection of pairs of JPEG compression, transplant JPEG steganographic analysis in the design of the adjacent joint density characteristics, and the joint density and DCT domain edge density characteristics of fusion, as a detector, learning classifier using edge density and adjacent joint density characteristics and identify the smartphone source and capture after operation [12].

JPEG double compressed image detection can be divided into compression detection based on different quantization and the same quantization matrix [13]. The feature classification and detection results of the specific algorithm are shown in **Table 1**, the recognition effect is comprehensively considered according to the detection time and detection effect described in the corresponding

Table 1. JPEG double compressed image feature classification and detection effect.

category		feature		recognition effect
different quantization matrix	block alignment	quantified DCT coefficients	the absolute difference values of the DC-AC coefficient and the AC-AC coefficient were calculated respectively [17]	general
			difference in histogram of quantization coefficient of DCT [15] [16]	good
			difference in DCT coefficients before and after compression [9]	good
		first significant digit [7] [17] [18]	the first significant number of DCT coefficient [14]	general
			DCT coefficient low-frequency point first significant digit [17]	good
			first significant digit of DCT coefficient based on Markov model [18]	excellent
	block is not aligned	difference in adjacent coefficients [19]		good
		percentage of JPEG coefficient [20]		good
		quantization noise [42]		excellent
identical quantization matrix		disturbance threshold [21]		general
		truncation error and rounding error [22]		good
		convergence of block property [23] (only for jpeg-100)		good

literature, which is recorded as "general", "good" and "excellent". In recent years, with the in-depth research of machine learning and deep learning, the method of deep learning is also applied in image forensics [24] [25] [26] [27] [28]. Literature [29] proposes a convolutional neural network detection algorithm based on double JPEG compression. Literature [30] and literature [31] respectively use naive Bayesian classifier and SVM classifier to detect and extract double JPEG compressed images. **Table 2** and **Table 3** are AUC values of three algorithms in literature [29] [30] and [31] respectively in two data sets. It can be concluded from the two table data that the algorithm in literature [29] is superior to the other two algorithms, especially in the case of QF2. Although the algorithm achieves good results, the computational complexity is obviously higher than the other two algorithms.

3. JPEG Block Effect Inconsistency Detection

3.1. Generation of JEPG Image Block Effect

In JPEG coding, the two-dimension DCT transformation is performed for each sub-block after partitioning. Although the computation of DCT transformation can be significantly reduced in this way, the correlation of pixel values between original sub-blocks may be ignored. In the next quantization stage, in order to achieve image compression, the quantization step size at the high frequency

Table 2. AUC values of literature [29], literature [30] and literature [31] in the large data set.

QF1 \ QF2		60	70	80	90
60	literature [29]	0.68	0.95	0.99	1.00
	literature [30]	0.50	0.97	0.99	0.99
	literature [31]	0.50	0.90	0.74	0.94
70	literature [29]	0.95	0.67	1.00	1.00
	literature [30]	0.85	0.48	1.00	0.99
	literature [31]	0.72	0.68	0.75	0.97
80	literature [29]	0.98	0.99	0.44	1.00
	literature [30]	0.90	0.93	0.44	1.00
	literature [31]	0.50	0.82	0.40	0.85
90	literature [29]	0.89	0.91	0.97	0.45
	literature [30]	0.68	0.67	0.82	0.50
	literature [31]	0.54	0.65	0.71	0.65

Table 3. AUC values of references [29] [30] and [31] in the small figure data set.

QF1 \ QF2		60	70	80	90
60	literature [29]	0.64	0.95	0.98	0.94
	literature [30]	0.53	0.95	0.97	0.95
	literature [31]	0.53	0.90	0.81	0.78
70	literature [29]	0.88	0.52	0.96	0.98
	literature [30]	0.82	0.54	0.95	0.95
	literature [31]	0.70	0.57	0.80	0.84
80	literature [29]	0.93	0.89	0.52	0.98
	literature [30]	0.69	0.84	0.54	0.96
	literature [31]	0.50	0.74	0.44	0.73
90	literature [29]	0.74	0.73	0.79	0.48
	literature [30]	0.69	0.73	0.75	0.60
	literature [31]	0.45	0.54	0.74	0.52

position is generally larger in the quantization table. Therefore, after quantization, most of the high frequency components at the edge of each subblock will be lost, resulting in discontinuity at the boundary of the block in the decoded image, thus forming the block effect [32]. The block effect of an untampered JPEG image should be the same, but the local block effect of the tampered image will be changed, and the block effect can be detected to determine whether the image has been tampered. The quantization step will lead to the loss of a lot of infor-

mation during JPEG compression, and the quantization error will be introduced during the rounding operation, denoted as $e(u, v)$, and the quantization step can be expressed as shown in formula (1): they are unavoidable.

$$F^{Q}(u,v) = round\left(\frac{F(u,v)}{Q(u,v)}\right) = \frac{F(u,v)}{Q(u,v)} + e(u,v),\ \ u,v = 0,1,\cdots,7 \tag{1}$$

The reverse quantization operation is carried out at the decoding end, as shown in formula (2), the DCT coefficient after the reverse quantization is obtained:

$$F(u,v) = F^{Q}(u,v) \times Q(u,v) = F(u,v) + e(u,v) \times Q(u,v),\ \ u,v = 0,1,\cdots,7 \tag{2}$$

Then DCT inverse transformation is carried out to obtain the decoded image, so that the distribution of decoding quantization error $e(u, v) \times Q(u, v)$ can be obtained in the whole decoded image. The decoding quantization error will be superimposed during the block processing of JPEG image, and then the decoding will break the correlation between each sub-block in the image, so the block-effect phenomenon is formed at the sub-block boundary.

3.2. Algorithm Based on JEPG Image Block Effect

In recent years, domestic and foreign researchers have proposed many algorithms to eliminate the block effect [33]-[38], but these algorithms in the block effect is used to eliminate the blurred image at the same time be tampering with the evidence, so the algorithm of image block effect to eliminate only able to increase the quality of compressed image, JPEG tampering with the harsh conditions of image blind forensics has not improved. Literature [39] first proposed a fast and effective method to detect JPEG block effect, that is, if there is no compression, the difference between adjacent pixels intersecting the block boundary should be similar to the difference between adjacent pixels within the block, but the difference between adjacent pixels intersecting the block boundary will be different after JPEG compression. **Figure 2** shows the difference between the pixels within each 8 × 8 block with an intersecting block boundary with a compression quality factor of 85 in Lena image, as shown in formula (3):

$$\begin{aligned} Z'(x,y) &= |A + D - B - C| \\ Z''(x,y) &= |E + H - F - G| \end{aligned} \tag{3}$$

where (x, y) represents the coordinates of A position in each block. By calculating the histogram of $Z'(x,y)$ and $Z''(x,y)$ of 3 positions (4, 4), (2, 4) and (3, 3), the difference strength of block effect of H1 and H2 is shown in formula (4):

$$K_{(x,y)}(n) = |H_1(n) - H_2(n)|,\ \ n \in [0.255 \times 2] \tag{4}$$

In this formula, $H_1(n)$ and $H_2(n)$ respectively represent the total number of bin values of n in the histogram of Z' and Z''. It can be seen that the block effect difference of JPEG image is the largest at the intersection of block boundary.

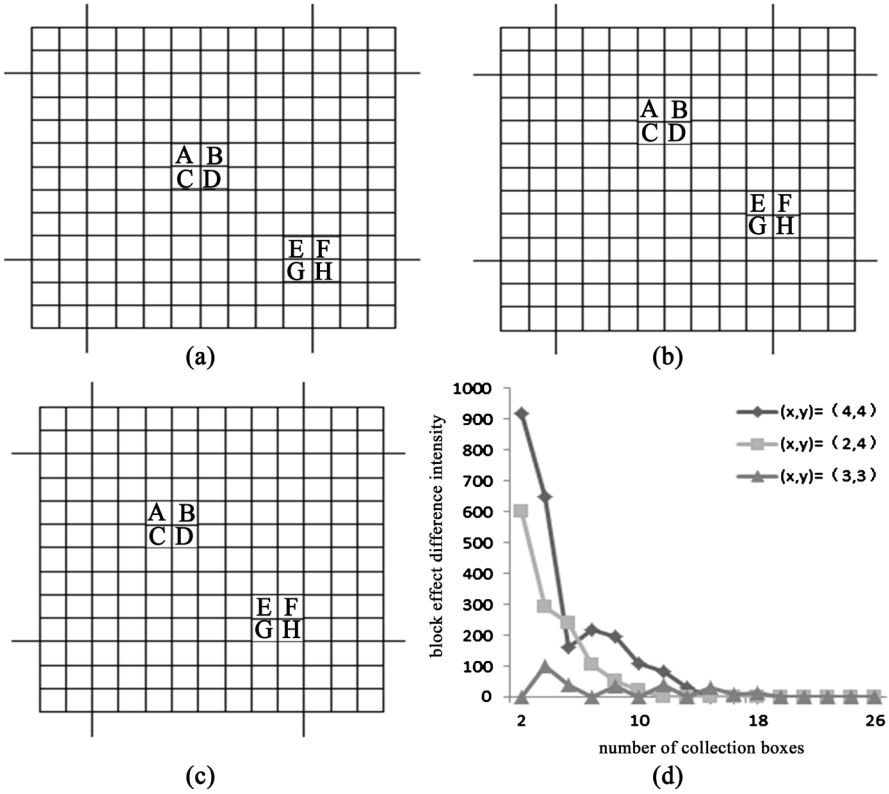

Figure 2. Example of block effect difference of JPEG image. (a) $(x, y) = (4, 4)$; (b) $(x, y) = (2, 4)$; (c) $(x, y) = (3, 3)$; (d) Histogram comparison of (x, y) under different coordinates.

Ye Shuiming *et al.* [40] selected a certain region of the image, took the Fourier transform of the DCT coefficient in this region, estimated the original quantization matrix according to the frequency domain characteristics, and used the quantization matrix of this region to represent the regions with large differences as tampering regions when calculating the block effect of the whole image. However, this method is only applicable to images with large compression quality factors. Wei Weimin *et al.* [41] proposed a measurement algorithm for block effect measurement of JPEG spectrum to identify the authenticity of the image. Based on the spectrum analysis, the algorithm made a second-order difference to the image and defined a new index for block effect measurement, which was used for blind forensics of tampering images. Chen, Y. [42] proposed a new technique that USES quantized noise model to detect the block effect caused by dual JPEG compression. The source images used are all JPEG formats, and the periodic features of JPEG images are represented in spatial and transform domains. The quantization noise model is as follows: $Ax = c = c' + n' = c'' + n''$, A represents the base matrix of DCT components with A size of 64 × 64, x represents the initial strength of 8 × 8 blocks, c' and c'' represent the quantization DCT coefficient vector after primary and secondary compression, n' and n'' are the corresponding quantization noise. The more the JPEG image is compressed, the closer the noise quantization histogram is to Gaussian distribution. In this method, the image is firstly decomposed according to the principle

of block effect, and then the low-frequency compensation is carried out. Only 15 DCT coefficients of the low-frequency are compensated here. Finally, the quantized noise model is modified to detect the double-compression block effect of block alignment or misalignment.

Many scholars have studied the mesh mismatch between the block-effect grid of the tampered region and the background region, and recognized the tampered region according to the extraction of block-effect grid. Tralic, D. *et al.* [43] proposed that the tamper region of JPEG forged image is detected and located according to the mismatch of image block-effect grid. This detection method can effectively process the image of smooth copy region boundary through the value of average neighboring pixels, and is realized by extracting and analyzing the grid block effect of block components introduced in the process of JPEG compression. Image compression for many times will produce block-effect mesh offset. Huang Wei [44] *et al.* introduced background information irrelevant to the original image in the process of image re-acquisition. Whether the original of image is offset is detected by using the average information loss of image to conduct block-effect mesh. Compared with the traditional method, this method has higher precision and shorter average detection time.

There must be mismatch inconsistency between block-effect grid of original JPEG image and block-effect grid of tampered image. Based on this assumption, blind forensics is effective in most cases, and detection will fail only if the pasted tampering area coincides with the surrounding original image block-effect grid, but the probability of this happening is only 1/64, that is, 1.56% [45].

4. Conclusions

4.1. Existing Problems

With the rapid development of image processing technology, image tampering has tended to be normalized. Although the blind forensics technology of JPEG image tampering has achieved some effects, it has not made many breakthroughs in recent years and there is no perfect architecture, which is mainly reflected in the following aspects:

1) The method is highly targeted. Most of the blind forensics of JPEG image tampering is for a specific tampering method, such as single compression, double compression, splicing, copy and paste, etc. Because without any prior knowledge when analyzing an image, it is difficult to detect the features of the image forgery to be detected, in order to meet the actual requirements, it is necessary to develop a fusion algorithm that can detect complex image tampering.

2) The forensics algorithm based on the statistical characteristics of JPEG images relies too much on the classifier and the selection of training samples, and most forensics algorithms need to rely on pre-training. For the poor performance of common blind detection, most forensics methods do not have a unified measurement standard.

3) Lack of public database for image testing. Many of the existing methods use

proprietary databases or some open source databases, and the images may come from different digital devices. Due to the difference between training samples and test samples, these differences have a low coupling degree, which will lead to different detection results of the same algorithm in different image databases. Therefore, it is impossible to effectively compare the advantages and disadvantages of each algorithm, and there is no unified standard model for the judgment of experimental results. In order to analyze and compare all kinds of tampering images and detection technologies objectively, it is necessary to establish a common image database and unify system evaluation norms and methods.

4.2. Research Prospect

Blind forensics of JPEG image tampering is a kind of passive forensics. Tampering detection can be divided into two types: double JPEG compression detection and block effect inconsistency detection. So far, the solutions to the problems faced are not completely mature, and there is still a certain gap with the actual application. Based on the summary and analysis of the existing research work, future research prospects can be considered from the following aspects:

1) Most JPEG image dual compression methods are only effective when the second compression quality factor QF2 is higher than the first QF1. When QF1 > QF2, the detection effect of the algorithm is poor. In the case of large JPEG second compression quality factor, forensic algorithm detection is still effective, which is the future research trend.

2) When the image is tampered with a lower compression quality factor, the original JPEG compression trace of the tampered area will be destroyed, and the tampering detection difficulty will increase. Therefore, when the tampered image is compressed and saved again with a lower quality factor than the original image, the blind forensics method of JPEG tampered image based on block effect measurement usually has poor or even invalid detection results. The faked JPEG image which is compressed again with a quality factor smaller than the original image can be further analyzed by combining other features, such as combining with the dual quantization of the JPEG image.

3) In recent years, with the rapid development of information and computer research, some fields related to digital image blind forensics research are also constantly innovating and making progress. At present, the rapidly developing statistical machine learning, deep learning, cloud computing, computer vision, big data and so on can provide valuable references for the research on the blind forensics of JPEG image tampering.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Duan, X.T., Peng, T., Li, F.F. and Wang, J. (2015) Blind Detection of Forensics Im-

age Based on JPEG Double Quantization Effect. *Proceedings of DPCS* 2015, **35**, 3198-3202. (In Chinese)

[2] Zheng, E.G. and Ping, X. J. (2010) Passives-Blind Forensics for a Class of JPEG Image Forgey. *Journal of Electronics & Information Technology*, **32**, 394-399. (In Chinese)

[3] Lukas, J. and Fridrich, J. (2003) Estimation of Primary Quantization Matrix in Double Compressed JPEG Images. *Proceedings of the* 2003 *Digital Forensic Research Workshop*, Piscataway, 67-84.

[4] Lin, T., Chang, M. and Chen, Y. (2011) A Passive-Blind Forgery Detection Scheme Based on Content-Adaptive Quantization Table Estimation. *IEEE Transactions on Circuits and Systems for Video Technology*, **21**, 421-434. https://doi.org/10.1109/TCSVT.2011.2125370

[5] Farid, H. (2009) Exposing Digital Forgeries from JPEG Ghosts. *IEEE Transactions on Information Forensics and Security*, **4**, 154-160. https://doi.org/10.1109/TIFS.2008.2012215

[6] He, J., Lin, Z., Wang, L., *et al.* (2006) Detecting Doctored JPEG Images via DCT Coefficient Analysis. In: Leonardis, A., Bischof, H. and Pinz, A., Eds., *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 423-435. https://doi.org/10.1007/11744078_33

[7] Fridrich, J., Goljan, M. and Du, R. (2001) Steganalysis Based on JPEG Compatibility. *ITCom* 2001: *International Symposium on the Convergence of IT and Communications*, International Society for Optics and Photonics, 275-280. https://doi.org/10.1117/12.448213

[8] Lin, Z., He, J., Tang, X., *et al.* (2009) Fast, Automatic and Fine-Grained Tampered JPEG Image Detection via DCT Coefficient Analysis. *Pattern Recognition*, **42**, 2492-2501. https://doi.org/10.1016/j.patcog.2009.03.019

[9] Duan, X.T., Peng, T., Li, F.F. and Wang, J. (2017) Blind Separation of Tampered Images Based on JPEG Double Compression Properties. *Journal of University of Jinan* (*Science and Technology*), **31**, 87-96. (In Chinese)

[10] Shih, F.Y. and Shi, Y.Q. (2012) Passive Detection of Copy-Paste Forgery between JPEG Images. *Journal of Central South University*, **19**, 2839-2851. https://doi.org/10.1007/s11771-012-1350-5

[11] Zhou, X.J., Li, F. and Xiong, B. (2012) Blind Detection of Synthetic Image Based on JPEG Quantization Distortion. *Application Research of Computers*, **29**, 2346-2349. (In Chinese)

[12] Liu, Q., Cooper, P.A., Chen, L., *et al.* (2013) Detection of JPEG Double Compression and Identification of Smartphone Image Source and Post-Capture Manipulation. *Applied Intelligence*, **39**, 705-726. https://doi.org/10.1007/s10489-013-0430-z

[13] Wang, Z.F., Zhu, L., Zeng, C.Y., *et al.* (2018) Survey on Recompression Detection for Digital Images. *Computer Science*, **9**, 20-29. (In Chinese)

[14] Fu, D.D., Shi, Y.Q. and Su, W. (2007) A Generalized Benford's Law for JPEG Coefficients and Its Applications in Image Forensics. *Proceedings of SPIE*, **6505**, 58-61. https://doi.org/10.1117/12.704723

[15] Wang, H.M. and Yang, X.Y. (2014) Detection Method for JPEG Image Based on the Difference of DCT Coefficient Histograms. *Journal of Sichuan University* (*Advanced Engineering Science*), **46**, 41-46. (In Chinese)

[16] Wang, J.W., Liu, G.J., Dai, Y.W., Zhou, L.-N. and Guo, Y.-B. (2009) A New Method for Estimating the Primary Quantization Step of JPEG Double-Compression. *Jour-*

nal of Electronics & Information Technology, **31**, 836-839. (In Chinese)

[17] Li, B., Shi, Y.Q. and Huang, J. (2008) Detecting Doubly Compressed JPEG Images by Using Mode Based First Digit Features. 2008 *IEEE* 10*th Workshop on Multimedia Signal Processing*, Cairns, Australia, 8-10 October 2008, 730-735.

[18] Dong, L.S., Kong, X.W., *et al*. (2011) Double Compression Detection Based on Markov Model of the First Digits of DCT Coefficients. 2011 *Sixth International Conference on Image and Graphics*, Hefei, 12-15 August 2011, 234-237. https://doi.org/10.1109/ICIG.2011.100

[19] Chen, C., Shi, Y.Q. and Su, W. (2008) A Machine Learning Based Scheme for Double JPEG Compression Detection. 2008 19*th International Conference on Pattern Recognition*, Tampa, FL, 8-11 December 2008, 1-4. https://doi.org/10.1109/ICPR.2008.4761645

[20] Bianchi, T. and Piva, A. (2012) Detection of Nonaligned Double JPEG Compression Based on Integer Periodicity Maps. *IEEE Transactions on Information Forensics and Security*, **7**, 842-848. https://doi.org/10.1109/TIFS.2011.2170836

[21] Huang, F., Huang, J. and Shi, Y.Q. (2010) Detecting Double JPEG Compression with the Same Quantization Matrix. *IEEE Transactions on Information Forensics and Security*, **5**, 848-856. https://doi.org/10.1109/TIFS.2010.2072921

[22] Yang, J., Xie, J., Zhu, G., Kwong, S. and Shi, Y.-Q. (2014) An Effective Method for Detecting Double JPEG Compression with the Same Quantization Matrix. *IEEE Transactions on Information Forensics and Security*, **9**, 1933-1942. https://doi.org/10.1109/TIFS.2014.2359368

[23] Lai, S.Y. and Bohme, R. (2013) Block Convergence in Repeated Transform Coding: JPEG-100 Forensics, Carbon Dating, and Tamper Detection. 2013 *IEEE International Conference on Acoustics*, *Speech and Signal Processing*, Vancouver, 26-31 May 2013, 3028-3032. https://doi.org/10.1109/ICASSP.2013.6638214

[24] Belhassen, B. and Matthew, C.S. (2017) On the Robustness of Constrained Convolutional Neural Networks to JPEG Post-Compression for Image Resampling Detection. 2017 *IEEE International Conference on Acoustics*, *Speech and Signal Processing*, New Orleans, LA, 5-9 March 2017, 2152-2156.

[25] Rao, Y. and Ni, J.Q. (2016) A Deep Learning Approach to Detection of Splicing and Copy-Move Forgeries in Images. 2016 *IEEE International Workshop on Information Forensics and Security*, Abu Dhabi, 4-7 December 2016, 2157-4774. https://doi.org/10.1109/WIFS.2016.7823911

[26] Zhou, P., Han, X.T., Morariu, V.I. and Davis, L.S. (2018) Learning Rich Features for Image Manipulation Detection. 2018 *IEEE Conference on Computer Vision and Pattern Recognition*, Salt Lake City, UT, 18-23 June 2018, 1053-1061. https://doi.org/10.1109/CVPR.2018.00116

[27] Geethu, V. and Arun, K.M.N. (2016) Detection of Double JPEG Compression on Color Image using Neural Network Classifier. *International Journal for Innovative Research in Science & Technology*, **3**, 175-181.

[28] Amerini, I., Uricchio, T., Ballan, L. and Caldelli, R. (2017) Localization of JPEG Double Compression through Multi-Domain Convolutional Neural Networks. 2017 *IEEE Conference on Computer Vision and Pattern Recognition Workshops*, Honolulu, HI, 21-26 July 2017, 2160-7516. https://doi.org/10.1109/CVPRW.2017.233

[29] Wang, Q. and Zhangk R. (2016) Double JPEG Compression Forensics Based on a Convolutional Neural Network. *EURASIP Journal on Information Security*, **2016**, 23. https://doi.org/10.1186/s13635-016-0047-y

[30] Bianchi, T. and Piva, A. (2012) Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts. *IEEE Transactions on Information Forensics and Security*, **7**, 1003-1017. https://doi.org/10.1109/TIFS.2012.2187516

[31] Amerini, I., Becarelli, R., Caldelli, R. and Del Mastio, A. (2014) Splicing Forgeries Localization through the Use of First Digit Features. 2014 *IEEE International Workshop on Information Forensics and Security*, Atlanta, GA, 3-5 December 2014, 143-148. https://doi.org/10.1109/WIFS.2014.7084318

[32] Zhao, J., Guo, J.C. and Zhang, Y. (2013) Survey: Blind Forensic of JPEG Forgeries Based on Blocking Artifacts. *Journal of Image and Graphics*, **18**, 613-620. (In Chinese)

[33] Singh, J., Singh, S., Singh, D. and Uddin, M. (2011) A Signal Adaptive Filter for Blocking Effect Reduction of JPEG Compressed Images. *International Journal of Electronics and Communications*, **65**, 827-839. https://doi.org/10.1016/j.aeue.2011.01.012

[34] Jung, C., Jiao, L.C., Qi, H.T. and Sun, T. (2012) Image Deblocking via Sparse Representation. *Signal Processing*: *Image Communication*, **27**, 663-677. https://doi.org/10.1016/j.image.2012.03.002

[35] Seok, B.Y., Kyuha, C. and Jong, B.R. (2011) Post Processing for Blocking Artifact Reduction. 2011 18*th IEEE International Conference on Image Processing*, Brussels, 11-14 September 2011, 1509-1512.

[36] Nath, V.K. and Hazarika, D. (2012) Blocking Artifacts Suppression in Wavelet Transform Domain Using Local Wiener Filtering. 2012 3*rd National Conference on Emerging Trends and Applications in Computer Science*, Shillong, India, 30-31 March 2012, 93-97. https://doi.org/10.1109/NCETACS.2012.6203306

[37] Suo, S.Y., He, X.H., Xiong, S.H., *et al*. (2018) Image Deblocking Algorithm Using Adaptive High-Dimensional Nonlocal Total Variational for Compressed Image. *Science Technology and Engineering*, **10**, 224-230. (In Chinese)

[38] Bhardwaj, D. and Pankajakahan, V. (2018) A JPEG Blocking Artifact Detector for Image Forensics. *Signal Processing*: *Image Communication*, **68**, 155-161. https://doi.org/10.1016/j.image.2018.07.011

[39] Fan, Z.G. and Queiroz, R.L. (2003) Identification of Bitmap Compression History: JPEG Detection and Quantizer Estimation. *IEEE Transactions on Image Processing*, **12**, 230-235. https://doi.org/10.1109/TIP.2002.807361

[40] Ye, S.M., Sun, Q.B. and Chang, E.C. (2007) Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact. 2007 IEEE International Conference on Multimedia and Expo, Beijing, 2-5 July 2007, 12-15. https://doi.org/10.1109/ICME.2007.4284574

[41] Wei, W.M. and Tang, Z.J. (2009) Blind Detection of Composite Images by Measuring Inconsistencies of JPEG Blocking Artifact. *Journal of Image and Graphics*, **14**, 2387-2390. (In Chinese)

[42] Chen, Y. and Hsu, C. (2011) Detecting Recompression of JPEG Images via Periodicity Analysis of Compression Artifacts for Tampering Detection. *IEEE Transactions on Information Forensics and Security*, **6**, 396-406. https://doi.org/10.1109/TIFS.2011.2106121

[43] Tralic, D., Petrovic, J. and Grgic, S. (2012) JPEG Image Tampering Detection Using Blocking Artifacts. 2012 19*th International Conference on Systems*, *Signals and Image Processing*. Vienna, 11-13 April 2012, 11-13.

[44] Huang, W., Huang, T.Q., Zhang, X.L. and Xiao, H. (2017) JPEG Recapture Image

Tamper Detection Method Based on Block Effect Grid Offset. *Chinese Journal of Network and Information Security*, **3**, 24-30. (In Chinese)

[45] Zhao, J., Guo, J. and Zhang, Y. (2013) Survey: Blind Forensic of JPEG Forgeries Based on Blocking Artifacts. *Journal of Image and Graphics*, **18**, 613-620. (In Chinese)