EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

Detection of tampered region for JPEG images by using mode-based first digit features

Xiang Hua Li[1], Yu Qian Zhao[2*], Miao Liao[2], Frank Y Shih[3] and Yun Q Shi[4]

Abstract

With the widespread availability of image editing software, digital images have been becoming easy to manipulate and edit even for non-professional users. For a tampered Joint Photographic Experts Group (JPEG) image, the tampered region usually has different JPEG compression history from the authentic region, which can be used to detect and locate the tampered region. In this article, we propose to apply the statistical features of the first digits of individual alternate current modes and support vector machine to detect and locate the tampered region. Experimental results show that our proposed method is effective for detecting three popularly used image manipulations. Its expectation of the percentage of overlap between the detected tampered region and the truth tampered region is higher than the existing algorithms.

Keywords: Image forensic, Tampered region detection, Benford's law, JPEG compression

Introduction

With the development of increasingly sophisticated digital image processing software, it has been becoming easy to create image forgery from one or multiple images without leaving visible clues. As a result, people's confidence in the reliability and veracity of digital images is declining. Furthermore, some applications may also bring legal crisis. Therefore, developing technologies to identify whether the content of an image has been tampered is becoming increasingly important.

Digital image forensic technologies include passive (blind) detection and active detection. The active detection includes active fragile digital watermarking, digital signature technology, and others. However, active detection only works when prior information can be embedded into original images. Therefore, to some extent due to the limitations of active detection, it cannot fundamentally prevent the development of image tampering. Ultimately, we should pay more attention to the passive detection method. Although a forged image may easily escape one or a few detection algorithms, it is difficult to escape all detection algorithms. Therefore, researchers have been developing more passive detection algorithms to detect the tampered images.

Currently, Joint Photographic Experts Group (JPEG) is the most widelyused image format. Human eyes have a higher sensitivity for the low-frequency signal than the high-frequency signal. Through reducing the high-frequency information, JPEG compression allows images to retain a high compression ratio and simultaneously obtain a satisfactory image quality. For a tampered JPEG image, the tampered region usually has different JPEG compression history from the authentic region. The tampered digital image is generally difficult to be identified by human eyes; however, it is usually left behind some invisible clues or statistical artifacts. Based on these clues or artifacts, JPEG digital forensic technologies have undergone continuous development and improvement.

Popescu and Farid [1] proposed an efficient technique to detect image recompression with resample effect, which always appears in the quantized discrete cosine transform (DCT) coefficient histogram. Based on the DCT of small fixed-size image blocks, Huang et al. [2] presented an efficient technique to automatically detect duplicated regions in a tampered image. This method fails if the tampered region comes from other images. Stamm xand Liu [3] proposed an algorithm for detecting forged images by statistical intrinsic fingerprints. This method can detect global and local

* Correspondence: zhaocsu@hotmail.com
[2]School of Geosciences and Info-physics, Central South University, Changsha, Hunan 410083, China
Full list of author information is available at the end of the article

contrast enhancement, identify histogram equalization, and detect global addition of noise to a previously JPEG-compressed image. Peng et al. [4] proposed a novel scheme to detect and locate the tampered region based on compound statistics features, which is effective for copy–paste image forensics between various images. However, the detection results in [3,4] become unsatisfactory when local manipulations with small tampered regions are conducted.

Farid [5] proposed a tampered region detection method for the copy–paste operation based on JPEG Ghost. This method only works when the original JPEG quality factor of the tampered region is lower than that of the untampered region, and is also lower than the resaved quality factor of the composite image, which limits the usage of the method. Liu et al. [6] proposed a passive copy–move forgery detection method by computing the averaged sum of absolute difference (SAD). The method fails when the original quality factors of the inserted region and the authentic region are equal or almost equal. In addition, the obtained SAD image is a grayscale image, and the authors detect the tampered region from the SAD image by using threshold and mathematical morphology methods, which will significantly reduce the accuracy of locating the tampered region. Fan and de Queiroz [7] proposed an algorithm to detect whether an image has previously been JPEG compressed and further locate the whole position of block artifacts. The detection result of this method is easy to be interfered by mismatched block artifacts when a JPEG image is tampered by copy–paste. Li et al. [8] proposed a passive detection method for the doctored JPEG image via block artifact grid extraction. This method is effective for copy–paste, inpainting, and cropping manipulations with the doctored image saved in an uncompressed format, such as BMP and TIF. It fails if the image is saved in a JPEG format after being manipulated. Zhao et al. [9] presented a passive digital image forensic technique for detecting the tampered region of an inpainting JPEG image when the tampered image is saved in uncompressed format or in JPEG format.

Lin et al. [10] proposed an automatic tampered JPEG images detection method by examining the double quantization effect hidden among the DCT coefficients. The authors calculated the block posterior probability map (BPPM) according to Bayesian statistical characteristics of DCT coefficient histograms of a tampered JPEG image, and then located the tampered region by thresholding the BPPM. In this method, the obtained BPPM is only 1/64 of the original to-be-examined image in size, which may affect the final location accuracy of the tampered region, especially for small tampered region. Fu et al. [11] proposed that all JPEG coefficients (quantized DCT coefficients) of a singly compressed JPEG image follow the generalized Benford's law, and applied it to detect whether a bitmap image undergoes JPEG compressed previously, and if so, to estimate the original JPEG quality factor. Based on the above development, Li et al. [12] proposed mode-based first digit features (MBFDF) to detect whether a JPEG image has undergone double JPEG compression. This method is superior to all previous methods for distinguishing between single and double JPEG compression. However, both methods in [11,12] can only reveal the compression history of a given image, and cannot detect the local tampered region in a given image.

In this article, we propose a tampered region detecting algorithm based on machine learning and the statistical properties of the first digits, which are obtained from JPEG coefficients of individual AC modes. The rest of the article is organized as follows. "Analysis of the first digits' probability distribution by Benford's law" section focuses on the first digits' probability distribution of JPEG coefficients of singly and doubly compressed JPEG images. In "Detection algorithm for the tampered region" section, we describe a technique to detect whether any part of the detected image has different compression history from the remaining region. In "Experimental results and statistical analysis" section, we present experimental results and their statistical analysis. Conclusions are drawn in at last section.

Analysis of the first digits' probability distribution by Benford's law

As we know, JPEG image compression is divided into the following steps: 8 × 8 block extraction, DCT transform, quantization, and coding. An original uncompressed image is first partitioned into 8 × 8 pixel blocks. Then each block is converted to frequency space by a 2D DCT. The value located in the upper-left corner of the block is called *direct currentcoefficient*, and the other 63 values are called *alternate current (AC) coefficients*. Next, each block DCT coefficients are quantized by the JPEG quantization table.

According to Benford's law, for a set of real data, the values of the first digits are not uniformly distributed, but when the amount of data is large enough, the values of the first digits will meet a certain statistical law as follows:

$$p(d) = \log_{10}(1 + 1/d)(d = 1, 2, \ldots, 9) \quad (1)$$

where d is the value of the first digits and $p(d)$ denotes the probability of digital d.

Through experiments, Fu et al. [11] proposed that the probability distribution of the first digits of block DCT coefficients of uncompressed image follows Benford's law quite well, and the JPEG coefficients of a singly

compressed JPEG image follows the generalized Benford's law, as follows:

$$p(d) = N\log_{10}(1 + 1/(s + d^q))(d = 1, 2, \ldots, 9) \quad (2)$$

where N, s, and q are model parameters to precisely describe the distribution. Different compression factors correspond to different N, s, and q values.

Un-compressed image database (UCID) [13] is a color image database including 1,338 uncompressed TIFF images, which span a wide range of indoor and outdoor scenes with the size of 512 × 384. In our experiments, we conduct single JPEG compression three times (QF = 70, 80, and 90) and double JPEG compression three times (QF_1, QF_2 = 55, 70; 65, 80; 75, 90) for all 1,338 images in the UCID database. Note that unless specified in the article, we refer double JPEG compression to that an image is compressed twice by the same or different JPEG quality factors successively in the 8 × 8 blocks.

In Figure 1, the green (second) bars show the mean probability distribution of the first digits of JPEG coefficients for all singly compressed images, the yellow (third) bars show the mean probability distribution of the first digits of JPEG coefficients for all doubly JPEG compressed images with blocks mismatching (i.e., misalignments of JPEG blocks relative to their original lattice), and the red (forth) bars show that for all doubly JPEG compressed images with blocks matching. The mean probability distributions calculated by the generalized Benford's law as defined in Equation (2) with different JPEG quality factor (QF = 70, 80, and 90) are also shown in blue (first) bars for comparison. Obviously, the first digits' probability distributions of JPEG coefficients of singly compressed images and doubly compressed images with 8 × 8 blocks mismatching follow the generalized Benford's law quite well (see blue, green, and yellow bars), and those of doubly compressed JPEG images with 8 × 8 blocks matching seriously violate the generalized Benford's law (see red bars).

In JPEG compression, 8 × 8 quantization table is used. All of the JPEG coefficients located in the same position of the 8 × 8 blocks form a mode. We thus have in total 63 AC modes, ordered in zigzag scan sequencing. Each AC mode corresponds to one quantization step. In order to make the classification more accurate, it was proposed in [12] to calculate the first digits' probability distribution for individual AC modes, and use the χ^2 divergence as a metric to measure the degree of fitting for each AC mode. The value of χ^2 is defined as follows:

$$\chi^2 = \sum_{d=1}^{9} \frac{(pi(d) - \hat{p}_i(d))}{\hat{p}_i}(d) \quad (3)$$

where $p_i(d)$ $(d = 1,2, \ldots, 9)$ denotes the actual first digit probability distribution of JPEG coefficients for the ith AC mode, and $\hat{p}_i(d)$ denotes theoretical probability distribution calculated by generalized Benford's law. The smaller the χ^2 value, the better the AC mode fits into generalized Benford's law. Since high-frequency AC coefficients corresponding to the larger quantization step, the majority of high-frequency AC coefficients are quantified and rounded to zero. Therefore, the first digits' probability distribution of high-frequency AC modes will be serious departure from the generalized Benford's law, correspondingly, the value of χ^2 increases. Li et al. [12] compressed 1,338 UCID images at JPEG quality factor of QF ranging from 50 to 100 in a step of 10, then calculated the mean value of χ^2 divergence of 1,338 images for each AC mode and for each quality factor QF. Their experimental results are shown in Figure 2, from which

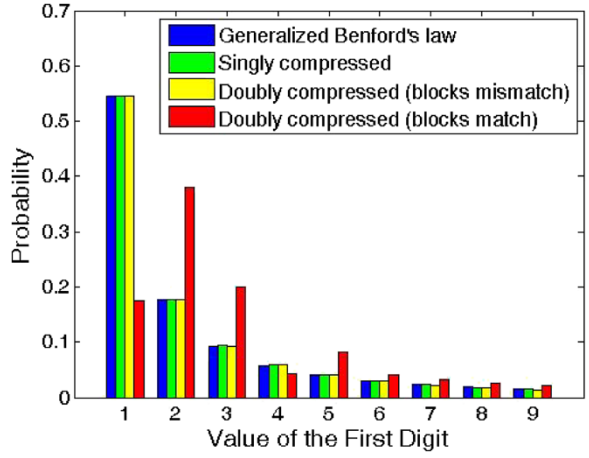

Figure 1 The mean probability distributions of the first digits of JPEG coefficients for all 1,338 images in UCID database with different compression history.

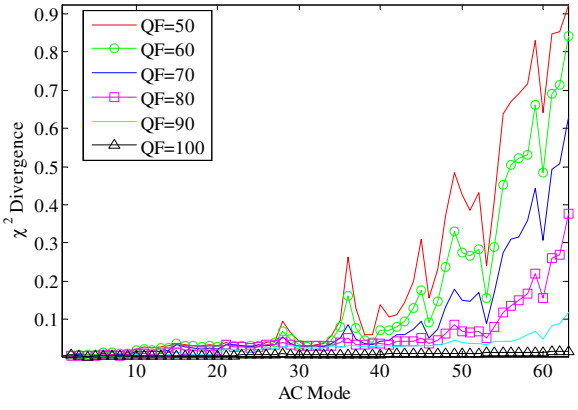

Figure 2 The χ^2 divergence between the first digits' probability distribution calculated by generalized Benford's law and the real probability distribution for each AC mode [12].

it is easily observed that the first digits' probability distribution of top 15 to 25 AC modes can follow the generalized Benford's law quite well.

Detection algorithm for the tampered region

Assuming a JPEG image is saved in JPEG format after being tampered, the un-tampered region usually has different compression history from the tampered region(s). This study is to detect and locate the tampered region(s) in a manipulated image. In this article, we put forward a novel detecting method. Figure 3 shows the work flow of our algorithm. The main detection steps are as follows:

Step 1. Train a two-class support vector machine (SVM) by using the MBFDF described above for, say, 1000 randomly selected singly JPEG compressed images (the original uncompressed images are from UCID) and their counterparts: the JPEG doubly compressed images with different QF values.
Step 2. Divide a test image into continuous non-overlapping 8 × 8 pixel blocks.
Step 3. Centering at each block, take a sub-image with the size of $(2n+1) \times (2n+1)$ blocks, where $n = 0, 1, 2, \ldots$.
Step 4. For each sub-image, calculate its first digits' probability distribution of JPEG coefficients of the first i AC modes to obtain a feature vector of $i \times 9$ dimensions, where each 9 features are probabilities of the nine first digits of one AC mode.
Step 5. Determine whether the sub-image under examination has been manipulated or not by applying SVM, and if yes, the block in the original image corresponding to the central block of the sub-image is considered as having been tampered.

From a statistical point of view, the larger the n is, the more obvious the statistical characteristics are. However, with the increasing of n, the accuracy of locating the tampered region will decrease. Therefore, in order to achieve high accuracy in locating the tampered region, the value of n should be small. However, the smaller the n, the more noise appears in the detection result. As a compromise, n is usually set as 1 or 2, and i is ranging from 15 to 25.

There are three kinds of popularly used manipulations, (1) copy–paste manipulation with the inserted region coming from the uncompressed images (referred to as JPEG + uncompressed); (2) copy–paste manipulation with the inserted region coming from JPEG images (referred to as JPEG + JPEG); (3) inpainting manipulation on JPEG images (referred to as JPEG + inpainting). In each manipulation, the composite image is finally saved in JPEG format. Now, we introduce the tampered region

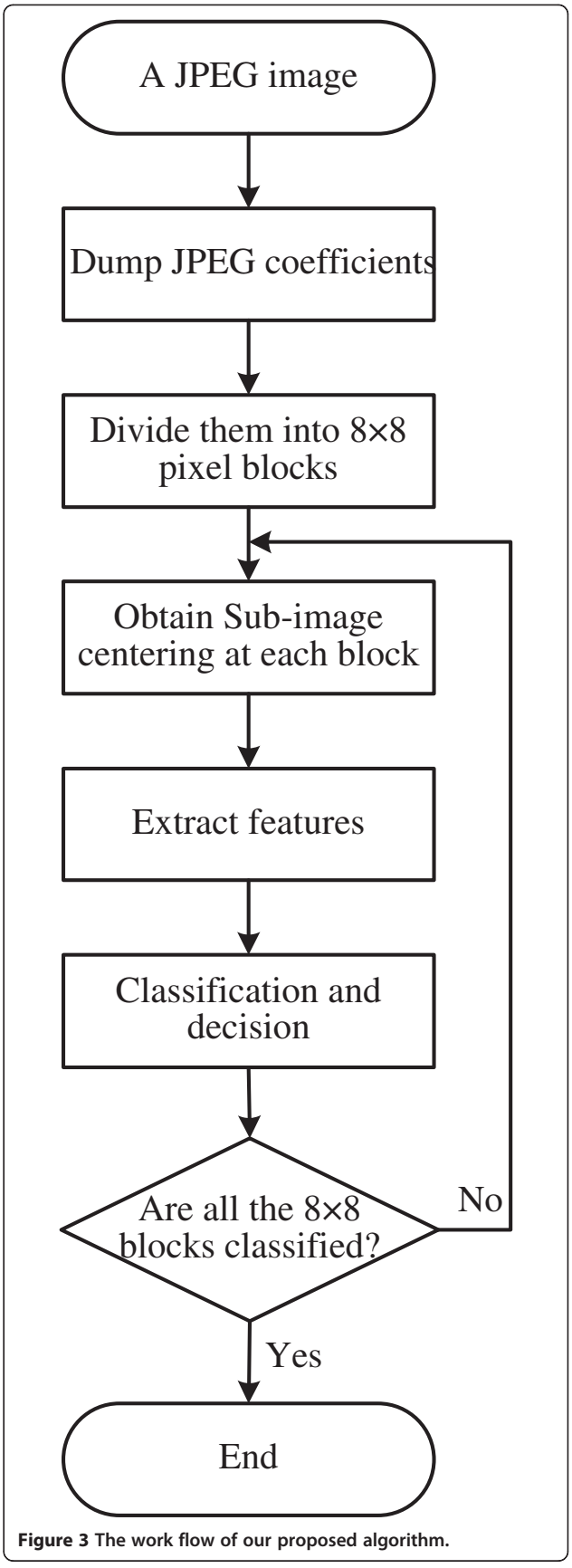

Figure 3 The work flow of our proposed algorithm.

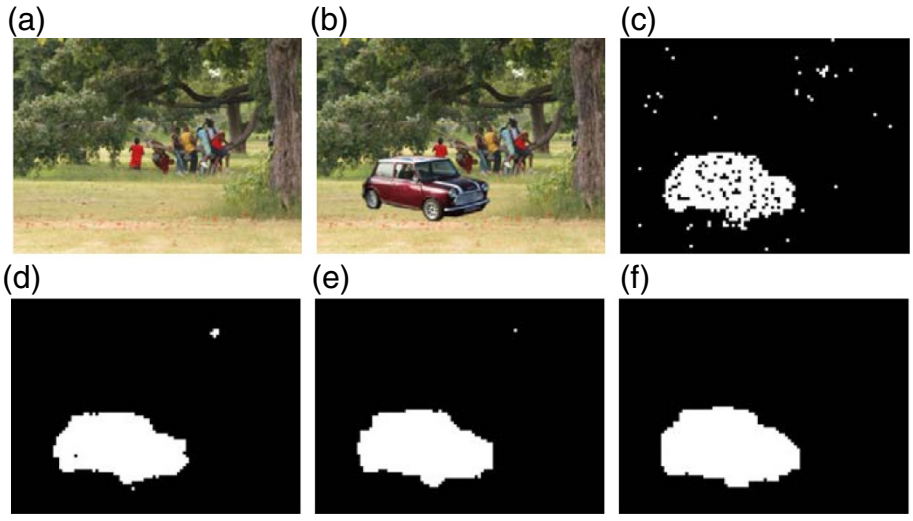

Figure 4 The detection of JPEG + uncompressed manipulation: (a) Original image, (b) tampered image, (c–f) the detection results with $i = 20$, and $n = 0$, 1, 2, and 3, respectively.

detecting method for the above three manipulations, respectively.

JPEG + uncompressed

For an original image with JPEG quality factor QF_1, we insert an uncompressed image such as TIF, BMP, and then save the composite image at JPEG quality factor QF_2 ($QF_1 \neq QF_2$). In this tampering scheme, the tampered region undergoes single JPEG compression, but the un-tampered region undergoes double JPEG compression.

Figure 4a shows the original image with JPEG quality factor $QF_1 = 60$, and Figure 4b is the copy–paste tampered image, in which the car was from an uncompressed image with the format of TIF. We save the composite image at JPEG quality factor $QF_2 = 75$. Clearly, the tampered region (car) in Figure 4b undergoes single JPEG compression ($QF_2 = 75$), while the un-tampered region undergoes double JPEG compression ($QF_1 = 60$, $QF_2 = 75$). Figure 4c–f shows the detection results of Figure 4b with the parameter $n = 0$, 1, 2, and 3, respectively. It is obvious that there is speckle noise in the detection result when the size of sub-image is small ($n = 0$). However, the noise is almost completely eliminated with $n = 1$, 2, or 3. Furthermore, Figure 4d,e can achieve a higher accuracy in locating the tampered region than Figure 4f, which will be further

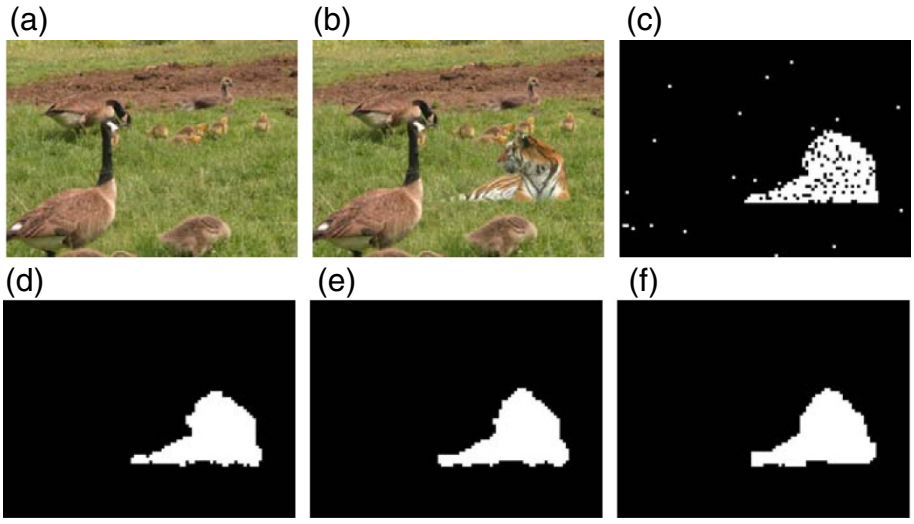

Figure 5 The detection of JPEG + JPEG manipulation with the original JPEG quality factor of the un-tampered region being different from that of the inserted region: (a) Original image, (b) tampered image, (c–f) the detection results with $i = 20$, and $n = 0$, 1, 2, and 3, respectively.

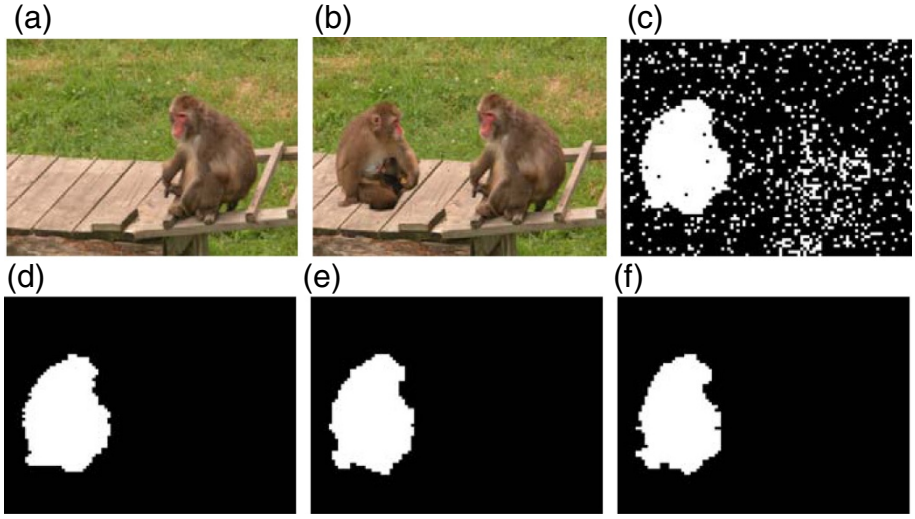

Figure 6 The detection of JPEG + JPEG manipulation with the original JPEG quality factor of the un-tampered region being equal to that of the inserted region; (a) Original image, (b) tampered image, (c–f) the detection results with $i = 20$, and $n = 0$, 1, 2, and 3, respectively.

discussed in "Experimental results and statistical analysis" section. Here, we select the first digits of the top 20 AC modes to calculate the feature vector, i.e., $i = 20$.

JPEG + JPEG

While an image was tampered with JPEG + JPEG manipulation, the un-tampered region undergoes double JPEG compression with blocks matching. Although the inserted region undergoes double JPEG compression, the probability of matching between the 8 × 8 grid of the original image and that of the copy–paste inserted image is only 1/64. Therefore, we can regard the tampered region of the composite image as singly compressed region in our proposed algorithm.

Figure 5a shows the original image with JPEG quality factor $QF_1 = 50$ and Figure 5b is the tampered image with the inserted tiger coming from a JPEG compressed image of quality factor 80. We save the composite image at JPEG quality $QF_2 = 70$. Figure 5c–f is the detection results of Figure 5b with the parameters $m = 20$, and $n = 0$, 1, 2, and 3, respectively. Obviously, the detection results are satisfactory with $n = 1$, 2, and 3.

For JPEG + JPEG manipulation, our proposed method is also effective if the original JPEG quality factor of the un-tampered region is equal to that of the inserted region, which is an advantage compared with the method in [6]. Figure 6a shows another original image with JPEG quality factor $QF_1 = 80$ and Figure 6b is the tampered

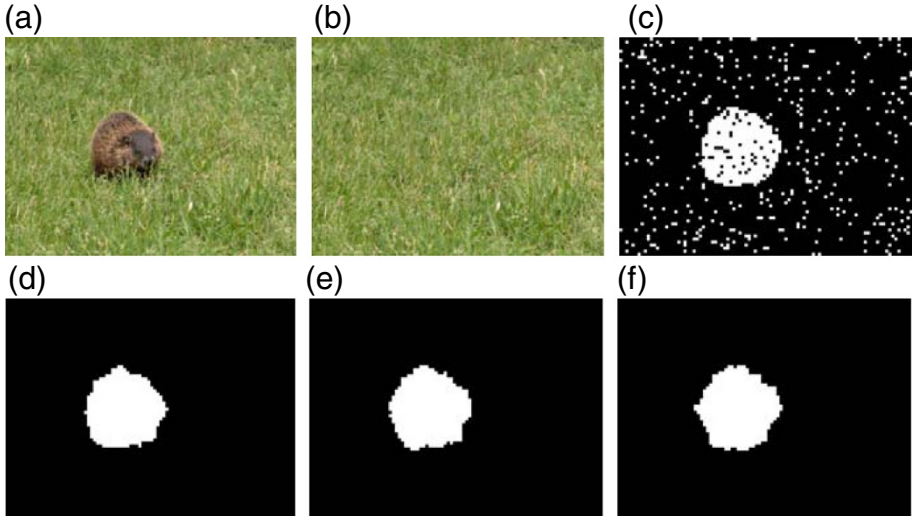

Figure 7 The detection for JPEG + inpainting manipulation: (a) Original image, (b) tampered image, (c–f) the detection results with $i = 20$, and $n = 0$, 1, 2, and 3, respectively.

Table 1 The detection performance of Figures 4, 5, 6, and 7 for different parameters *n*

n	Figure 4		Figure 5		Figure 6		Figure 7	
	OL	DE	OL	DE	OL	DE	OL	DE
0	0.7875	0.2313	0.7552	0.2722	0.5929	0.6774	0.6269	0.5342
1	**0.8612**	**0.1608**	**0.8584**	**0.1650**	**0.9117**	**0.0963**	**0.9073**	**0.1022**
2	0.8227	0.2155	0.8393	0.1892	0.9068	0.1008	0.8943	0.1182
3	0.7746	0.2909	0.8289	0.2032	0.9054	0.1014	0.8839	0.1310

image with the inserted monkey coming from a JPEG compressed image of the same quality factor 80. We save the composite image at JPEG quality $QF_2 = 90$. Figure 6c–f is the detection results of Figure 6b with the parameters $i = 20$, and $n = 0$, 1, 2, and 3, respectively. As can be seen, the detection results are satisfactory with $n = 1$, 2, and 3.

JPEG + inpainting

Inpainting is also a usually used imperceptible image tampering method, which selects some neighboring pixels to replace the original information in order to hide particular objects in the original image [14]. In this case, the tampered region consists of some random pixels. When an original image with the JPEG quality factor QF_1 is manipulated in the way of inpainting, and is then saved at JPEG quality factor QF_2, we can consider that the tampered region undergoes single JPEG compression with quality factor QF_2 and the un-tampered region undergoes double JPEG compression with the primary quality factor QF_1 and the secondary quality factor QF_2. Therefore, the tampered region could be available distinguished from the un-tampered region by our proposed algorithm.

Figure 7a shows the original image with JPEG quality factor $QF_1 = 75$, and Figure 7b is the tampered image obtained by applying inpainting operation proposed in [14] to conceal the small animal and saving the composite image at JPEG quality factor $QF_2 = 85$. Figure 7c–f is the detection results of Figure 7b with the parameters $i = 20$, and $n = 0$, 1, 2, and 3, respectively. Obviously, the detection results are satisfactory with $n = 1$, 2, and 3.

Experimental results and statistical analysis

In all of the above experiments, the detection results with the parameter n =1, 2, and 3 are all satisfactory. To judge the optimal parameter n and, correspondingly, the best detection result, in this article, we use two measures to evaluate the performance of different detection results. The first measure determines the percentage of overlap (OL) between the detected tampered region A_1 and the truth tampered region A_2:

$$OL = \frac{2(A_1 \cap A_2)}{(A_1 \cup A_2) + (A_1 \cap A_2)} \tag{4}$$

And the second measure represents the percentage of detection error (DE) which is defined as

$$DE = \frac{W_1 + W_2}{2 \times TR} \tag{5}$$

where W_1 is the number of the un-tempered region pixels classified as the tampered region pixels, W_2 is the number of the tampered region pixels classified as the un-tampered region pixels, and TR denotes the number of tampered region pixels in the ground truth. The bigger the OL value and the smaller the DE value, the better the detection performance is. Table 1 shows the detection performance of Figures 4, 5, 6, and 7, from which we can find that the detection performance is better with $n = 1$ than that with $n = 0$, 2 and 3.

To further testify the efficacy of our proposed algorithm, we randomly choose 1,000 singly compressed images and their doubly compressed counterparts from UCID database to train a two-class classification SVM, and randomly choose 700 images from another color image database [15] with each of size 768 × 576 as the test set. First, we conduct single JPEG compression for all 700 uncompressed images with JPEG quality factor QF_1. A central portion for each singly compressed image is tampered with JPEG + uncompressed and JPEG + JPEG manipulations, respectively, and then the entire image is saved at JPEG quality factor QF_2. Due to the tampered and un-tampered regions generated by the JPEG + inpainting manipulation have the same compression history, respectively, as those generated by the JPEG + uncompressed manipulation, we will not discuss

Table 2 The ME and STD of OL for the JPEG + uncompressed manipulation

Size		QF_2									
		75		80		85		90		95	
150 × 150		ME	STD	ME	STD	ME	STD	ME	STD	ME	STD
QF_1	50	0.9345	0.0345	0.9363	0.0076	0.9191	0.0319	0.9066	0.0424	0.8363	0.1158
	55	0.9370	0.0284	0.9333	0.0316	**0.9234**	0.0315	0.9117	0.0396	0.8653	0.0806
	60	**0.9275**	0.0566	0.9370	0.0267	0.9348	0.0080	0.9114	0.0336	0.8734	0.0800
	65	0.8813	0.0833	0.9388	0.0183	0.9319	0.0249	0.9197	0.0254	0.8859	0.0553

Table 3 The ME and STD of DE for the JPEG + uncompressed manipulation

Size		QF_2									
		75		80		85		90		95	
150 × 150		ME	STD	ME	STD	ME	STD	ME	STD	ME	STD
QF_1	50	0.0705	0.0626	0.0667	0.0083	0.0895	0.0605	0.1062	0.0751	0.2298	0.2541
	55	0.0669	0.0536	0.0719	0.0589	**0.0844**	0.0595	0.0996	0.0713	0.1705	0.1653
	60	**0.0819**	0.1077	0.0670	0.0514	0.0687	0.0090	0.0992	0.0624	0.1592	0.1633
	65	0.1375	0.1597	0.0637	0.0272	0.0733	0.0496	0.0883	0.0506	0.1348	0.1017

the JPEG + inpainting manipulation individually. In all of our experiments, the size of central tampered region is 150 × 150 pixels. We choose the top 20 AC modes to calculate the feature vector, and the parameter used for determining the size of sub-image is $n = 1$. The JPEG quality factor QF_1 ranges from 50 to 65 in a step of 5 and the JPEG quality factor QF_2 ranges from 75 to 95 in a step of 5. Next, we detect these tampered images by applying our proposed algorithm.

Shown in Tables 2 and 3 are the mathematical expectation (ME) and standard deviation (STD) of OL and DE, respectively, for the detected results of 700 tampered images with JPEG + uncompressed manipulation, and the inserted regions are from TIF images. Tables 4 and 5 show the ME and STD of OL and DE, respectively, for JPEG + JPEG manipulation, and the inserted regions are from JPEG compressed images. As expected, the MEs of OLs for JPEG + uncompressed manipulation are larger than those for JPEG + JPEG manipulation, and the MEs of DEs for JPEG + uncompressed manipulation are smaller than those for JPEG + JPEG manipulation, which are mainly because of the effect of JPEG block artifacts brought by the copy–paste inserted JPEG compressed image (as presented above, the probability of matching between the 8 × 8 grid of the original image and that of the copy–paste inserted image is 1/64 for JPEG + JPEG manipulation).

Figure 8a,b shows the probability distribution of OL and DE for 700 detected results with the JPEG + uncompressed manipulation with the JPEG quality factors QF_1, $QF_2 = 55$, 85; and 60, 75, respectively. Figure 9a,b shows the probability distribution of OL and DE for 700 detected results with the JPEG + JPEG manipulation with the JPEG quality factors QF_1, $QF_2 = 50$, 80; and 65, 90, respectively. From Figures 8 and 9, it is easy to conclude that the detection results are satisfactory with our proposed method.

We also compare our proposed algorithm with the SAD algorithm proposed in [6] and the BPPM algorithm proposed in [10] using the 700 tampered images in [15]. Assuming 700 randomly chosen original images is each first JPEG compressed with quality factor 65, then conduct JPEG + uncompressed manipulation and the entire image is saved at the JPEG quality factor 85 after being tampered. The size of tampered region is 150 × 150 pixels. We calculate the ME and STD of OL and DE, respectively,

Table 4 The ME and STD of OL for the JPEG + JPEG manipulation

Size		QF_2									
		75		80		85		90		95	
150 × 150		ME	STD	ME	STD	ME	STD	ME	STD	ME	STD
QF_1	50	0.8905	0.0332	**0.8930**	0.0124	0.8756	0.0298	0.8691	0.0398	0.8170	0.1100
	55	0.8981	0.0292	0.8875	0.0309	0.8794	0.0300	0.8756	0.0370	0.8413	0.0777
	60	0.8989	0.0563	0.8909	0.0274	0.8921	0.0126	0.8728	0.0311	0.8485	0.0747
	65	0.8731	0.0823	0.9006	0.0267	0.8843	0.0248	**0.8804**	0.0248	0.8551	0.0513

Table 5 The ME and STD of DE for the JPEG + JPEG manipulation

Size		QF_2									
		75		80		85		90		95	
150 × 150		ME	STD	ME	STD	ME	STD	ME	STD	ME	STD
QF_1	50	0.1248	0.0634	**0.1194**	0.0154	0.1439	0.0603	0.1539	0.0751	0.2571	0.2514
	55	0.1146	0.0558	0.1283	0.0604	0.1390	0.0602	0.1450	0.0706	0.2039	0.1714
	60	0.1178	0.1104	0.1236	0.0539	0.1208	0.0157	0.1478	0.0613	0.1921	0.1602
	65	0.1524	0.1640	0.1110	0.0500	0.1318	0.0513	**0.1371**	0.0513	0.1754	0.1007

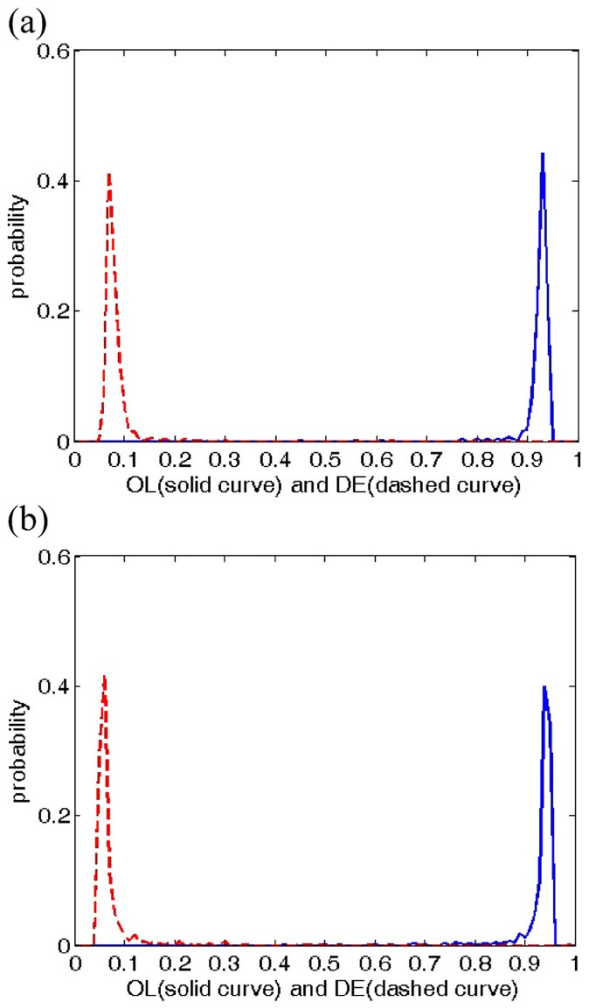

Figure 8 The probability distributions of OL and DE for JPEG + uncompressed manipulation: (a) The JPEG + uncompressed manipulation with the JPEG quality factors $QF_1 = 55$ and $QF_2 = 85$; (b) The JPEG + uncompressed manipulation with the JPEG quality factors $QF_1 = 60$ and $QF_2 = 75$. In each panel, the red dashed curve corresponds to the probability distribution of DE, and the blue solid curve denotes the probability distribution of OL. See also Tables 2 and 3.

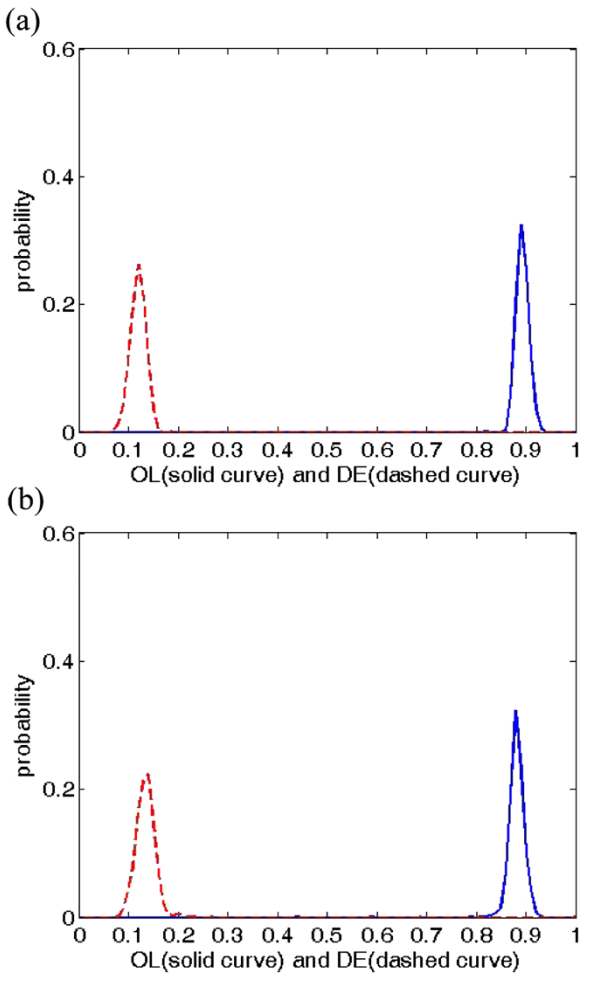

Figure 9 The probability distributions of OL and DE for JPEG + JPEG manipulation: (a) The JPEG + JPEG manipulation with the JPEG quality factors $QF_1 = 50$ and $QF_2 = 80$; (b) The JPEG + JPEG manipulation with the JPEG quality factors QF_1, =65 and $QF_2 = 90$. In each panel, the red dashed curve corresponds to the probability distribution of DE, and the blue solid curve denotes the probability distribution of OL. See also Tables 4 and 5.

with 700 detection results for three different detection methods. The detection performances are shown in Table 6. It can clearly be seen that our proposed method has a more satisfactory detection performance than other two algorithms.

Conclusion

In this article, we focus on analyzing the first digits' probability distributions of JPEG coefficients for images with different JPEG compression history, and further present an efficient and automatic detection method by using MBFDF to decide whether a given JPEG image has locally been manipulated or not, and if so, to locate the tampered region.

There are several advantages with the proposed method. First, it can accurately detect and locate the tampered region. Second, it is effective for different kinds of forgery techniques: (1) copy–paste manipulation with the inserted region coming from uncompressed

Table 6 The comparison of the detection performance of our proposed algorithm with SAD algorithm [6] and BPPM algorithm [10]

Algorithm	OL		DE	
	ME	STD	ME	STD
SAD algorithm [6]	0.32682	0.2555	3.4839	2.1818
BPPM algorithm [10]	0.8906	0.1288	0.1416	0.2546
Our proposed algorithm	0.9319	0.0249	0.0733	0.0496

images; (2) copy–paste manipulation with the inserted region coming from JPEG images; (3) inpainting manipulation on JPEG images. Third, it is an automatic tampered JPEG images detecting method and we donot require any prior knowledge. Finally, the detection accuracy is high and DE is small.

Competing interests
The authors declare that they have no competing interests.

Acknowledgments
This study was supported by the National Natural Science Foundation of China (Grant No. 61172184) and the Hunan Provincial Natural Science Foundation of China (Grant No. 12JJ6062). The authors would like to thank Drs. Bin Li and Gang Yu for their valuable suggestions.

Author details
[1]School of Civil Engineering, Central South University, Changsha, Hunan 410083, China. [2]School of Geosciences and Info-physics, Central South University, Changsha, Hunan 410083, China. [3]Department of Computer Science, New Jersey Institute of Technology, Newark, NJ 07102, USA. [4]Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA.

Received: 5 March 2012 Accepted: 13 August 2012
Published: 30 August 2012

References
1. A. Popescu, H. Farid, Statistical tools for digital forensics. Lecture Notes Comput. Sci. **3200**, 395–407 (2005)
2. Y. Huang, W. Lu, W. Sun, D. Long, Improved DCT-based detection of copy-move forgery in images. Forensic Sci. Int. **206**, 178–184 (2011)
3. M.C. Stamm, K.J.R. Liu, Forensic detection of image manipulation using statistical intrinsic fingerprints. IEEE Trans. Inf. Forensics Security **5**(3), 492–506 (2011)
4. F. Peng, Y. Nie, M. Long, A complete passive blind image copy-move forensics scheme based on compound statistic features. Forensics Sci. Int. **212**, e21–e25 (2011)
5. H. Farid, Exposing digital forgeries from JPEG ghosts. IEEE Trans. Inf. Forensics Security **4**(1), 154–160 (2009)
6. Z. Liu, X. Li, Y. Zhao, Passive detection of copy-paste tampering for digital image forensics, in*Proc.* Fourth Int. Conf. Intelligent Comput. Technol. Automation **2**, 649–652 (2011)
7. Z. Fan, R.L. de Queiroz, Identification of bitmap compression history: JPEG detection and quantizer estimation. IEEE Trans. Image Process. **12**(2), 230–235 (2003)
8. W. Li, Y. Yuan, N. Yu, Passive detection of doctored JPEG image via block artifact grid extraction. Signal Process. **89**(9), 1821–1829 (2009)
9. Y.Q. Zhao, M. Liao, F.Y. Shih, Y.Q. Shi, Tampered region detection of inpainting JPEG images. Optik – Int. J. Light Electron Opt., (2012). doi:10.1016/j.ijleo.2012.08.018
10. Z. Lin, J. He, X. Tang, C.-K. Tang, Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recognit. **42**, 2492–2501 (2009)
11. D. Fu, Y.Q. Shi, Q. Su, A generalized Benford's law for JPEG coefficients and its applications in image forensics. Proc. SPIE **6505**, 65051L1–65051L11 (2007)
12. B. Li, Y.Q. Shi, J. Huang, Detecting doubly compressed JPEG images by using mode based first digit features, in *IEEE International Workshop on Multimedia Signal Processing* (Cairns, Queensland, Australia, 2008), pp. 730–735
13. G. Schaefer, M. Stich, *UCID—an uncompressed colour image database. Technical Report, School of Computing and Mathematics* (Nottingham Trent University, UK, 2003)
14. A. Criminisi, P. Perez, K. Toyama, Region filling and object removal by exemplar-based inpainting. IEEE Trans. Image Process. **13**(9), 1200–1212 (2004)
15. A. Olmos, F.A.A. Kingdom, *McGill Calibrated Colour Image Database* (2004). http://tabby.vision.mcgill.ca

doi:10.1186/1687-6180-2012-190
Cite this article as: Li *et al.*: Detection of tampered region for JPEG images by using mode-based first digit features. *EURASIP Journal on Advances in Signal Processing* 2012 **2012**:190.