Robust Median Filtering Forensics Based on the Autoregressive Model of Median Filtered Residual

Xiangui Kang[*†], Matthew C. Stamm[†], Anjie Peng[*] and K. J. Ray Liu[†]
[*]Dept. of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA.
E-mail: isskxg@mail.sysu.edu.cn, mcstamm@umd.edu, kjrliu@umd.edu.
[†]School of Information Science &Technology, Sun Yat-Sen University, Guangzhou, GD 510006 China.

Abstract— **One important aspect of multimedia forensics is exposing an image's processing history. Median filtering is a popular noise removal and image enhancement tool. It is also an effective tool in anti-forensics recently. An image is usually saved in a compressed format such as the JPEG format. The forensic detection of median filtering from a JPEG compressed image remains challenging, because typical filter characteristics are suppressed by JPEG quantization and blocking artifacts. In this paper, we introduce a robust median filtering detection scheme based on the autoregressive model of median filtered residual. Median filtering is first applied on a test image and the difference between the initial image and the filtered output image is called the median filtered residual (MFR). The MFR is used as the forensic fingerprint. Thus, the interference from the image edge and texture, which is regarded as a limitation of the existing forensic methods, can be reduced. Because the overlapped window filtering introduces correlation among the pixels of MFR, an autoregressive (AR) model of the MFR is calculated and the AR coefficients are used by a support vector machine (SVM) for classification. Experimental results show that the proposed median filtering detection method is very robust to JPEG post-compression with a quality factor as low as 30. It distinguishes well between median filtering and other manipulations, such as Gaussian filtering, average filtering, and rescaling and performs well on low-resolution images of size 32 × 32. The proposed method achieves not only much better performance than the existing state-of-the-art methods, but also has very small dimension of feature, i.e., 10-D.**

I. INTRODUCTION

Blind forensics techniques can verify the authenticity of multimedia data without access to the original source, which is very important when contents can be shaved easily. Some content preserving manipulations, such as: filtering [1 - 3], resampling [4], compression [5], and contrast enhancement [6][21] do not damage the authentic value of an image in general, but their blind detection is forensically important [1-3].

The median filter is a popular noise removal and image enhancement tool. It can affect forensic methods in various ways. First, a median filter is capable of removing statistical traces of the blocking artifacts by JPEG compression and defeat JPEG forensic algorithms [7]. It is also an effective counter-forensics tool for hiding traces of resampling [9]. Additionally, the actual state of an image prior to manipulation may influence the set of tools available to analyze the image, or how to interpret the evidence derived from these tools. For example, in steganalysis, the choice of a suitable spatial-domain detector might depend upon the actual state of a cover image and its properties [16].

An image is usually saved in a compressed format such as the JPEG format. Recently, in multimedia forensics and steganalysis, exposing the processing history has drawn much attention [1-3]. A forensic method is generally required to be robust against lossy compression, due to the task of exposing the processing history of possibly severely compressed multimedia. However, this is a challenging work because JPEG quantization and blocking artifacts may destroy the subtle traces that could be utilized to detect median filtering.

In this paper, we propose to perform median filtering on a test image first and output the filtered image. We then obtain the difference between the test image and the median filtered image, which is called the median filtered residual (MFR). The median filtered residual is used as the forensic fingerprint. Thus, the interference from the image edge and texture, which is regarded as a limitation of the existing forensic methods, can be reduced. Because the overlapped window filtering introduces correlation among the pixels of MFR, an autoregressive (AR) model of the MFR is calculated and the AR coefficients are fed into a support vector machine (SVM) for classification. The trained classifier is applied to discriminate a median filtered image from a non-altered image. The proposed method is very robust to JPEG post-compression. It distinguishes well between median filtering and other manipulations, such as Gaussian filtering, average filtering, and rescaling and performs well on low resolution images of size 32 ×32. The proposed method not only achieves much better performance than the existing state-of-the-art methods, but also has very small dimension of feature, i.e., 10-D.

The rest of this paper is organized as follows. In Section 2, we will briefly review some of the existing works on detection of median filtering. In Section 3, the median filtered residual and its AR model are introduced. In Section 4, the proposed MFR algorithm is compared with the state-of-the-art methods [1 - 2] and our experimental results are reported. Finally, we draw the conclusion in Section 5.

II. PRIOR RELATED WORKS

The median filter replaces a pixel with the median of pixels in a small window of size $w \times w$. 3 × 3 and 5 × 5 median filtering are the most widely used forms of median filtering, especially the former. Median filtering is performed window by window with the windows overlapping each other. For example, input an image $x(i,j)$, and output a filtered image:

$$\begin{aligned} & y(i,j) = median\{x(i+h, j+v) \\ & \mid (h,v) \in (-\frac{w-1}{2},...,0,...,\frac{w-1}{2})\} \qquad (1) \\ & (i,j) \in (1,...,M) \times (1,...,N) \end{aligned}$$

where $M \times N$ is the size of the input image. A theoretical analysis of the general relationship between the input and output distributions of the median filter is very cumbersome, because it is a non-linear smoother. Hence, the analysis of median filtering has been largely confined to some specific features of interest [1].

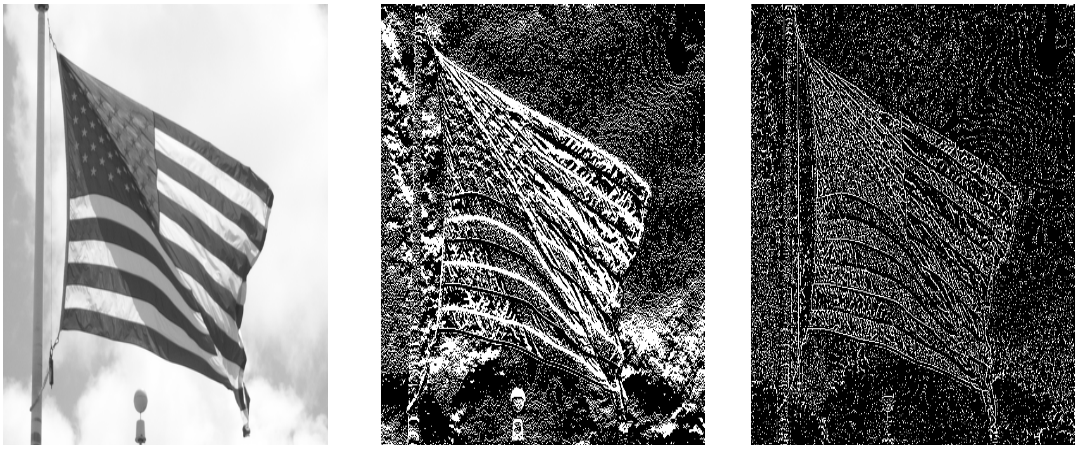
The median filter can remove noise and preserve edges in an image. It can produce constant or nearly constant regions, which are called streak (linear patches) or amorphous blotches [10]. Bovik analyzed this phenomenon quantitatively and obtained the probability that the median values stemming from overlapping windows are equal [10].

There are some existing forensic methods of median filtering. Swaminathan et al. [11] developed a reliable technique based on the intrinsic fingerprints in digital images, to differentiate a median filtered image from an unmodified digital camera image; the true positive rate of median filtering is 70-80% at a false positive rate of 10%. Chuang et al. [12] introduced a tampering detection approach based on the empirical frequency response. Their proposed approach could distinguish between median filtering and other kinds of content preserving manipulation, e.g., JPEG compression, up-sampling, down-sampling, average filtering, and histogram equalization, with an accuracy of about 90%. As pioneering works of median filtering forensics [11-12], the robustness against post-compression was little considered.

Kircher and Fridrich [1] and Cao et al. [3] take the first order difference of an input image as the forensics fingerprint. Assuming an input image is $x(i, j)$, the first order difference is defined as follows:

$$\begin{aligned} & d_{i,j}^{(k,l)} = x(i,j) - x(i+k, j+l), \\ & (i,j) \in (1,...,M) \times (1,...,N), \qquad (2) \\ & (k,l) \in (-1,01) \times (-1,0,1) \,\&\, (k,l) \neq (0,0) \end{aligned}$$

Assume $H^{(k,l)}$ = $\{\ldots, h_{-2}^{(k,l)}, h_{-1}^{(k,l)}, h_{0}^{(k,l)}, h_{1}^{(k,l)}, h_{2}^{(k,l)}, \ldots\}$ is the corresponding histogram of $d_{i,j}^{(k,l)}$. Streaking resulting from median filtering tends to increase the ratio $\rho^{(k,l)} = h_0^{(k,l)} / h_1^{(k,l)}$ Kirchner and Fridrich [1] proposed using the ratio $\rho^{(k,l)}$ as a detection statistic for median filtering. For a median filtered image, the ratio $\rho^{(k,l)} >> 1$. They also developed a weighted median of this ratio to lessen the influence of saturation in an image. In order to improve the robustness against JPEG compression, which defeats the method of using a weighted median of $\rho^{(k,l)}$, Kirchner and Fridrich [1] used subtractive pixel adjacency matrix (SPAM) features [15] to describe the first order difference $d_{i,j}^{(k,l)}$, as shown in Equation (2). The detector obtained reliable results for an uncompressed image and JPEG post-compressed image with a quality factor 90 and 80 on a 512 × 512 grayscale image. However, the SPAM method shares the following weakness: the robustness of the detector against compression rapidly decreases when the size of the test image and the compression quality factor



(a) (b) (c)

Fig. 1. (a) Original image; (b) first-order difference; (c) MFR

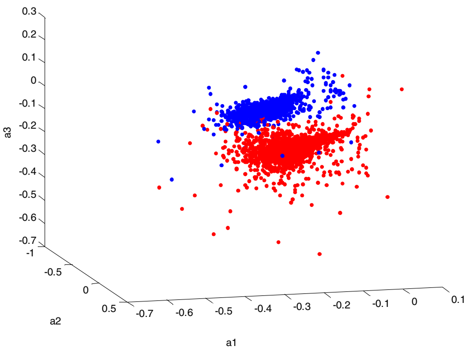


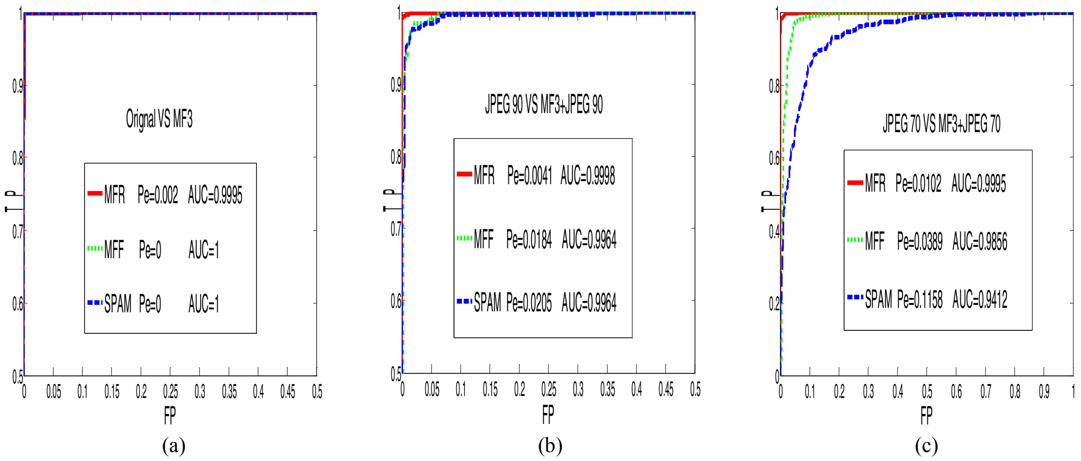
Fig. 2.The AR coefficients of the auto-covariance $R(k, l)$ for unaltered images (red) and the 3x3 median filtered images(blue).

become small. For example, the performance of a 3 × 3 median filtering detector severely degrades when a 512 × 384 test image is JPEG compressed with quality factor less than 90.

Cao et al. [3] proposed that the probability of zeros $h_0^{(k,l)}$ in the first-order difference $d_{i,j}^{(k,l)}$ of a test image in textured regions is the statistical fingerprint of median filtering. Their experimental results show that median filtering is detectable with high accuracy in the case of a median filtered image versus an original non-compressed image. However, their method is not robust to JPEG compression.

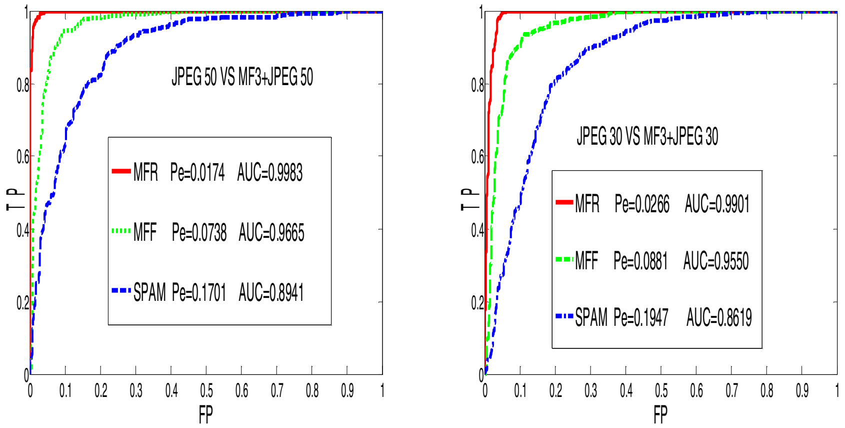
Median values originating from overlapping filter windows are dependent upon each other. The degree of dependence is related to the size of the window and the distance of the pixels. Yuan [2] proposed that local dependence among pixels within a 3 × 3 window is a specific characteristic of median filtering, and constructed a 44-D feature, which is called the median filtering feature (MFF in short), to detect median filtering. The MFF method achieves better performance of detecting 3 × 3 median filtering than that of the SPAM method [1], and comparable robustness to JPEG compression with the SPAM method on detection of 5 × 5 median filtering. The MFF method can also discriminate median filtering from other smoothers, such as a Gaussian filter and moving average filter etc.

Overall, the robustness against JPEG post-compression remains a challenging problem. [1] and [3] take the first order difference $d_{i,j}^{(k,l)}$ as the forensic trace. However, the first order difference $d_{i,j}^{(k,l)}$ contains largely the edge and texture information of an image. Fig. 1 shows the first order difference $d_{i,j}^{(1,0)}$ of an image (Fig. 1a). The edge and texture are obvious in Fig. 1b. The edge and texture interfere with the median filtering detector and thus, deteriorate the performance. Chen *et al* [17] also used the first and second order differences as forensic fingerprints. Yuan [2] used the local dependence among the pixels within a 3 × 3 window. However, the local



(a) (b) (c)

Fig.3. ROC curves of detecting 3x3 median filtering on (a) uncompressed images; (b) JPEG 90 post compressed images; (c) JPEG 70 post compressed images



(a) (b)

Fig.4. ROC curves of detecting 3x3 median filtering on different JPEG compressed images. (a) JPEG 50; (b) JPEG 30.

content of an image, such as edge and texture also has large impact on the detector.

III. MEDIAN FILTERED RESIDUAL

In order to remove the interference from the image content, such as edge and texture, we propose to extract the forensic trace as follows. Apply 3 × 3 median filtering on a test image $x(i, j)$ and obtain the output image $y(i, j)$. The filtered residual is:

$$d(i,j) = y(i,j) - x(i,j),\quad (i,j) \in (1,\cdots,M)\times(1,\cdots,N) \tag{3}$$

where $d(i, j)$ is the median filtered residual (MFR). Fig. 1c shows that the median filtered residual contains less image content, i.e., edge and texture, compared with the image (first order) difference.

Because the overlapped window filtering introduces correlation among the pixels of MFR, we model the MFR using a $n = 10$ order autoregressive (AR) model in order to detect both 3x3 median filtering and 5x5 median filtering. Fig. 2 shows that the AR coefficients (a_1, a_2, a_3) of the MFR from a previous 3 × 3 median filtered images and from the unaltered images are clustered and separated very well.

We propose the following median filtering detection method:

(1) For all images with size of $M \times N$, extract the 2-D MFR array by performing 3 × 3 median filtering.

(2) Fit the MFR to an AR model of order 10 in the row direction and in the column direction [19].

(3) Input the AR coefficients to an SVM classifier trained to classify between median filtered and unaltered images. We employ a C-SVM with Gaussian kernel $k(x,y) = \exp(-\gamma\|x-y\|^2)$ ($\gamma>0$) as the classifier [14]. We search for the best parameters of c and γ in the multiplicative grid $(c, \gamma) \in \{2^i, 2^j \mid 4i, 4j \in Z)\}$ using five-fold cross-validation, and the searching step size of i, j are 0.25. We use those parameters to get the classifier model on the training set.

IV. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed approach, we employ the UCID image database which consists of 1338 uncompressed RGB images of size 512 × 384 [13] and BOWS image database [20]. Because the results with two image databases are similar to each other and the UCID database is widely used ([2-3], [5-7]), the results with the UCID database are reported in detail in this paper. Many of the images in the UCID database have significant regions of either saturated pixels or largely smooth patches. Some images are out of focus or contain blur from camera shake. All of the images are converted to gray-scale images before any further processing. The size of the training set is approximately 60% of the database size (850 images). The rest of the images (488 images) constitute the testing image set.

The performance of the proposed MFR algorithm is evaluated using the area under the ROC curves (AUC in short form) and the minimal average decision error P_e under the assumption of equal priors and equal costs [1].

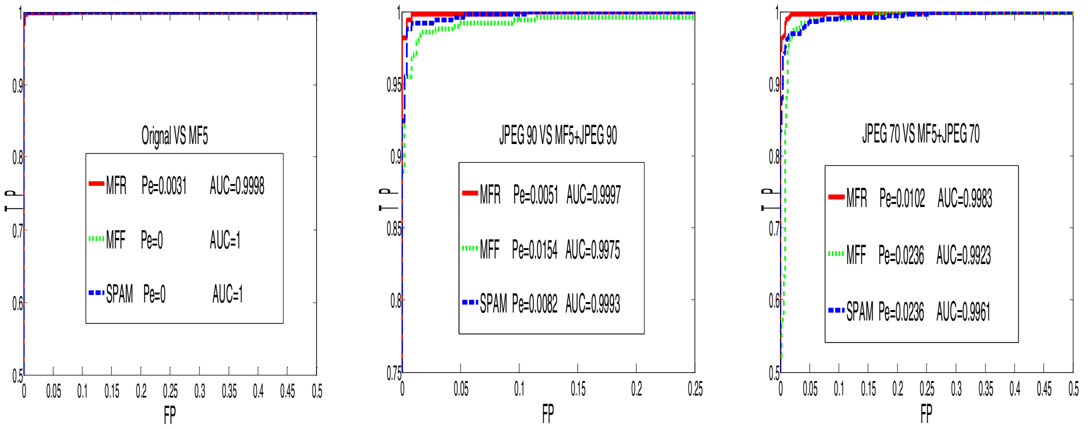
$$P_e = \min(\frac{P_{fp} + 1 - P_{tp}}{2}) \tag{4}$$

where P_{fp} and P_{tp} denote the false positive (FP) and true positive rates (TP), respectively.

TABLE I **P_E AND AUC OF MEDIAN FILTERING DETECTORS OF MF3 AND MF5**

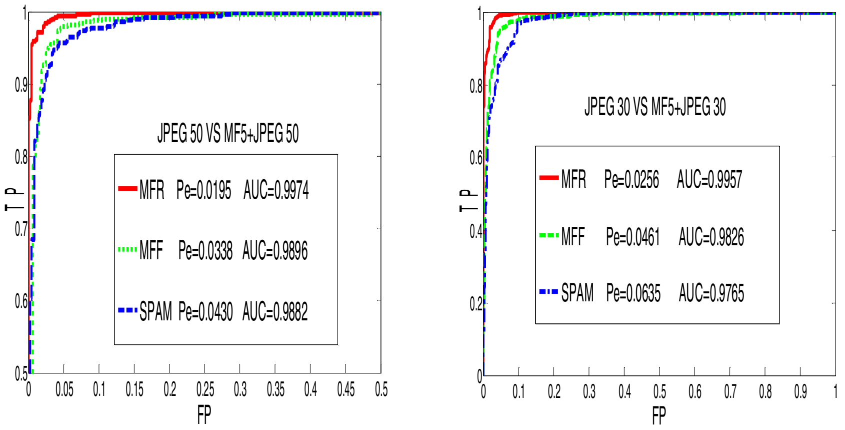
		MF3			MF5		
		MFR	MFF	SPAM	MFR	MFF	SPAM
Dimension		10	44	343	10	44	343
JPEG 90	P_e (%)	0.41	1.84	2.05	0.51	1.54	0.82
	AUC(%)	99.98	99.64	99.64	99.97	99.75	99.93
JPEG 70	P_e (%)	1.02	3.89	11.6	1.02	2.36	2.36
	AUC(%)	99.95	98.56	94.12	99.83	99.23	99.61
JPEG 50	P_e (%)	1.74	7.38	17.0	3.38	3.38	4.30
	AUC(%)	99.83	96.65	89.41	99.74	98.96	98.82
JPEG 30	P_e (%)	2.66	8.81	19.47	2.56	4.61	6.35
	AUC(%)	99.01	95.50	86.19	99.57	98.26	97.65

We compare the proposed MFR method with the state-of-the-art works – both the SPAM method [1] and Yuan's



(a) (b) (c)

Fig.5. ROC curves of detecting 5x5 median filtering on (a) uncompressed images; (b) JPEG 90 compressed images;(c)JPEG 70 compressed images



(a) (b)

Fig.6. ROC curves of detecting 5x5 median filtering on JPEG post compressed image with different QF. (a) JPEG 50; (b) JPEG 30.

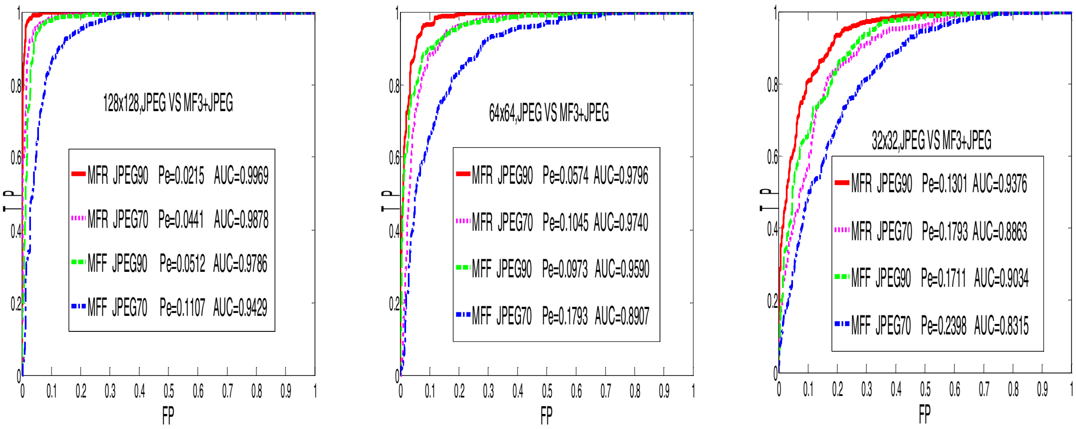


Fig.7. ROC curves of discriminating 3x3 median filtering on a JPEG post-compressed image for varying image size 128x128(left), 64x64(middle), 32x32(right)

median filter feature (MFF) method [2]. For SPAM methods, only the horizontal and vertical features are chosen, which results in 343 dimensions of feature. The MFF method has 44 dimensions of feature [2]. SVM training for the three methods is similar. The ROC curves of detecting 3 × 3 median filtering (MF3 in short form) and 5 × 5 median filtering (MF5 in short form) are shown in Figs 3-9. The detailed classification results are shown in Table I. "Original VS MF3" denotes that the original unmodified image is the negative sample, and the 3 × 3 median filtered image is the positive sample. "MF3+JPEG70" denotes the composite operation of median filtering and JPEG post-compression with quality factor 70.

1) Detect MF3 on an uncompressed image

For the uncompressed gray-scale image set, the three methods have similar performance; MF3 can be detected at P_e as low as 0.0051 or 0 (Fig. 3a).

2) Detect MF3 on a JPEG post-compressed image

Our proposed method is much more robust against JPEG post-compression. It is observed that the proposed MFR classifier achieves much better performance than both the SPAM classifier and the MFF classifier. The ROC curve of the proposed MFR method is always above the ROC curve of the other two methods. In particular, the advantage of the MFR method over the other two comparison methods increases when the JPEG compression quality changes from 90 to 30 (Figs 3&4, respectively). It demonstrates that the proposed MFR method is much more robust against JPEG compression than the other methods. The minimal average decision error P_e of MFR classifier is P_e = 0.0041, 0.0102, 0.0174, 0.0266 for JPEG 90, JPEG 70, JPEG 50, JPEG 30 respectively, AUC = 0.9998, 0.9995, 0.9983, 0.9901 respectively. For the *SPAM* classifier, P_e = 0.0205, 0.1158, 0.1701, 0.1947 respectively, AUC = 0.9964, 0.9412, 0.8941, 0.8619 respectively. For the MFF classifier, P_e = 0.0184, 0.0389, 0.0738, 0.0881 respectively, AUC = 0.9964, 0.9856, 0.9665, 0.9550 (Table I).

3) Detect MF5

A similar significant improvement in performance is observed in the detection of 5 × 5 median filtering. The detection results of 5 × 5 median filtering are shown in Figs 5&6 and Table I. Better performance over both comparison methods, is achieved in the detection of 5 × 5 median filtering on different JPEG post-compressed images. For MFR classifier, P_e = 0.0051, 0.0102, 0.0195, 0.0256 for JPEG 90, JPEG 70, JPEG 50, JPEG 30 respectively, AUC = 0.9997, 0.9983 0.9974, 0.9957 respectively. For the SPAM classifier, P_e = 0.0082, 0.0236, 0.043, 0.0635 respectively, AUC = 0.9993, 0.9961, 0.9882, 0.9765 respectively. For the MFF classifier, P_e = 0.0154, 0.0236, 0.0338, 0.0461respectively. AUC = 0.9975, 0.9923, 0.9896, 0.9826 respectively (Table I). The experimental result shows that the performance of the MFR classifier keeps excellent when the JPEG compression quality factor changes from 90 to 30 in detection of 5x5 median filtering.

4) Detect median filtering in a low-resolution and post-compressed image

The ability to detect median filtering in low-resolution images is essential for detecting forgery when a portion of a median filtered image is inserted into a non-median filtered image. We first crop an image block with size of 128 × 128, 64 × 64 and 32 × 32 from the center of an image, and then build a corresponding training set and testing set. The SPAM detector is an evaluation of second-order Markov chains of the first-order difference of an image, and the detectability degrades severely for low-resolution images. As indicated in [2], MFF is superior to SPAM in the detection of 3 × 3 median filtering on an image of low resolution. For the sake of

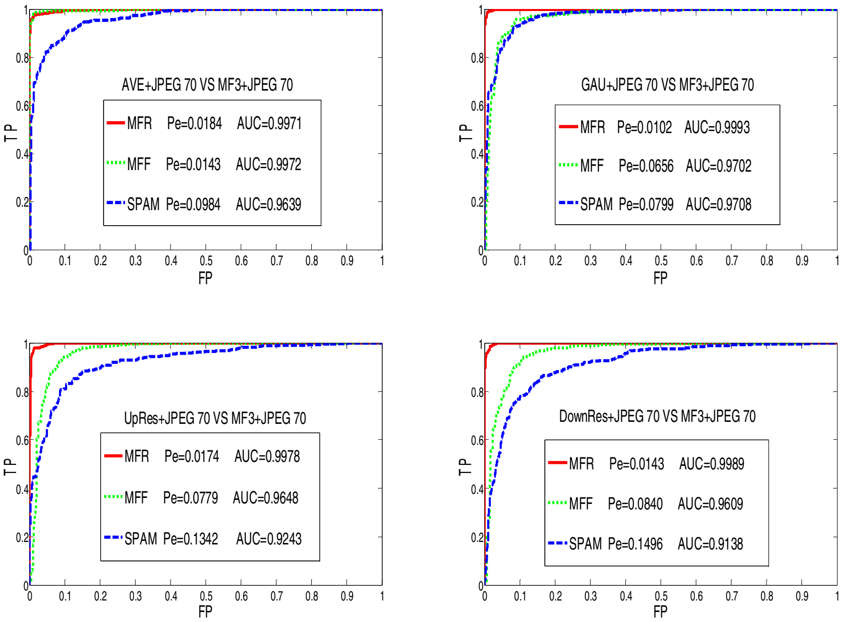


Fig.8. ROC curves of discriminating 3x3 median filtering on a JPEG 70 post-compressed image from average filtering(top left), Gaussian filtering(top right), upscaling(bottom left), downscaling(bottom right).

brevity, we only compare MFR with MFF on JPEG 90 or JPEG 70 post-compressed images. It is obvious that the performance of the proposed MFR detector is much better than that of the MFF detector (Fig. 7). For the resolution as low as 32x32, MFR detector obtains reliable results for both JPEG 90 (P_e = 0.1301, AUC = 0.9376) and JPEG 70 (P_e = 0.1793, AUC = 0.8863) compression. The similar experimental results are obtained in the detection of 5x5 median filtering on an image of low resolution.

5) Distinguish median filtering from other manipulations

Differentiating median filtering from other manipulations is very important for manipulation

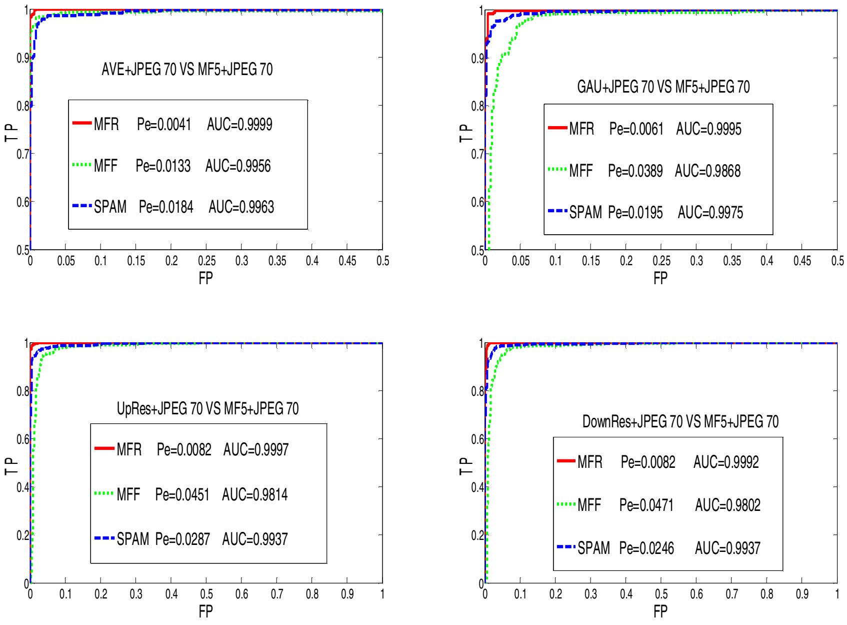


Fig.9. ROC curves of discriminating 5x5 median filtering (MF5) from average filtering (top left), Gaussian filtering (top right), up-scaling (bottom left), downscaling (bottom right).

forensics. Finally, we test whether the proposed MFR method and the comparison methods can differentiate median filtering from other popular tools, including average filtering (AVE), Gaussian filtering (GAU), upscaling operations (UpRes) and downscaling operations (DownRes). The interpolation adopted in a rescaling operation is bilinear. The upscaling factor is set to 1.1, while the downscaling factor is 0.9. For an image without post-processing by JPEG compression, the three methods can distinguish median filtering (3 × 3 or 5 × 5) from other operations perfectly well; the minimal average decision error P_e of the MFR classifier in distinguishing median filtering from other operations achieves zero. For the case of an image post-processed by JPEG 70, experimental results show that MFR can discriminate 3 × 3 median filtering from the other four operations with high accuracy (the worst value of P_e is only 0.0184) (Fig. 8). For 5 ×5 median filtering, we obtain similar results. The proposed classifier can distinguish 5 × 5 median filtering from other manipulations with high accuracy (Fig. 9) and the proposed method outperforms both comparison methods, achieving the best performance.

The results in Table I and these figures indicate that the performance of our proposed method is very superior and stable, even when the JPEG compression quality factor becomes low. The P_e of MFR method varies from 0.0041 to 0.0266, while AUC varies from 0.9901 to 0.9998. The performance of both the MFF and SPAM classifiers deteriorates severely when the JPEG compression quality factor is low. The MFR classifier achieves much better robustness against JPEG post-compression than both comparison methods.

In this paper, we do not discuss the case of median filtering pre-compression, i.e., median filtering of already JPEG compressed images because a low pre-compression quality can even increase the detector's performance.

V. Conclusions

In this paper, we propose to use median filtering residual to detect median filtering. The major contributions of this paper are as follows:

1) We have shown that applying median filtering to extract the median filtered residual is a very effective median filtering detection method. Compared with the technique of using image differences as the forensic fingerprint, the interference from the image edge and texture can be reduced.

2) Because the overlapped window filtering introduces correlation among the pixels of MFR, the n = 10 order autoregressive (AR) model is used to describe the MFR in order to detect median filtering with a window no larger than 5x5.

3) Experimental results on several large image databases show the proposed method is very robust to JPEG post-compression, distinguishing well between median filtering and other manipulations such as Gaussian filtering, average filtering and rescaling, and it performs well on low-resolution images of size 32 ×32. The proposed method achieves not only much better performance than the existing state-of-the-art methods, but also has very small (least among three methods) dimension of feature.

The developed method is suitable for use in the forensics of image processing history and can enhance security in resisting anti-forensic attack. The proposed filtered residual fingerprint can be applied to detect linear filtering, compressive sensing compression and other signal manipulation and this would be a part of our future work.

Acknowledgment

This work was supported by NSFC(61070167), 973 program (2011CB302204), PPFMEC(20110171110042) and NSFC (U1135001). The authors thank Dr. H. Yuan for providing the code of MFF scheme in [2].

References

[1] M. Kirchner and J. Fridrich. On detection of median filtering in digital images. In *Proc. SPIE, Electronic Imaging, Media Forensics and Security II*, vol. 7541, pp. 1–12, 2010.

[2] Haidong Yuan. Blind Forensics of Median Filtering in Digital Images. *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1335-1345, Dec. 2011.

[3] Gang Cao, Yao Zhao, Rongrong Ni, Lifang Yu and Huawei Tian. Forensic detection of median filtering in digital images. In *Proc.2010 IEEE Int. Conf. Multimedia and EXPO* 2010, pp. 89–94, 2010.

[4] A. C. Popescu and H. Farid. Exposing digital forgeries by detecting traces of resampling. *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp.758-767, 2005.

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

[6] M. C. Stamm and K. J. R. Liu. Forensic estimation and reconstruction of a contrast enhancement mapping, In *International Conf. on Acoustics, Speech and Signal Processing*, Dallas, Texas, USA, 2010.

[7] M. C. Stamm and K. J. Ray Liu. Anti-Forensics of Digital Image Compression. *IEEE Trans. Inf. Forensics Security*, vol. 6, no.3, pp.1050-1065, Sept 2011.

[8] A. E. Dirik and N. Memon. Image tamper detection based on demosaicing artifacts. In *International Conference Proceedings on Image Processing*, Cairo, 2009.

[9] M. Kirchner and R. Bohme. Hiding traces of resampling in digital images. *IEEE Trans. Inf. Forensics Security*, vol. 3, no.4, pp. 582–592, Dec. 2008.

[10] A. C. Bovik. Streaking in median filtered images. *IEEE Transactions on Acoustics, Speech and Signal Processing*, 35(4), pp. 493-503, 1987.

[11] A. Swaminathan, M. Wu, and K. J. Liu. Digital image forensics via intrinsic fingerprints. *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 101–117, 2008.

[12] W. H. Chuang, A. Swaminathan, and M. Wu. Tampering identification using empirical frequency response. In *Proc. IEEE Int. Conf. Acoust., Speech and Signal Processing*, pp. 1517–1520, 2009.

[13] G. Schaefer and M. Stich. 2004. UCID-An uncompressed color image database. In Proceedings of *SPIE, Storage and Retrieval Methods and Applications for Multimedia*, 2004, pp. 472–480.

[14] Chih-Chung Chang and Chih-Jen Lin. LIBSVM: a library for support vector machines.*ACM Transactions on Intelligent Systems and Technology*, 2:27:1~27:27, 2011.

[15] T. Pevý, P. Bas, and J. Fridrich. Steganalysis by subtractive pixel adjacency matrix. *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 215–224, Jun. 2010.

[16] A. D. Ker and R. Bohme. Revisiting weighted stego-image stegoanalysis, in *Proceedings of SPIE, Electronic Imaging: Security, Forensics, Steganography and Watermarking of Multimedia Contents X*, vol. 6819, pp. 5, 2008.

[17] C. Chen, J. Ni et al, "Blind Median Filtering Detection Using Statistics in Difference Domain", in *Proc. of information Hiding 2012*, Berkerly, USA, May. 2012.

[18] X. Kang, J. Huang, W. Zeng, "Efficient General Print-Scanning Resilient Data Hiding Based on Uniform Log-Polar Mapping," *IEEE Transactions on Information Forensic and Security*, vol. 5, no.1, pp.1-12, Mar. 2010.

[19] Steven M. Kay, "Modern spectral estimation: theory and application," Prentice Hall, Englewood Cliffs, NJ, USA, 1998.

[20] http://boss.gipsa-lab.grenoble-inp.fr/BOSSRank/index.php?model-VIEW&tmpl-materials.

[21] M. C. Stamm and K. J. R. Liu, "Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", IEEE Trans. on Information Forensics and Security, vol. 5, no. 3, pp. 492 - 506, Sep. 2010.