BLIND METHODS FOR DETECTING IMAGE FAKERY

Babak Mahdian
Institute of Information Theory and
Automation of the ASCR
Pod Vodárenskou věží 4, 18208 Prague
Czech Republic
mahdian@utia.cas.cz

Stanislav Saic
Institute of Information Theory and
Automation of the ASCR
Pod Vodárenskou věží 4, 18208 Prague
Czech Republic
ssaic@utia.cas.cz

Abstract - In today's digital age, it is possible to effortlessly create image forgeries without leaving any obvious traces of tampering. In this paper we bring a brief review of existing blind methods for detecting image fakery. Blind methods are regarded as a new direction and work without using any prior information about the image being investigated or its source.

Index Terms - Image forensics, Image Fakery, Tamper detection, Forgery detection, Authentication.

I. INTRODUCTION

The trustworthiness of photographs has an essential role in many areas, including: forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services, medical imaging, and journalism. The art of making image fakery has a long history (for an example of earlier image forgeries see Figure 1). But, in today's digital age, it is possible to very easily change the information represented by an image without leaving any obvious traces of tampering. This is mainly due to the advent of low–cost, high–performance computers and more friendly human–computer interfaces. Despite this, no system yet exists which accomplishes effectively and accurately the image tampering detection task.

There are many ways to categorize the image tampering based on various points of view (for an categorization see, for example, [2]). Generally, we can say that the most often operations in photo manipulation are:

- Deleting or hiding a region in the image.
- Adding a new object into the image.
- Misrepresenting the image information.

The digital information revolution and issues concerned with multimedia security have also generated several approaches to authentication and tampering detection. Generally, these approaches could be divided into active and passive–blind approaches. The area of active methods simply can be divided into the data hiding approach and the digital signature approach.

By data hiding we refer to methods embedding secondary data into the image. The most popular part of this area belongs to digital watermarks [1, 16, 24]. Many watermarks have been proposed so far. Digital watermarking assumes an inserting of a digital watermark at the source side (e.g., camera) and verifying the mark integrity at the detection side. Watermarks mostly are inseparable from the digital image they are embedded in, and they undergo the same transformations as the image itself. A major drawback of watermarks is that the they must be inserted either at the time of recording the image, or later by a person authorized to do so. This limitation requires specially equipped cameras or subsequent processing of the original image. Furthermore, some watermarks may degrade the image quality.

The digital signature approach [10, 11, 25] consists mainly of extracting unique features from the image at the source side and encoding these features to form digital signatures. Afterwards signatures are used to verify the image integrity.

In this work, we focus on blind methods, as they are regarded as a new direction and in contrast to active methods, they work in absence of any protecting techniques and without using any prior information about the image or the camera that took the image. To detect the traces of tampering, blind methods use the image function and the fact that forgeries can bring into the image specific detectable changes (e.g., statistical changes).

Our aim is to provide a brief review of a recent and relevant blind mathematical and computational image forgery detection methods. We do not contemplate to go into

Figure 1: An example of earlier image forgeries. In the winter of 1948, the photographer Karel Hájek and Vlado Clementis, one of the victims of the purges following the coup of 1948, were removed from the photograph (Czechoslovakia).

details of particular methods or describe results of comparative experiments.

Please note that when digital watermarks or signatures are not available, the blind approach is the only way to make the decision about the trustworthiness of the investigated image. Image forensics is a burgeoning research field and promise a significant improvement in forgery detection in the never–ending competition between image forgery creators and image forgery detectors.

II. METHODS

In recent years various methods for detecting image fakery appeared. In this paper we focus on blind methods using the detection of traces of

- near–duplicated image regions,
- interpolation and resampling,
- inconsistencies in chromatic aberration,
- noise inconsistencies,
- double JPEG compression,
- inconsistencies in color filter array (CFA) interpolated images,
- inconsistencies in lighting.

A. Detection of Near–Duplicated Image Regions

In a common type of digital image forgery, called copy–move forgery, a part of the image is copied and pasted into the another part of the same image, typically with the intention to hide an object or a region (for an example see Figure 2). The copy–move forgery brings into the image several near–duplicated image regions. So, detection of such regions may signify tampering. It is important to note that duplicated regions mostly are not identical. This is caused by lossy compression algorithms, such as JPEG, or by possible additional use of retouch tools. Existing near–duplicated regions detection methods mostly have several steps in common: tiling the image with overlapping blocks, feature representation and matching of these blocks.

The first copy–move detection method has been proposed by Fridrich et al. [4]. The detection of duplicated regions is based on matching the quantizied lexicographically sorted discrete cosine transform (DCT) coefficients of overlapping image blocks. The lexicographically sorting of DCT coefficients is carried out mainly to reduce the computational complexity of the matching step. The second method has been proposed by Popescu and Farid [18] and is similar to [4]. This method differs from [4] mainly in the representation of overlapping image blocks. Here, the principal component transform (PCT) has been employed in place of DCT. The next copy–move detection method has been proposed by B. Mahdian and S. Saic [13]. In this work, overlapping blocks are represented by 24 blur moment invariants up to the seventh order. This allows successful detection of copy–move forgery, even when blur degradation, additional noise, or arbitrary contrast changes are present in the duplicated regions. The blocks matching phase is carried out using a kd–tree representation.

B. Detection of Traces of Resampling and Interpolation

When two or more images are spliced together (for an example see Figure 3), to create high quality and consistent image forgeries, almost always geometric transformations such as scaling, rotation or skewing are needed. Geometric transformations typically require a resampling

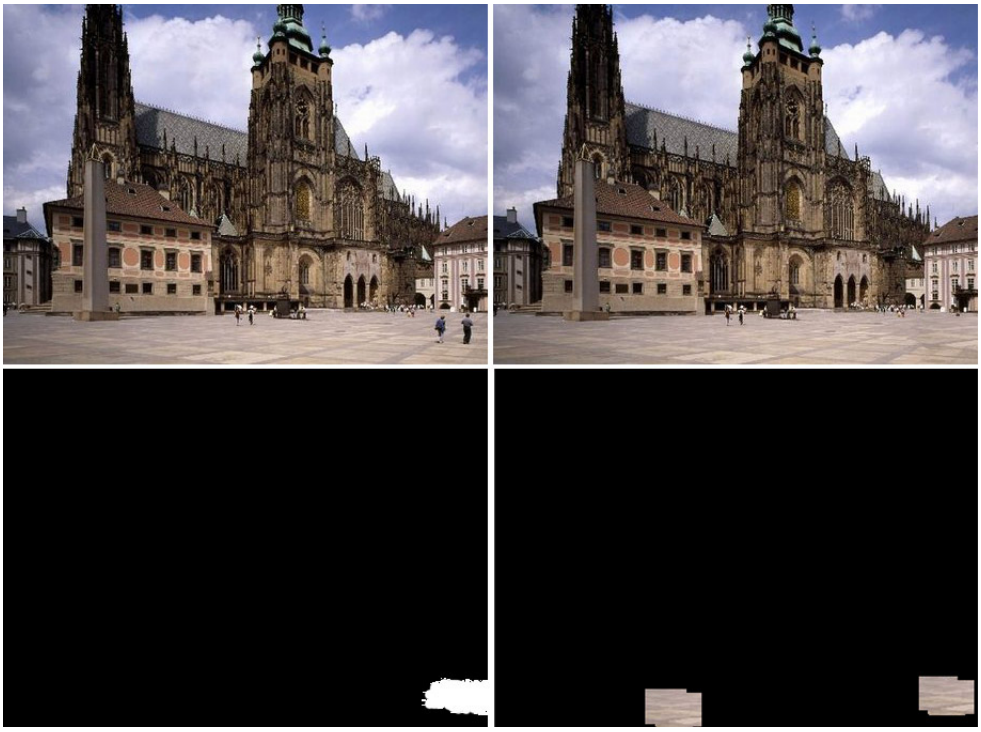

Figure 2: Shown are: original image (top left), an example of a copy–move forgery (top right), the difference between the original image and its fake version (bottom left), and the duplicated regions map created by application of the near–duplicated image regions detection method [13] to the top right image.

and interpolation step. Therefore, by having sophisticated resampling/interpolation detectors, altered images containing resampled portions can be identified and their successful usage significantly reduced. Existing detectors use the fact that the interpolation process brings into the signal specific detectable statistical changes.

In [20], A. C. Popescu and H. Farid have analyzed the imperceptible specific correlations brought into the resampled signal by the interpolation step. Their interpolation detection method is based on the fact that in a resampled signal it is possible to find a set of periodic samples that are correlated in the same way as their neighbors. The core of the method is an Expectation/Maximization (EM) algorithm. The main output of the method is a probability map containing periodic patterns if the investigated signal has been resampled. In [12], B. Mahdian and S. Saic have analyzed specific periodic properties present in the covariance structure of interpolated signals and their derivatives. Furthermore, an application of Taylor series to the interpolated signals showing hidden periodic patterns of interpolation is introduced. The paper also proposes a method capable of easily detecting traces of scaling, rotation, skewing transformations and any of their arbitrary combinations. The method works locally and is based on a derivative operator and radon transformation. In [9], Matthias Kirchner gives an analytical description about how the resampling process influences the appearance of periodic artifacts in interpolated signals. Furthermore, this paper introduces a simplified resampling detector based on cumulative periodograms. In [5], A. C. Gallagher in an effort to detect interpolation in digitally zoomed images has found that linear and cubic interpolated signals introduce periodicity in variance function of their second order derivative. This periodicity is simply investigated by computing the DFT of an averaged signal obtained from the second derivative of the investigated signal. Another work concerned with the detection of resampling and interpolation has been proposed by S. Prasad and K. R. Ramakrishnan [23]. Similar to [5], the authors have noticed that the second derivative of an interpolated signal produces detectable periodic properties. The periodicity is simply detected in the frequency domain by analyzing a binary signal obtained by zero crossings of the second derivative of the interpolated signal.

C. Detection of Inconsistencies in Chromatic Aberration

Optical imaging systems are not ideal and often bring different types of aberrations into the captured images.

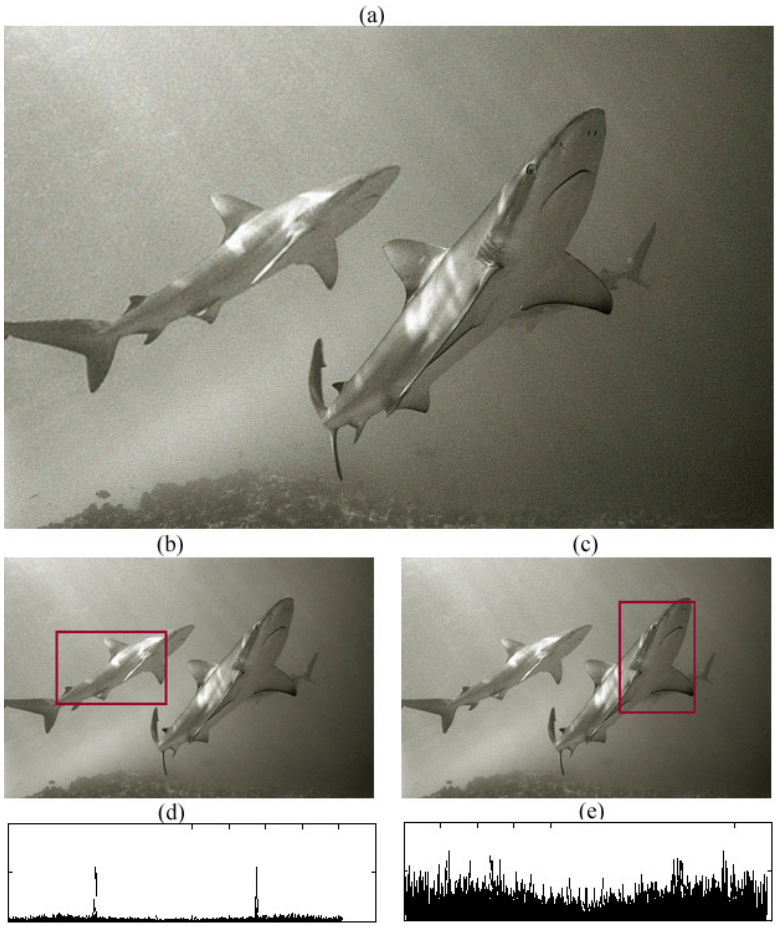

Figure 3: Shown are: an image containing a resampled region (a). In this image, the shark on the left side has been resized by factor 1.4 using the bicubic interpolation. Output of the resampling detector described in [12] is shown in (d). Peaks clearly signify the presence of interpolation. The method has been applied to the denoted region shown in (b). The output of [12] applied a non–resampled region is shown in (c). The testes region is shown in (c).

Chromatic aberration is caused by the failure of the optical system to perfectly focus light of all wavelengths. This type of aberration can be divided into longitudinal and lateral. Lateral aberration happens by a spatial shift in the locations where light of different wavelengths reach the sensor. This causes various forms of color imperfections in the image.

As shown in [6], when an image is altered, the lateral chromatic aberration can become inconsistent across the image. This may signify tampering. It is possible to model the lateral aberration as an expansion/contraction of the color channels with respect to one another. In [6], M. K. Johnson and H. Farid approximate this using a low-parameter model. The model describes the relative positions at which light of varying wavelength strikes the sensor. The model parameters are estimated using an automatic technique based on maximizing the mutual information between color channels.

D. Detection of Image Noise Inconsistencies

A commonly used tool to conceal traces of tampering is addition of locally random noise to the altered image regions. Generally, the noise degradation is the main cause of failure of many active and passive image forgery detection methods. Typically, the amount of noise is uniform across the entire authentic images. Adding locally random noise may cause inconsistencies in the images noise (for an example see Figure 4). Therefore, the detection of various noise levels in an image may signify tampering.

A. C. Popescu and H. Farid have proposed in [19] a noise inconsistencies detection method based on estimat-

Figure 4: Shown are the original image (a), the doctored image containing a duplicated region additionally corrupted by local additive white Gaussian noise with $\sigma = 2.5$(b) the noise corrupted region (c) and the output of the method proposed in [14] applied to the doctored image (d).

ing the noise variance of overlapping blocks by which they tile the entire investigated image. The method uses the second and fourth moments of the analyzed block to estimate the noise variance. The proposed method assumes white Gaussian noise and a non-Gaussian uncorrupted image. Another method capable of detecting image noise inconsistencies is proposed in [14] by B. Mahdian and S. Saic. The method is based on tiling the high pass diagonal wavelet coefficients of the investigated image at the highest resolution with non–overlapping blocks. The noise variance in each block is estimated using a widely used medianbased method. Once the noise variance of each block is estimated, it is used as a homogeneity condition to segment the investigated image into several homogenous subregions.

E. Detection of Double JPEG Compression

The Joint Photographic Experts Group (JPEG) has become an international standard for image compression. In order to alter a JPEG image, typically the image must be loaded onto a photo–manipulating software, decompressed and after the editing process is finished, the digital image must be compressed again and re–saved. Hence, the newly created JPEG image will be double or more times JPEG compressed. This introduces specific detectable changes into the image. So, detection of these artifacts and the knowledge of images JPEG compression history can be helpful in finding the traces of tampering.

In [3], J. Fridrich and J. Lukas describe characteristic features that occur in DCT histograms of individual coefficients due to double compression. Furthermore, they propose a neural network classifier based method capable of estimating the original quantization matrix from double compressed images. Another method has been proposed by A.C. Popescu and H. Farid in [22]. They also use the fact that double JPEG compression introduces specific artifacts detectable in the histograms of DCT coefficients. They have proposed a quantitative measure for mentioned artifacts and used it to distinguish between single and double JPEG compressed images.

F. Detection of Inconsistencies in Lighting

As well–known, the problem of estimating the illuminant direction is a popular task in in computer graphics [15, 17, 26]. Photographs are taken under different lighting conditions. Thus, when two or more images are spliced

together to create an image forgery, it is difficult to keep the lighting conditions (light sources, directions of lights, etc.) correct and consistent across the image (e.g., shadings). Therefore detecting lighting inconsistencies can be a proper way to find the traces of tampering.

As pointed out in [7], under certain simplifying assumptions, arbitrary lighting environments can be modeled with a 9–dimensional model based on a linear combination of spherical harmonics. In [7], M. K. Johnson and H. Farid have shown how to approximate a simplified lower–order 5–dimensional version of this model from a single image and how to stabilize the model estimation in the presence of noise. Another work from same authors [8] focuses on image forgeries created by splicing photographs of different people. As pointed out in [8], specular highlights that appear on the eye are a powerful way to get valuable information about the light sources. Based on this fact authors suggest how to estimate the light source from these highlights and use the potential inconsistencies as an evidence of tampering.

G. *Detection of Inconsistencies in Color Filter Array Interpolation*

Many digital cameras are equipped with a single chargecoupled device (CCD) or complementary metal oxide semiconductor (CMOS) sensor (mainly due to the cost considerations). These sensors are monochromatic. Typically, the color images are obtained in conjunction with a color filter array. The most often used filter is called Bayer filter (named for its inventor, doctor B.E. Bayer from Eastman Kodak) which gives information about the intensity of light in red, green, and blue wavelength regions (the filter pattern is 50% green, 25% red and 25% blue). So, using a CFA, at each pixel location only a single color sample is captured. Missing colors are computed by an interpolating process, called CFA interpolation. This process introduces specific correlations between the pixels of the image (a subset of pixels within a color channel are periodically correlated to their neighboring pixels), which can be corrupted by the tampering process. Hence, these hardware features can also be used to detect the traces of forgery.

A.C. Popescu and H. Farid in [21] have described the specific correlations brought by the CFA interpolation into the image and have proposed a method capable of their automatic detection. The method is based on an expectation/maximization (EM) algorithm and uses a simple linear model. The method is evaluated for several different CFA interpolation algorithms: bilinear, bicubic, smooth hue transition, median–based, gradient-based, adaptive color plane and the threshold–based variable number of gradients.

III. CONCLUSIONS

Our focus in this paper has been addressed to digital image forensics. Digital image forensics is a new and rapidly growing research field. We have introduced various existing blind methods for image tamper detection. Probably the main drawback of existing methods is highly limited usability and reliability. This is mainly caused by the complexity of the problem and the blind character of approaches. But it should be noted that the area is growing rapidly and results obtained promise a significant improvement in forgery detection in the neverending competition between image forgery creators and image forgery detectors.

IV. ACKNOWLEDGEMENTS

This work has been supported by the Czech Science Foundation under the project No. GACR 102/08/0470.

V. REFERENCES

[1] M. Arnold, M. Schmucker, and S. D. Wolthusen. *Techniques and Applications of Digital Watermarking and Content Protection*. Artech House, Inc., Norwood, MA, USA, 2003.

[2] H. Farid. Creating and detecting doctored and virtual images: Implications to the child pornography prevention act. *Department of Computer Science, Dartmouth College*, TR2004-518:13, 2004.

[3] J. Fridrich and J. Lukas. Estimation of primary quantization matrix in double compressed jpeg images. In *Proceedings of DFRWS*, volume 2, Cleveland, OH, USA, August 2003.

[4] J. Fridrich, D. Soukal, and J. Lukas. Detection of copy–move forgery in digital images. In *Proceedings of Digital Forensic Research Workshop*, pages 55–61, Cleveland, OH, USA, August 2003. IEEE Computer Society.

[5] A. C. Gallagher. Detection of linear and cubic interpolation in jpeg compressed images. In *CRV '05: Proceedings of the The 2nd Canadian Conference on Computer and Robot Vision (CRV'05)*, pages 65–72, Washington, DC, USA, 2005. IEEE Computer Society.

[6] M. Johnson and H. Farid. Exposing digital forgeries through chromatic aberration. In *ACM Multimedia and Security Workshop*, Geneva, Switzerland, 2006.

[7] M. Johnson and H. Farid. Exposing digital forgeries in complex lighting environments. *IEEE Transactions on Information Forensics and Security*, 3(2):450–461, 2007.

[8] M. Johnson and H. Farid. Exposing digital forgeries through specular highlights on the eye. In *9th International Workshop on Information Hiding*, Saint Malo, France, 2007.

[9] M. Kirchner. Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue. In *in Proceedings of ACM Workshop on Multimedia and Security*, September 2008.

[10] C. Y. Lin and S. F. Chang. Generating robust digital singnature for image/video authentication. In *ACM Multimedia Workshop*, pages 115–118, 1998.

[11] C. S. Lu and H. M. Liao. Structural digital signature for image authentication: an incidental distortion resistant scheme. In *MULTIMEDIA '00: Proceedings of the 2000 ACM workshops on Multimedia*, pages 115–118, New York, NY, USA, 2000. ACM Press.

[12] B. Mahdian and S. Saic. Blind authentication using periodic properties of interpolation. *IEEE Transactions on Information Forensics and Security, in press (DOI: 10.1109/TIFS.2004.924603), 2008*.

[13] B. Mahdian and S. Saic. Detection of copy–move forgery using a method based on blur moment invariants. *Forensic science international*, 171(2–3):180–189, 2007.

[14] B. Mahdian and S. Saic. Detection of resampling supplemented with noise inconsistencies analysis for image forensics. In *International Conference on Computational Sciences and Its Applications*, pages 546–556, Perugia, Italy, July 2008. IEEE Computer Society.

[15] J. marie Pinel, H. Nicolas, and C. L. Bris. Estimation of 2d illuminant direction and shadow segmentation in natural video sequences. In *in Proceedings of VLBV*, pages 197–202, 2001.

[16] P. Moulin. The role of information theory in watermarking and its application to image watermarking. *Signal Processing*, 81(6):1121–1139, 2001.

[17] A. P. Pentland. Finding the illuminant direction. *Journal of the Optical Society of America (1917-1983)*, 72:448–455, April 1982.

[18] A. Popescu and H. Farid. Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Department of Computer Science, Dartmouth College, 2004.

[19] A. Popescu and H. Farid. Statistical tools for digital forensics. In *6th International Workshop on Information Hiding*, pages 128–147, Toronto, Cananda, 2004.

[20] A. Popescu and H. Farid. Exposing digital forgeries by detecting traces of re-sampling. *IEEE Transactions on Signal Processing*, 53(2):758–767, 2005.

[21] A. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. *IEEE Transactions on Signal Processing*, 53(10):3948–3959, 2005.

[22] A. C. Popescu. *Statistical Tools for Digital Image Forensics*. PhD thesis, Department of Computer Science, Dartmouth College, Hanover, NH, 2005.

[23] S. Prasad and K. R. Ramakrishnan. On resampling detection and its application to image tampering. In *Proceedings of the IEEE International Conference on Multimedia and Exposition*, pages 1325–1328, Toronto, Canada, 2006.

[24] C. Rey and J.-L. Dugelay. A survey of watermarking algorithms for image authentication. *EURASIP Journal on applied Signal Processing Volume 2002 N6 - June 2002, special issue on image analysis for multimedia interactive services*, pages 613–621, 2002.

[25] M. Schneider and S. F. Chang. A robust content based digital signature for image authentication. In *IEEE International Conference on Image Processing (ICIP'96)*, 1996.

[26] Q. Zheng and R. Chellappa. Estimation of illuminant direction, albedo, and shape from shading. *IEEE Trans. Pattern Anal. Mach. Intell.*, 13(7):680–702, 1991.

VI. VITA

Stanislav Saic received the M.Sc. degree in Physical Electronics from the Czech Technical University, Prague, Czech Republic, in 1973, and the CSc. degree (corresponding to Ph.D. degree) in Radioelectronics from the Czechoslovak Academy of Sciences, Prague, Czech Republic, in 1980. Since 1973, he has been with the Institute of Information Theory and Automation, Academy of Sciences of the Czech Republic, Prague, where he held the position of Head of the Department of Image Processing in 1985 - 1994. His current research interests include all aspects of digital image and signal processing, particularly Fourier transform, image filters, remote sensing and geosciences.

Babak Mahdian received the M.Sc. degree in Computer Science from the University of West Bohemia, Plzen, Czech Republic, in 2004, and the Ph.D. degree in Mathematical Engineering from the Czech Technical University, Prague, Czech Republic, in 2008. He is currently with the Institute of Information Theory and Automation, Academy of Sciences of the Czech Republic, Prague. His current research interests include all aspects of digital image processing and pattern recognition, particularly digital image forensics.