OPTIMAL COUNTERFORENSICS FOR HISTOGRAM-BASED FORENSICS

Pedro Comesaña-Alfaro[*] *Fernando Pérez-González*[*]

University of Vigo - SPAIN
EE Telecomunicacion
Campus Universitario, 36310 Vigo- Spain
{pcomesan|fperez}@gts.uvigo.es

ABSTRACT

There has been a recent interest in counterforensics as an adversarial approach to forensic detectors. Most of the existing counterforensics strategies, although successful, are based on heuristic criteria, and their optimality is not proven. In this paper the optimal modification strategy of a content in order to fool a histogram-based forensics detector is derived. The proposed attack relies on the assumption of a convex cost function; special attention is paid to the Euclidean norm, obtaining the optimal attack in the MSE sense. In order to prove the usefulness of the proposed strategy, we employ it to successfully attack a well-known algorithm for detecting double JPEG compression.

Index Terms— Histogram-based forensics, multimedia forensics, optimal counterforensics strategy, transportation theory.

1. INTRODUCTION

In the last decades, due to both technological and sociocultural evolution, multimedia contents have become precious assets with implicit and explicit value that creators and owners want to preserve. Parallel to the spread and importance of multimedia contents, the number and power of editing tools that are available even to non-skilled users have also increased, thus compromising the trustability of digital assets to the extent that their use as legal evidence is being put into question.

Passive multimedia forensics has quickly evolved in the last years to face the challenging problem of assessing the processing, coding and editing steps a content has gone through. A lesson already learned in watermarking and steganography research, the emergence of forensics has naturally led to an arms race between the forensic detector designers and *adversaries*. In fact, this race epitomizes the current trend of *Adversarial Signal Processing* [1] which considers the existence of a smart adversary in the design of binary decision functions. In the case of multimedia forensics, examples of this race are sprouting in the literature. We review some relevant instances next, noticing that the list is by no means exhaustive.

Popescu and Farid [2] presented in their seminal work not just a well-known resampling detection technique, but also counterforensic attacks aiming at resampling detectors. The case of JPEG compression detection is probably one of the forensic problems that has been paid a larger attention due to its practical implications [3, 4, 5]. This has quickly given rise to counterforensic schemes such as those proposed in [6, 7], or also in [8], accepted in this conference, and where the JPEG quantization detectors proposed in [3, 7, 9] are attacked by following a variational approach that minimizes a distortion function by using a projected subgradient method. Unsurprisingly, counter counter-forensics have been also suggested, clearly reflecting the existence of a (so far, iterative) game between forensic system designers and adversaries [9].

Lukas and Fridrich [10], and then Pevny and Fridrich [11] have proposed double JPEG compression detection algorithms; the latter, to which will devote special attention in this work, was initially designed for steganography, although it is recognized as a milestone also in forensics. Later, several other double JPEG compression detection schemes have been presented, including [12, 13, 14]. Recently, counterforensic double JPEG attacks have been also proposed, such as the one due to Sutthiwan and Shi [15].

Another problem where this game was played is the Fixed Pattern Noise (FPN) [16] and Photo Response Non-Uniformity Noise (PRNU) [17] detection, where not just counterforensics [18], but counter-counterforensics have been also put forward [19].

Although these counterforensic strategies are generally successful, a common characteristic of most of them is that they are suboptimal, implying that their optimality is not proven (or even discussed) under any meaningful criterion. An additional drawback of most of them, is that they are aimed at specific forensics problems, and their extension to broader scenarios is not straightforward. A remarkable exception is the recent work by Barni *et al*. [20], where a general methodology is proposed, which is shown to be able to cope with two different problems, specifically, gamma-correction and histogram stretching.

Leveraging on [20], the objective of this work is to propose a general (non-targeted) attacking method, with the distinctive feature of a single target function whose optimization is consistently pursued in the different steps of the attack design. Specifically, we will focus our attention on the so-called histogram-based forensic detectors, that take their decisions just based on the histogram of a (generally, transform-based) function of the input samples.

The remaining of this paper is organized as follows: Sect. 2 presents the main result in this work, deriving the optimal strategy (in terms of distortion) that a smart attacker should seek. This strategy is put into practice in Sect. 3, where the double-JPEG compression detector in [11] is optimally attacked. Finally, conclusions and future work are presented in Sect. 4.

[*]Research supported by the European Union under project REWIND (Grant Agreement Number 268478), the European Regional Development Fund (ERDF) and the Spanish Government under projects DYNACS (TEC2010-21245-C02-02/TCM) and COMONSENS (CONSOLIDER-INGENIO 2010 CSD2008-00010), and the Galician Regional Government under projects "Consolidation of Research Units" 2009/62, 2010/85 and SCALLOPS (10PXIB322231PR).

2. MAIN RESULT

In this section we derive the optimal attacking strategy under certain distortion conditions.

2.1. Problem formulation

Let $\mathbf{x}$ be a vector containing the samples of a discrete signal in its original space; $\mathbf{x}$ is assumed to belong to a finite set $\mathcal{X} \subset \mathbb{R}^N$. We assume that $\mathbf{x}$ can be transformed through a function $f(\cdot)$, yielding $\mathbf{y} = f(\mathbf{x})$, which belongs to a set $\mathcal{Y}$ verifying $\mathcal{Y} \subset \mathbb{R}^N$. Furthermore, we will assume $f(\cdot)$ to be a bijection. The identity function, the full-frame DFT and the block-DCT transform are examples of this transformation.

A basic element in every forensics system is the forensic detector $\phi_x : \mathcal{X} \mapsto \{0, 1\}$, that decides between two alternative hypotheses H_0 and H_1. For instance, H_1 can be "$\mathbf{x}$ is doubly-compressed" and H_0 "$\mathbf{x}$ is not doubly-compressed". In those detectors working in the transform domain, ϕ_x is defined in terms of $\phi_y : \mathcal{Y} \mapsto \{0, 1\}$, so $\phi_x(\mathbf{x}) = \phi_y(f(\mathbf{x}))$. Given ϕ_x, the acceptance and rejection regions are defined in the original space as

$$\mathcal{R}_k^x \doteq \{\mathbf{x} \in \mathcal{X} : \phi_x(\mathbf{x}) = k\},\ k = 0, 1,$$

with a similar definition for $\mathcal{R}_k^y$, $k = 0, 1$.

We are interested in solving the following optimization problem:
Problem: Given $\mathbf{x} \in \mathcal{R}_1^x$ and a function $g^x : \mathcal{X} \times \mathcal{X} \mapsto \mathbb{R}$, solve

$$\mathbf{x}^* = \arg \min_{\mathbf{x}' \in \mathcal{R}_0^x} g^x(\mathbf{x}, \mathbf{x}'). \quad \square$$

A typical choice for g is the squared Euclidean distance, i.e., $g^x(\mathbf{x}, \mathbf{x}') = ||\mathbf{x} - \mathbf{x}'||^2$, although perceptual measures like the Structural Similarity Index (SSIM) [21] are possible.

Based on the bijective nature of f, the previous problem definition is equivalent to

$$\mathbf{y}^* = \arg \min_{\mathbf{y}' \in \mathcal{R}_0^y} g^x(f^{-1}(\mathbf{y}), f^{-1}(\mathbf{y}')),$$

where $\mathbf{y}^* = f(\mathbf{x}^*)$.

For the sake of simplicity, we will limit our discussion to the case where there exists a function $g^y : \mathcal{Y} \times \mathcal{Y} \mapsto \mathbb{R}$ such that $g^x(f^{-1}(\mathbf{y}), f^{-1}(\mathbf{y}')) = g^y(\mathbf{y}, \mathbf{y}')$. For instance, this is met when f is an orthonormal transform and g^x and g^y are Euclidean distances. Under this assumption, we can alternatively work in the transform domain, i.e.,

$$\mathbf{y}^* = \arg \min_{\mathbf{y}' \in \mathcal{R}_0^y} g^y(\mathbf{y}, \mathbf{y}'). \tag{1}$$

In this paper we are mainly interested on histogram-based detectors. We will use the cumulative histogram of $\mathbf{y}$, which is defined in terms of the boundary points between histogram bins. Specifically, if the histogram bins are delimited by the set of points $\mathcal{B} = \{b_0, b_1, \ldots, b_{n_1}\}$, where $b_0 < b_1 < \ldots < b_{n_1}$, $b_0 = -\infty$, $b_{n_1} = \infty$, we define the cumulative histogram of $\mathbf{y}$ in terms of $\mathcal{B}$ as

$$H(b_i, \mathbf{y}) = \frac{1}{N} \sum_{j=1}^{N} \mathbf{1}(y_j \leq b_i), i = 1, \ldots, n_1,$$

where $\mathbf{1}(\cdot)$ is 1 if its boolean argument is true, and 0 otherwise. The definition guarantees that $0 \leq H(b_i, \mathbf{y}) \leq 1$. For the sake of simplicity, we define $H(\mathcal{B}, \mathbf{y}) \doteq [H(b_1, \mathbf{y}), H(b_2, \mathbf{y}), \ldots, H(b_{n-1}, \mathbf{y})]$, while the set containing all the valid $H(\mathcal{B}, \mathbf{y})$ will be denoted by $\mathcal{H}$.

The inverse mapping of $H(b_i, \mathbf{y})$ is denoted by $H^{-1}(p, \mathbf{y})$, and is defined as

$$H^{-1}(p, \mathbf{y}) \doteq \arg \min_{b_i, 1 \leq i \leq n_1 : H(b_i, \mathbf{y}) \geq p} b_i.$$

Definition: For a given set of histogram bin boundary points $\mathcal{B}$, the test statistic ϕ_y is histogram-based if there exists a function $\phi_H : \mathcal{H} \mapsto \{0, 1\}$ such that $\phi_y(\mathbf{y}) = \phi_H(H(\mathcal{B}, \mathbf{y}))$ for all $\mathbf{y} \in \mathcal{Y}$. $\square$

Therefore, given $\mathcal{B}$, for a histogram-based test we can define the equivalent acceptance and rejection sets as

$$\mathcal{R}_k^H \doteq \{H(\mathcal{B}, \mathbf{y}) : \phi_H(H(\mathcal{B}, \mathbf{y})) = k\},\ k = 0, 1.$$

We introduce $g^H : \mathcal{H} \times \mathcal{H} \mapsto \mathbb{R}$ to quantify the similarity between histograms:

$$g^H(H(\mathcal{B}, \mathbf{y}), H(\mathcal{B}, \mathbf{y}')) \doteq \min_{\mathbf{y}'' : H(\mathcal{B}, \mathbf{y}'') = H(\mathcal{B}, \mathbf{y}')} g^y(\mathbf{y}, \mathbf{y}''). \tag{2}$$

We can state now the main result in this paper
Lemma: The solution to (1) is equivalent to

$$H^\sharp(\mathcal{B}, \mathbf{y}^\sharp) = \arg \min_{H'(\mathcal{B}, \mathbf{y}') \in \mathcal{R}_0^H} g^H(H(\mathcal{B}, \mathbf{y}), H'(\mathcal{B}, \mathbf{y}')), \tag{3}$$

$$\mathbf{y}^* = \arg \min_{\mathbf{y}' : H(\mathcal{B}, \mathbf{y}') = H^\sharp(\mathcal{B}, \mathbf{y}^\sharp)} g^y(\mathbf{y}, \mathbf{y}'). \quad \square \tag{4}$$

The procedure comprised by the three optimization steps in Eqs. (2-4), can be justified in terms of *optimal transportation theory* [22]. It is also reminiscent of the strategy recently proposed for the counterforensics problem by Barni *et al*. [20], which will be discussed in detail in Sect. 2.4. At this point we remark that our work differs from [20] in the strategy of constructing both g^y and g^H directly from g^x in order to find the attack that optimizes the target in the original domain.

2.2. A relevant particular case

For the case where g^y is component-wise additive and dependent on the difference between the input vectors, i.e., $g^y(\mathbf{y}, \mathbf{y}') = \sum_{i=1}^N g^{y_i}(y_i - y_i')$, each g^{y_i} is convex, and $\mathcal{B} = \mathcal{Y}$, we can write

$$y_i = H^{-1}(H(y_i, \mathbf{y}), \mathbf{y}),$$

and it can be shown that

$$g^H(H(\mathcal{B}, \mathbf{y}), H(\mathcal{B}, \mathbf{y}')) = \sum_{j=1}^N g\left[H^{-1}\left(\tfrac{j}{N}, \mathbf{y}\right) - H^{-1}\left(\tfrac{j}{N}, \mathbf{y}'\right)\right]. \tag{5}$$

This result can be seen as the discrete counterpart of optimal transportation on the real line [22], where instead of the distribution function we use the cumulative histogram. In fact, (5) also provides directions on how to modify $\mathbf{y}$ into a signal with histogram $H^\sharp(\mathcal{B}, y^\sharp)$, i.e., to solve (4). Specifically, if we denote by π an ordering permutation of $\mathbf{y}$, i.e., $y_{\pi_0} \leq y_{\pi_1} \leq \ldots y_{\pi_N}$, and by τ a similarly defined ordering of $\mathbf{y}^\sharp$, then the optimal modification algorithm is nothing but

$$y_{\pi_i}^* = y_{\tau_i}^\sharp, \quad i = 1, \ldots, N. \tag{6}$$

Note that ties in the ordering of $\mathbf{y}$ and $\mathbf{y}^\sharp$ can be arbitrarily reordered without affecting the value of the target function. Then, for the particular case in this section, the original problem involving the three optimizations in (2), (3), and (4), only requires one numerical optimization, i.e. (3).

2.3. Example

Next, we illustrate how the general approach outlined in the previous sections can be applied to a well-known practical scenario. We focus now on the case of JPEG-compressed images, with DCT histogram-based detection and PSNR as distortion measure. In such framework $\mathbf{x}$ would be the pixels, $\mathbf{y}$ their block-DCT transformed coefficients, and g^x and g^y the Euclidean norm.

The result given in the last section indicates that in order to move an image $\mathbf{x} \in R_1^x$ to R_0^x with a minimum MSE (or equivalently, maximum PSNR), one should seek the histogram $H^\sharp(\mathcal{B}, \mathbf{y}^\sharp)$ defined according to (3), which in this case is simply

$$g^H(H(\mathcal{B}, \mathbf{y}), H(\mathcal{B}, \mathbf{y}')) = \sum_{j=1}^{N} \left[H^{-1}\left(\tfrac{j}{N}, \mathbf{y}\right) - H^{-1}\left(\tfrac{j}{N}, \mathbf{y}'\right)\right]^2.$$

Once $\mathbf{y}^\sharp$ is found, the optimal modification in the block-DCT coefficient domain of the original image $\mathbf{y}$ is implemented as (6). Again, it is important to note that just one numerical optimization, the computation of $H^\sharp(\mathcal{B}, \mathbf{y}^\sharp)$, is involved in this approach.

Even though it could be argued that the PSNR used in this section lacks perceptual significance, it is important to emphasize that due to the form of the solution in (6), the attack will not focus on specific regions of the image, but will be evenly spread over all the involved DCT coefficients. In fact, the degrees of freedom granted by the ties in (6), which do not affect the PSNR, can also be exploited to reduce the perceptual distortion while keeping the PSNR. In any case, we note that other distortion measures as the SSIM do fit in the general framework provided in Sect. 2.1, which means that they can be addressed by resorting to the three-stage optimization given by Eqs. (2-4).

2.4. Comparison with previous art

A result quite similar to the particular case discussed in the last section was reported by Eggers *et al*. in [23], where it was applied to the minimum Euclidean distortion histogram mapping problem in steganography.

In the forensics field, Barni *et al*. has very recently proposed in [20] a counterforensics technique which is similar to our approach. However, in Barni et al.'s work different target functions are used in the three solution stages (specifically, chi-square, information divergence and SSIM), instead of a unique target throughout the entire procedure, as it occurs in our case. We remark that both g^y and g^H directly derive from g^x. This allows us, for instance, to determine the value of the manipulation distortion in the original domain as a simple function of the original and the target distorted histograms.

Therefore, the 3-step optimization in [20] is reduced here to a one-step optimization (the equivalent to histogram retrieval in Barni et al.'s work, i.e., the determination of $H^\sharp(\mathcal{B}, \mathbf{y}^\sharp)$). Once such cumulative histogram is obtained, we give a closed, as opposed to iterative or numerical, procedure to compute the signal in the original domain that produces the required histogram with minimal distortion. In this way, the iterative procedures used in [20] are avoided, with a consequent reduction of the computational cost.

Another significant difference with [20] is that no specific forensic detector is used therein; instead the smart attacker tries to find the mapping strategy that minimizes the Kullback-Leibler divergence (KLD) between the histograms of the modified and original signals; the rationale behind this strategy is that the KLD measures the distinguishability between distributions. However, when the attacker is aware of the particular detector being used (a reasonable assumption from Kerckhoff's principle), then it is possible to devise an optimal attack that takes advantage of such knowledge, as we will illustrate in the next Section.

3. EXPERIMENTAL RESULTS

In order to show the validity of our strategy, we focus on the framework described in Sect. 2.3. The used forensic detector is the double-JPEG compression detector proposed in [11], and the considered database is UCIDv2 [24]. Following Kerckhoff's principle, we assume that the detector is perfectly known by the adversary.

The scheme proposed in [11] considers $9\,8\times 8$-block DCT coefficients, and computes for each of them its 16-bin histogram, where each bin is centered at the integer multipliers of the quantization step. These histograms are fed to a SVM with Gaussian kernel. To train and test the Support Vector Machine (SVM) used in [11], and determine the SVM parameters C and γ, 380 images were randomly chosen for the training and 380 for testing. Each of those images was doubly JPEG-compressed, with Quality Factor (QF) of the first compression all the values in $\{0, 10, 20, \ldots, 100\}$, while the second quality factor was fixed to 70, i.e., the SVM was trained for a specific QF, as proposed in [11]. Additionally, all the images were also compressed just once with QF$=70$, in order to provide the second training class to the SVM; consequently, the two classes fed to the SVM for training (and similarly those used for testing) had 4180 and 380 images, respectively.

Parameters C and γ were chosen following the strategy proposed in [11]; namely, they were sampled in a logarithmic domain, and then exhaustive search was performed. The criterion used for selecting the values was the maximization of the well-known Area Under Curve, which resulted in $C = 2^3$ and $\gamma = 2^{-5}$. Once the SVM has been fixed, we had to decide the detection threshold the SVM soft output will be compared to; in this case we tried to obtain approximately the same value for both probabilities of error (i.e., false negative, P_{fn}, and false positive, P_{fp}, that is, the probabilities of respectively deciding that the image was compressed once, when it was actually compressed twice, and viceversa), obtaining $P_{fn} = 0.1557$ and $P_{fp} = 0.1478$ for a threshold equal to -0.1574. Furthermore, due to the possible rounding effects in the histogram probabilities related to the use of a finite number of DCT coefficients, a tolerance of 0.02 was added, so the optimization process considered a conservative value for the threshold of -0.1774.

In order to test the performance of the proposed attacking strategy, a challenging situation was chosen: the attacker would try to modify doubly JPEG-compressed images with a first QF as small as 10, and a second QF$=70$, while fooling the detector to decide that the resulting image was only once compressed. This should be achieved maximizing the PSNR between the original doubly-compressed and the attacked versions of each image.

To avoid the possible bias in the results due to reusing images from the training and test sets, we decided to use a fresh set of 380 images in the performance evaluation. One of those images was JPEG-compressed only once with QF$=70$, while the others were compressed twice: first with QF$=10$ and then with QF$=70$. The once-compressed image was used to move the input image to the boundary of the detection region, and then start an optimization algorithm.

The PSNR achieved by averaging the MSE is 35.78 dB, while the minimum PSNR for a single image is 30.93 dB, and the maximum 40.21 dB. It is important to note that the SVM soft outputs actually lie around the desired value (i.e., -0.1774), with empirical mean -0.1741 and variance $1.1 \cdot 10^{-4}$. This variability is due to the

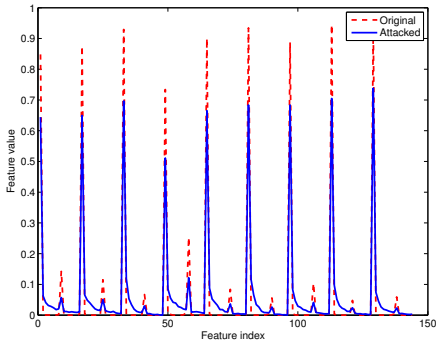

Fig. 1. Histogram of an original image and its optimally attacked version.

use of real-valued (instead of discrete-valued) optimization, which causes the probabilities assigned by the optimization algorithm not to be achievable in practice. In fact, 20 out of the 379 images would be still detected as doubly compressed. However, this problem would be easily solved by considering a larger tolerance value, or introducing a postprocessing stage where these rounding effects could be smoothed. We have implemented the second strategy, by slightly modifying the target histogram for those images where the double compression is still detected. Specifically, instead of modifying the original histogram by the difference with respect to the target one, the applied modification is a scaled version of that difference; if a scaling factor of just 1.01 is applied, then all the images are classified as singly compressed. All the PSNRs computed from the average MSE, the maximum PSNR and the minimum one keep the values presented above for the given precision (i.e., ± 0.01 dB).

For the sake of illustration, Fig. 1 shows the histogram of an original signal and its attacked counterpart. It is worth to point out that the proposed scheme tries to fill the gaps left by the first quantization. Nevertheless, contrarily to typical noise-addition strategies, in this case the noise is optimally designed to fool the detector and simultaneously achieve the maximum PSNR with respect to the original.

As a comparison, we have tested the attack proposed in [15], which is specifically designed for fooling doubly-JPEG compression detectors, in the same experimental framework. As described in [15], we used the bilinear interpolation, although the shrink-zoom parameter was reduced to 0.5 in order to increase the effect of the attack. The PSNR obtained by averaging the MSE is 26.51 dB, that is, more than 9 dB worse than ours, although only 50.4% of the images have been classified as non-doubly compressed (94.7% in our case).

4. CONCLUSIONS AND FUTURE WORK

We have proposed an optimal counterforensic strategy for histogram-based detectors; this strategy considers a fixed distortion which is consistently used throughout the derivation of the method. Interestingly, for some transform and distortion functions of practical value, the proposed method reduces to a single optimization, with a significant reduction in computational cost.

We remark that the (minimum) attacking distortion obtained in this way could be used as a measure of the robustness of a given forensic scheme against smart adversaries. This would complement the usual robustness measures, as the ROC, that do not consider the possibility of smart adversaries.

Among the future lines, we plan to use our methodology to attack other histogram-based detectors. Furthermore, as the PSNR is known to be an inadequate distortion measure in perceptual terms, we will address the use of other measures as the SSIM. In this sense, as the SSIM is non-convex, it would be worth deriving a convex proxy that could speed-up the optimization here proposed.

5. REFERENCES

[1] Mauro Barni and Fernando Pérez-González, "Coping with the enemy: Advances in adversary-aware signal processing," in *Accepted IEEE ICASSP*, Vancouver, Canada, May 2013.

[2] Alin C. Popescu and Hany Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp. 758–767, February 2005.

[3] Zhigang Fan and Ricardo L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Transactions on Image Processing*, vol. 12, no. 2, pp. 230–235, February 2003.

[4] W. Sabrina Lin, Steven K. Tjoa, H. Vicky Zhao, and K. J. Ray Liu, "Digital image source coder forensics via intrinsic fingerprints," *IEEE Transactions on Informations Forensics and Security*, vol. 4, no. 3, pp. 460–475, September 2009.

[5] Weiqi Luo, Yuangen Wang, and Jiwu Huang, "Detection of quantization artifacts and its applications to transform encoder identification," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 810–815, December 2010.

[6] Matthew C. Stamn, Steven K. Tjoa, W. Sabrina Lin, and K. J. Ray Liu, "Anti-forensics of jpeg compression," in *Proc. IEEE ICASSP*, Dallas, TX, March 2010, pp. 1694–1697.

[7] Giuseppe Valenzise, Marco Tagliasacchi, and Stefano Tubaro, "The cost of jpeg compression anti-forensics," in *Proc. IEEE ICASSP*, Prague, Czech Republic, May 2011, pp. 1884–1887.

[8] Wei Fan, Kai Wang, François Cayre, and Zhang Xiong, "A variational approach to jpeg anti-forensics," in *Accepted IEEE ICASSP*, Vancouver, Canada, May 2013.

[9] Shi Yue Lai and Rainer Bohme, "Countering counter-forensics: the case of jpeg compression," in *Lectures Notes in Computer Science. Proc. of the 13th international conference on Information Hiding*, Prague, Czech Republic, May 2011, vol. 6958, pp. 285–298, Springer.

[10] Jan Lukas and Jessica Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. of DFRWS*, 2003.

[11] Tomas Pevny and Jessica Fridrich, "Detection of double-compression in jpeg images for applications in steganography," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 2, pp. 247–258, June 2008.

[12] Weiqi Luo, Zhenhua Qu, Jiwu Huang, and Guoping Qiu, "A novel method for detecting cropped and recompressed image block," in *Proc. IEEE ICASSP*, Honolulu, HI, April 2007, pp. 217–220.

[13] Fangjun Huang, Jiwu Huang, and Yun Qing Shi, "Detecting double jpeg compression with the same quantization matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 848–856, December 2010.

[14] Tiziano Bianchi and Alessandro Piva, "Detection of non-aligned double jpeg compression based on integer periodicity maps," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 842–848, April 2012.

[15] Patchara Sutthiwan and Yun Q. Shi, "Anti-forensics of double jpeg compression detection," in *Lectures Notes in Computer Science. Proc. of the International Workshop on Digital-Forensics and Watermarking*, Atlantic City, NJ, October 2011, vol. 7128, pp. 411–424, Springer.

[16] Jan Lukas, Jessica Fridrich, and Miroslav Goljan, "Digital camera identification from sensor patter noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, June 2006.

[17] Mo Chen, Jessica Fridrich, Miroslav Goljan, and Jan Lukas, "Determining image origin and integrity using sensor noise," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 74–90, March 2008.

[18] Thomas Gloe, Matthias Kirchner, Antje Winkler, and Rainer Bohme, "Can we trust digital image forensics?," in *Proc. of the 15th International Conference on Multimedia*, Augsburg, Germany, 2007, pp. 78–86.

[19] Miroslav Goljan, Jessica Fridrich, and Mo Chen, "Sensor noise camera identification: Countering counter-forensics," in *Proc. of SPIE Media Forensics and Security*, 2010, vol. 7541.

[20] Mauro Barni, Marco Fontani, and Benedetta Tondi, "A universal technique to hide traces of histogram-based image manipulations," in *Proc. of ACM Workshop on Multimedia and Security*, Coventry, UK, September 2012, pp. 97–104.

[21] Zhou Wang, Alan C. Bovik, Hamid R. Sheikh, and Eero P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, April 2004.

[22] Svetlozar T. Rachev and Ludger Ruschendorf, *Mass Transportation Problems*, Springer, 1998.

[23] Joachim J. Eggers, Robert Bauml, and Bernd Girod, "A communicaitons approach to image steganography," in *Proc. of SPIE. Security and Watermarking of Multimedia Contents 2002*, San Jose, CA, January 2002, vol. 4675, pp. 26–37.

[24] Gerald Schaefer and Michal Stich, ""UCID - An Uncompressed Colour Image Database"," in *Proc. of SPIE. Storage and Retrieval Methods and Applications for Multimedia 2004*, San Jose, CA, CA, vol. 5307, pp. 472–480.