# CONCEALABILITY-RATE-DISTORTION TRADEOFF IN IMAGE COMPRESSION ANTI-FORENSICS

*Xiaoyu Chu, Matthew C. Stamm, Yan Chen and K. J. Ray Liu*

Dept. of Electrical and Computer Engineering, University of Maryland, College Park

## ABSTRACT

Due to the ease with which digital multimedia content can be modified, a number of techniques to forensically detect forgeries have been developed. Meanwhile, anti-forensic operations have been developed to defeat forensic techniques. When anti-forensics is applied, a forger must balance between the amount that editing fingerprints have been concealed and the distortion introduced to the content. Additionally, the forger may compress the forgery for storage or transmission, which introduces a tradeoff between data rate and distortion. In this paper, we define a measure of an anti-forensic technique's effectiveness which we call concealability and examine the tradeoff between concealability, rate, and distortion. We then characterize the concealability-rate-distortion (C-R-D) surface for double JPEG compression anti-forensics. To do this, we propose a new technique known as flexible anti-forensic dither to hide double JPEG fingerprints. From our experiments, we identify two surprising results related to the C-R-D surface.

***Index Terms***— Digital Forensics, Anti-Forensics, JPEG compression, Concealability, Rate and Distortion.

## 1. INTRODUCTION

Digital editing software can easily be used to create forgeries from digital multimedia content. Because of this, the authenticity of digital multimedia content must often be verified before it can be trusted. As a result, researchers have developed several forensic techniques to detect various types of forgeries [1–4] and identify a multimedia signal's acquisition history [5–7]. One set of particularly important image forensic techniques are those that deal with an image's compression history [8–12].

By contrarst, an intelligent forger can create anti-forensic techniques to prevent their forgeries from being detected. Several anti-forensic techniques have been developed to hide traces of JPEG compression [13], eliminate evidence of frame deletion in digital videos [14], conceal image resizing [15], and falsify an image's photo response non-uniformity fingerprint [16]. It is critical to study anti-forensics in order to understand the set of actions that an intelligent forger will likely take.

When applying anti-forensics, a forger must balance a tradeoff between how likely their forgery will be concealed and the distortion introduced into their forgery by anti-forensics. Since most multimedia signals are compressed for storage or transmission, the forger will likely apply compression to their forgery. During compression, it is well known that a tradeoff between the data rate and the distortion introduced into the signal must be balanced. Therefore, in the case of compressing a forgery in which anti-forensics is used, the rate, distortion, and probability that the forgery is concealed are all related. A forger must balance a tradeoff between all three of these quantities.

This tradeoff naturally occurs in the case of double JPEG compression. Since most images are compressed as JPEGs during storage or transmission, a forger will likely create their forgery from JPEG images. Similarly, the forgery will also likely to be compressed as the same JPEG format. As a result, double JPEG compression fingerprints will likely be left in the forged image. Since many techniques exist to identify forgeries by detecting double compression [9–12, 17–22], a forger must use anti-forensic techniques to modify the DCT coefficients of an image. This will introduce distortion into the image [23]. Similarly, JPEG compression operates by quantizing these DCT coefficients, which also introduces distortion. To ensure that the total distortion does not rise above a certain level, the forger must balance the amount of distortion introduced by JPEG compression and anti-forensics. Adjusting the strength of anti-forensics and JPEG compression will lead to changes in the likelihood that the forgery is concealed and the data rate respectively.

In this paper, we define the concept of the concealability of a forgery and propose a framework to study the tradeoff between rate, distortion, and concealability. We evaluate this tradeoff in the case of double JPEG compression anti-forensics. Specifically, we first propose a technique to adjust the strength of JPEG compression anti-forensics by adding *flexible anti-forensic dither* to an image's DCT coefficients. We then experimentally determine the Concealability-Rate-Distortion surface for anti-forensic JPEG double compression. By analyzing this surface, we find two surprising results. One is that under certain conditions, using a lower secondary quality factor is always better than using a higher one, because the former can achieve much lower rate without increasing distortion or decreasing concealability. The other is that in certain conditions, increasing the anti-forensic strength will decrease the data rate.

## 2. JPEG COMPRESSION FORENSICS OVERVIEW

JPEG is the most widely used lossy image compression format. When an image is JPEG compressed, it is first segmented into blocks, then the discrete cosine transform (DCT) of each block is computed. The resulting DCT coefficients are quantized using a quantization table that specifies the quantization stepsize for each DCT subband. Finally, the sequence of quantized DCT coefficients are entropy coded. As a result of quantization, the DCT coefficients of a JPEG compressed image will take values that are integer multiples of the quantization stepsize. This is a well known fingerprint of JPEG compression and can be detected by examining the histogram of each subband of DCT coefficients [24].

If an image is JPEG compressed a second time using a different quantization table, a new set of double JPEG compression fingerprints occur. The mismatch between the quantization stepsizes causes an unequal number (even none) of quantized DCT coeffi-

Email: {cxygrace,mcstamm,yan,kjrliu}@umd.edu.

978-1-4799-0356-6/13/$31.00 ©2013 IEEE

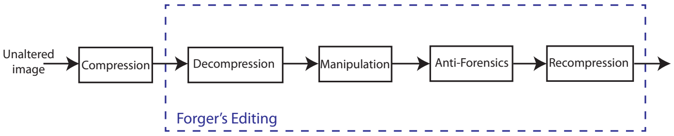


**Fig. 1**. A typical process for a forger's editing, where anti-forensics and recompression are the two controllable processes for the forger to set up.

cients in the first compression be mapped into each quantized value during the second compression. Moreover, this number changes periodically. As a result, periodic peaks or zeros will occur in the histogram of a double JPEG compressed image's DCT coefficients [9]. Because double JPEG compression fingerprints arise in many forgeries, several techniques have been created to detect double JPEG compression. One of the most successful techniques is the one proposed by Pevny and Fridrich [10]. This technique operates by taking the histogram values on the quantized bins of the lowfrequency subband coefficients as a feature vector. These features are used to train a support vector machine (SVM) to classify an image as double or single compressed.

In order to erase fingerprints from JPEG compression, Stamm and Liu proposed an anti-forensic technique to fully cover the quantization trace from JPEG compression [13]. Specifically, this technique modifies the DCT coefficients by adding an anti-forensic dither on each quantized coefficient, in order to remove the quantization effect in the histogram. After this technique has been applied, the distribution of the anti-forensically modified images DCT coefficients will match their distribution before compression JPEG. If the anti-forensically modified image is subsequently JPEG compressed, it will not contain double JPEG compression fingerprints. Instead, it will only appear to have been compressed once.

## 3. CONCEALABILITY-RATE-DISTORTION TRADEOFF

When a forgery is created from a JPEG compressed image, the image typically undergoes the processing shown in Fig. 1. First, the forger must decompress the image so that it can be edited. Next, the forger manipulates the image to create their forgery. In most scenarios, the forger will wish to recompress the manipulated image so that it can be more easily stored or transmitted. Since recompression will introduce double JPEG compression fingerprints, the forger will apply JPEG anti-forensics to hide their forgery [13]. Finally, the forger will recompress their forgery using a quality factor of their choice. For the purposes of this paper, we only consider the effects of recompression and JPEG anti-forensics.

Intuitively for anti-forensics, the forger must balance between the amount that double compression fingerprints are concealed and the distortion introduced by anti-forensics modification. When performing recompression, there is a well-known tradeoff between rate and distortion. In addition, Since anti-forensics alters the distribution of the DCT coefficients, it is possible for anti-forensics to affect the rate. On the other hand, the performance of double JPEG detection techniques depends on the relationship between the primary and secondary quality factors. As a result, the secondary quality factor affects the probability that the forgery will be detected in addition to the rate. From this, we can see that rate, distortion, and the probability that a forgery will be concealed are all related.

In order to characterize the tradeoff, we first define the term *concealability* as the quantity to measure the amount that the fingerprint has been concealed. Let $I$ denote the JPEG image obtained by the forger. We use the function $m(\cdot)$ to denote the modifications performed by the forger consisting of anti-forensics and recompression.

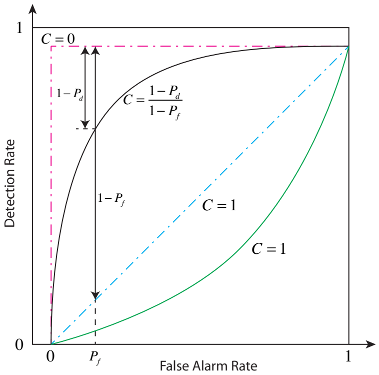


**Fig. 2**. Examples of concealabilities calculated from ROC curves.

Therefore, $m(I)$ is the anti-forensically modified and double compressed image. When the output image is examined by a forensic analyst, a hypothesis test is used where $H_0$ denotes that the image is single compressed and $H_1$ denotes that it is double compressed. A receiver operating characteristic (ROC) curve can be obtained by applying different decision thresholds and calculating the false alarm rates and detection rates. For a certain false alarm rate $P_f$, a corresponding decision rule $\delta_{P_f}(\cdot)$ is selected.

When anti-forensics applied, it will decrease the detection rate. However, as long as the detection rate is low enough so that it equals to $P_f$, the detection will perform like a random decision scenario with equal detection rate and false alarm rate. In this case, the anti-forensics has fully covered the fingerprint. Any further attempt to decrease the detection rate is unnecessary. In order to evaluate the extent of how close the forger has degenerated the forensic detector performance to random decision scenario, we define concealability as follows: For a certain false alarm rate $P_f$, and a modification function $m(\cdot)$ chosen by the forger, the concealability of the output image is

$$C(m, P_f) = \min\left(\frac{1-\mathbb{P}\Big(\delta_{P_f}\big(m(I)\big)=H_1\Big)}{1-P_f}, 1\right). \qquad (1)$$

An illustration of how to calculate concealability from a ROC curve is shown in Fig. 2.

To measure the distortion on the image introduced by the forger's editing, we take use of the quality assessment: mean structural similarity (MSSIM) [25], which is designed based on the human eye perception. Since distortion is inverse proportional to similarity, we give our distortion quantity as

$$D(m) = 1 - \text{MSSIM}\big(I, m(I)\big). \qquad (2)$$

Lastly, to measure the compression rate, we use the bitrate of the output sequence $m(I)$ as the rate quantity:

$$R(m) = \frac{\text{JPEG file size of } m(I)}{\text{number of pixels in } m(I)}. \qquad (3)$$

## 4. FLEXIBLE ANTI-FORENSIC DITHER

When creating a forgery, the forger must balance the tradeoff between concealability, rate, and distortion. To do this the forger can adjust the quality factor used when recompressing the image. Additionally, the forger would like to adjust the strength with which they apply anti-forensics. In its original form, the strength of anti-forensic dither is not variable [13]. To compensate for this, we propose a new technique using *flexible anti-forensic dither* to allow the forger to adjust the anti-forensic strength.

In order to show our flexible anti-forensic dither, which is added on DCT coefficients, we examine the procedures that DCT coefficients have gone through during the processing. We assume that a DCT coefficient $X$ in a particular DCT subband is distributed according to the Laplace distribution [26]

$$f(x, \lambda) = \frac{1}{2\lambda} e^{-\lambda/2}. \tag{4}$$

After the image undergoes its first compression, the value of the corresponding DCT coefficient $Y$ is given by

$$Y = q_1 \operatorname{round}(X/q_1). \tag{5}$$

Specifically, it obeys a quantized Laplace distribution with quantization stepsize $q_1$ [13].

Next, anti-forensics is applied. We modify each DCT coefficient in the compressed image by adding flexible anti-forensic dither $D_\alpha$ to it, where $\alpha \in [0, 1]$ denotes the anti-forensic strength. Thus, the anti-forensically modified coefficient is

$$Z = Y + D_\alpha. \tag{6}$$

When this coefficient is quantized again with another stepsize $q_2$ in the recompression process, the coefficient of the output image $m(I)$, denoted by $W$, is

$$W = q_2 \operatorname{round}(Z/q_2). \tag{7}$$

If no anti-forensics is applied, the distribution of $W$ will be far from a quantized Laplace distribution, but with periodic peaks or zeros on its quantized bins. By measuring the distance from the histogram of $W$ to a quantized Laplace distribution, the detector can identify double JPEG compression fingerprints.

Our flexible anti-forensic dither is designed in such way that when full strength is applied, i.e., $\alpha = 1$, the distribution of $W$ will be the same as a quantized Laplace distribution with quantization stepsize $q_2$. This is done by adding $D_1$ to $Y$ so that the distribution of $Z$ matches that of $X$ [13]. Specifically, in [13], the anti-forensic dither is constructed as follows: first, a maximum likelihood estimate of the parameter $\hat{\lambda}$ in (4) is calculated from the quantized DCT coefficient $Y$ [27]. Then, for a certain coefficient value $kq_1$ of $Y$, the conditioned distribution of $D_1$ is obtained by normalizing the partial distribution function $f(x, \hat{\lambda})$ on support $\big[(k-1/2)q_1, (k+1/2)q_1\big)$ and then centering it at $kq_1$.

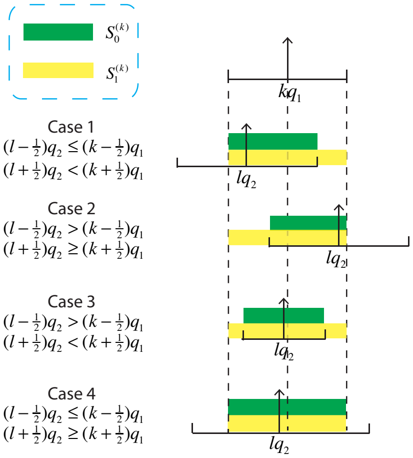
For $\alpha < 1$, we vary the strength of the anti-forensics by changing the support where the partial distribution is taken from and then do the similar normalizing and centralizing process. Let $S_\alpha^{(k)}$ denote the support for coefficient $kq_1$ under anti-forensic strength $\alpha$ . Then, from previous discussion, we have

$$S_1^{(k)} = \big[(k - 1/2)q_1, (k + 1/2)q_1\big). \tag{8}$$

When $\alpha = 0$, it is the case where no effect of anti-forensics will occur in DCT coefficients of the output image. However, it is not appropriate to assign $S_0^{(k)} = \emptyset$ because of the recompression. Instead, there exists a small region around $kq_1$ such that any deviation introduced by adding the flexible dither will vanish after the second quantization. Thus, we take $S_0^{(k)}$ as the maximum support included by $S_1^{(k)}$ such that no effect of anti-forensics will occur after recompression.

$$S_0^{(k)} = \Big[\max\big((k-\tfrac{1}{2})q_1, (l-\tfrac{1}{2})q_2\big), \min\big((k+\tfrac{1}{2})q_1, (l+\tfrac{1}{2})q_2\big)\Big), \tag{9}$$

where $l = \operatorname{round}(kq_1/q_2)$, is the index of the quantized bins in $W$ which $kq_1$ will be mapped into. An illustration of how to find $S_1^{(k)}$ and $S_0^{(k)}$ is shown in Fig. 3.



$S_0^{(k)}$
$S_1^{(k)}$
$kq_1$
Case 1
$(l-\frac{1}{2})q_2 \le (k-\frac{1}{2})q_1$
$(l+\frac{1}{2})q_2 < (k+\frac{1}{2})q_1$
$lq_2$
Case 2
$(l-\frac{1}{2})q_2 > (k-\frac{1}{2})q_1$
$(l+\frac{1}{2})q_2 \ge (k+\frac{1}{2})q_1$
$lq_2$
Case 3
$(l-\frac{1}{2})q_2 > (k-\frac{1}{2})q_1$
$(l+\frac{1}{2})q_2 < (k+\frac{1}{2})q_1$
$lq_2$
Case 4
$(l-\frac{1}{2})q_2 \le (k-\frac{1}{2})q_1$
$(l+\frac{1}{2})q_2 \ge (k+\frac{1}{2})q_1$
$lq_2$

**Fig. 3**. An illustration of how to determine $S_1^{(k)}$ and $S_0^{(k)}$ for a certain coefficient $kq_1$ in $Y$. The first row presents the coefficient value $kq_1$ we examine and its quantization interval in the first compression. The following four rows show $S_1^{(k)}$ and $S_0^{(k)}$ for four cases regarding the location of the coefficient $lq_2$ in $W$ and its quantization interval in the second compression.

Given the support for boundary values $\alpha = 0$ and $\alpha = 1$, we obtain the support for anti-forensic strength located within this range by interpolating between $S_0^{(k)}$ and $S_1^{(k)}$. Thus,

$$S_\alpha^{(k)} = (1 - \alpha)S_0^{(k)} + \alpha S_1^{(k)}. \tag{10}$$

Note that all operations on support $S_\alpha^{(k)}$ is element-wise, i.e., the lower bound and the higher bound of the support are calculated separated with the operations.

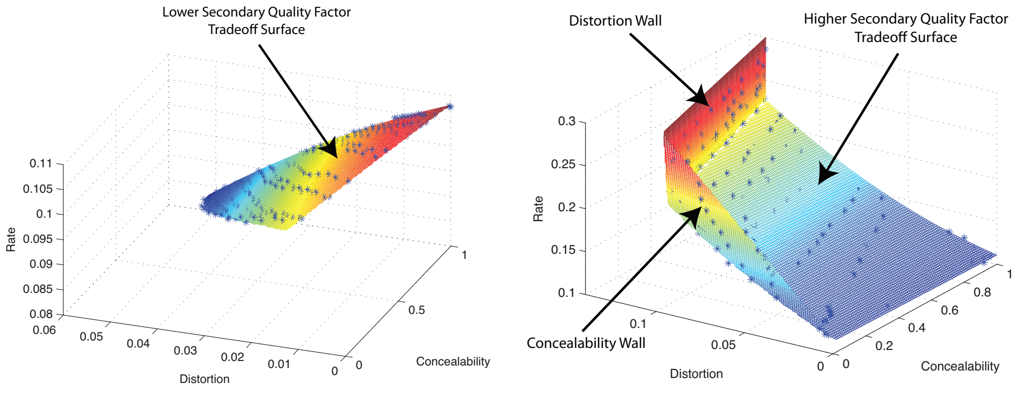
Given the support $S_\alpha^{(k)}$ for coefficient $kq_1$ and anti-forensic strength $\alpha$, we obtain the conditioned distribution of the flexible anti-forensic dither $D_\alpha$ by first normalizing the partial estimated distribution function $f(x, \hat{\lambda})$ on $S_\alpha^{(k)}$ and then centering this bounded distribution function at value $kq_1$. Formally,

$$\mathbb{P}(D_\alpha = d | Y = kq_1) = \frac{f(kq_1 + d, \hat{\lambda})}{\int_{S_\alpha^{(k)}} f(x, \hat{\lambda})dx} \mathbb{1}\big(kq_1 + d \in S_\alpha^{(k)}\big), \tag{11}$$

where $\mathbb{1}(\cdot)$ denotes the indicator function.

## 5. SIMULATION RESULTS AND ANALYSIS

In order to characterize the tradeoff of concealability-distortion-rate of image compression anti-forensics. We take 1300 unaltered images from UCID database [28] to do the simulation. We take the forensic technique in [10] to detect double JPEG compression fingerprints, where 1000 images are used for training the support vector machine and the other 300 images are for testing. To generate compressed images, we use the standard JPEG reference quantization table [11] with different quality factors. For the first compression, we fix the quality factor $Q_1 = 75$. We vary the second quality factor $Q_2$ in recompression from 60 to 90. For a certain $Q_2$, we build up the training database with 1000 single compressed images using compression quality factor $Q_2$ and 1000 double compressed images using quality factor $Q_1$ followed by $Q_2$. Furthermore, for a certain anti-forensic strength $\alpha \in [0, 1]$, we build up the test database with 300 single compressed images using quality factor $Q_2$ and 300 double compressed but been anti-forensically modified images using quality factor $Q_1$ followed by $Q_2$ and anti-forensic strength $\alpha$. In order to calculate the concealability, we take a uniform $P_f = 0.05$. Then



(a)

(b)

**Fig. 4**. Concealability-Distortion-Rate tradeoff points in 3-D plot and the fitting surfaces when (a) $Q_2 \leq Q_1$ and (b) $Q_2 > Q_1$.

for each $Q_2$, the hyperplane used to classify each test database is obtained by parallel moving the originally trained hyperplane so that if no anti-forensics is applied, we can obtain $P_f = 0.05$. Distortion and rate is calculated as the mean value from the test database.

With the variation on $Q_2$ and $\alpha$, we plot the obtained (C,R,D) points in two 3-D plots in Fig. 4, separated by whether $Q_2$ is lower or higher than $Q_1$. We characterize the tradeoff when the secondary quality factor is lower than the first one using the following polynomial surface

$$\begin{aligned} R &= 0.1018 + 0.0088C - 0.238D \\ &\quad -0.0025C^2 - 0.1037CD - 2.771D^2, \end{aligned} \tag{12}$$

which is shown in Fig. 4 (a). We can see that with a fixed concealability, rate decreases under a higher distortion constraint, which matches the R-D tradeoff. Note that our rate is defined as the bitrate of the output image, which is inversely proportional to the conventional defined compression rate.

When the secondary quality factor is higher than the primary quality factor, the C-R-D surface is more complex, as can be seen in Fig. 4 (b), we first examine the central region which has the largest area. It characterizes the tradeoff of concealability-rate-distortion. In this region, for a certain concealablity, rate actually increases with distortion, which contradicts to the conventional R-D tradeoff. This is because for higher secondary quality factors, in order to modify a double compressed image to single compressed one, the distortion introduced by anti-forensics is much higher than it needs for lower secondary quality factors. In addition, the distortion from recompression is very small and has much less effect on the total distortion. As a result, under this case, the region with both high distortion and high rate will be rarely considered. The tradeoff for the higher secondary quality factor scenario can be characterized using a polynomial surface

$$R = 0.1146 - 0.0038C + 0.5474D - 0.15CD + 3.738D^2. \tag{13}$$

Besides this region, we observe two walls on the boundary of the surface. One is at very low concealability, where further decrease concealability will result in a much larger rate. We call it the *concealability wall*, which can be expressed with surface

$$R = 0.1378 - 2.0084C + 2.9504D. \tag{14}$$

The other is at very high distortion, where a small change in distortion will lead to a dramatic increase on rate. We call this the *distortion wall*, and it can be characterized as a surface

$$R = 39.7255 + 118.4314C - 392.1569D. \tag{15}$$

Additionally from the experiment we performed, we find two surprising phenomena. The first one we find is that the forger is actually incentive to use a lower secondary quality factor rather than a higher one. This preference is due to the fact that the former can provide much lower rate without increasing distortion or decreasing concealability. This phenomenon occurs because that the rate is mainly controlled by recompression for both scenarios, but the distortion is much more affected by anti-forensics for higher secondary quality factor scenario. Traditionally, we would expect to sacrifice rate by choosing a higher secondary quality factor in order to decrease distortion. In an anti-forensic system, the introduction of anti-forensics will eliminate the benefit obtained on distortion from recompression and even reverse it to a worse result.

The second surprising phenomenon we find is that for lower secondary quality factors, when anti-forensic strength is applied on the image, the rate of the output image will actually decrease. This is surprising for that by introducing more distortion from the anti-forensic modification, we can not only obtain a higher concealability, but also have a lower rate of the output image. This phenomenon happens due to the different fingerprints left for lower secondary quality factors and higher secondary quality factors, and the entropy coding process in recompression. Specifically, for lower secondary quality factor scenario, change the coefficient histogram of a double compressed image into the one of a single compressed image actually decrease the entropy of the coefficients and thus results in a lower rate after recompression.

## 6. CONCLUSION

In this paper, we identified the tradeoff between concealability, rate, and distortion in anti-forensic systems. To do this, we defined the quantity concealability to measure the amount that editing fingerprints are concealed. We then examined the C-R-D tradeoff of double JPEG compression anti-forensics. In order to vary the strength of JPEG anti-forensics, we proposed a flexible anti-forensic dither to conceal double JPEG compression fingerprints. Then we experimentally characterized the C-R-D surfaces. Moreover, based on our experimental data, two surprising results have been revealed. One is that the forger tends to use a lower secondary quality factor rather than a higher one, for it can provide a much lower rate without increasing distortion or decreasing concealability. The other is that if the image is compressed using a lower secondary quality factor, the use of anti-forensics actually decreases the rate.

## 7. REFERENCES

[1] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," *IEEE Trans. on Signal Processing*, vol. 53, no. 2, pp. 758–767, Feb. 2005.

[2] H. Farid, "Blind inverse gamma correction," *IEEE Trans. on Information Forensics and Security*, vol. 10, no. 10, pp. 1428–1433, Oct. 2001.

[3] Matthias Kirchner A and Jessica Fridrich B, "On detection of median filtering in digital images," *Media Forensics and Security II, Proc. of SPIE-IS&T Electronic Imaging, SPIE*, vol. 7541, 754110, 2010.

[4] H. Farid, "Image forgery detection," *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[5] J. Lukáš, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Trans. on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, Jun. 2006.

[6] A. Swaminathan, M. Wu, and K.J.R. Liu, "Nonintrusive component forensics of visual sensors using output images," *IEEE Trans. on Information Forensics and Security*, vol. 2, no. 1, pp. 91–106, Mar. 2007.

[7] X. Chu, M. C. Stamm, W. S. Lin, and K. J. Ray Liu, "Forensic identification of compressively sensed images," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, Mar. 2012, pp. 1837–1840.

[8] W. S. Lin, S. K. Tjoa, H. V. Zhao, and K. J. R. Liu, "Digital image source coder forensics via intrinsic fingerprints," *IEEE Trans. on Information Forensics and Security*, vol. 4, no. 3, pp. 460–475, Sep. 2009.

[9] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *6th International Workshop on Information Hiding*, Toronto, Canada, 2004.

[10] T. Pevný and J. Fridrich, "Detection of double-compression in JPEG images for applications in steganography," *IEEE Trans. on Information Forensics and Security*, vol. 3, no. 2, pp. 247–258, Jun. 2008.

[11] X. Feng and G. Doërr, "JPEG recompression detection," in *Proc. of SPIE, Media Forensics and Security II*, Feb. 2010, vol. 7541, pp. 0J1–0J10.

[12] F. Huang, J. Huang, and Y. Q. Shi, "Detecting double JPEG compression with the same quantization matrix," *IEEE Trans. on Information Forensics and Security*, vol. 5, no. 4, pp. 848 –856, Dec. 2010.

[13] M. C. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," *IEEE Trans. on Information Forensics and Security*, vol. 6, no. 3, pp. 1050 –1065, Sep. 2011.

[14] M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Temporal forensics and anti-forensics for motion compensated video," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 4, pp. 1315–1329, Aug. 2012.

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

[16] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we trust digital image forensics?," in *Proc. 15th international conference on Multimedia*, New York, NY, USA, 2007, pp. 78–86.

[17] T. Pevný and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. of Digital Forensic Research Workshop*, Cleveland, Ohio, Aug. 2003.

[18] D. Fu, Y. Q. Shi, and W. Su, "A generalized Benford's law for JPEG coefficients and its applications in image forensics," in *Proc. of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents IX*, Feb. 2007, vol. 6505, pp. 1L1–1L11.

[19] Y. L. Chen and C. T. Hsu, "Detecting doubly compressed images based on quantization noise model and image restoration," in *IEEE International Workshop on Multimedia Signal Processing*, Oct. 2009, pp. 1–6.

[20] B. Mahdian and S. Saic, "Detecting double compressed JPEG images," in *3rd International Conference on Crime Detection and Prevention*, Dec. 2009, pp. 1–6.

[21] T.Bianchi and A.Piva, "Image forgery localization via block-grained analysis of jpeg artifacts," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 3, pp. 1003–1017, Jun. 2012.

[22] Bianchi T., De Rosa A., and Piva A., "Improved dct coefficient analysis for forgery localization in jpeg images," *Proc. IEEE ICASSP*, pp. 2444–2447, May 2011.

[23] Valenzise G., Tagliasacchi M., and Tubaro S., "The cost of jpeg compression anti-forensics," *Proc. IEEE ICASSP*, pp. 1884–1887, May 2011.

[24] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Trans. on Image Processing*, vol. 12, no. 2, pp. 230235, 2003.

[25] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. on Image Processing*, vol. 13, no. 4, pp. 600–612, Apr. 2004.

[26] E. Y. Lam, "A mathematical analysis of the DCT coefficient distributions for images," *IEEE Trans, on Image Proc.*, vol. 9, no. 10, pp. 1661–1666, Oct. 2000.

[27] J. R. Price and M. Rabbani, "Biased reconstruction for JPEG decoding," *IEEE Signal Processing Letters*, vol. 6, no. 12, pp. 297–299, 1999.

[28] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," *Proc. SPIE: Storage and Retrieval Methods and Applications for Multimedia*, vol. 5307, pp. 472480, 2004.