On Antiforensic Concealability With Rate-Distortion Tradeoff

Xiaoyu Chu, *Student Member, IEEE*, Matthew Christopher Stamm, *Member, IEEE*, Yan Chen, *Senior Member, IEEE*, and K. J. Ray Liu, *Fellow, IEEE*

***Abstract*— A signal's compression history is of particular forensic significance because it contains important information about the origin and authenticity of a signal. Because of this, antiforensic techniques have been developed that allow a forger to conceal manipulation fingerprints. However, when antiforensic techniques are applied to multimedia content, distortion may be introduced, or the data size may be increased. Furthermore, when compressing an antiforensically modified forgery, a tradeoff between the rate and distortion is introduced into the system. As a result, a forger must balance three factors, such as how much the fingerprints can be forensically concealed, the data rate, and the distortion, are interrelated to form a 3D tradeoff. In this paper, we characterize this tradeoff by defining concealability and using it to measure the effectiveness of an antiforensic attack. Then, to demonstrate this tradeoff in a realistic scenario, we examine the concealability-rate-distortion tradeoff in double JPEG compression antiforensics. To evaluate this tradeoff, we propose flexible antiforensic dither as an attack in which the forger can vary the strength of antiforensics. To reduce the time and computational complexity associated with decoding a JPEG file, applying antiforensics, and recompressing, we propose an antiforensic transcoder to efficiently complete these tasks in one step. Through simulation, two surprising results are revealed. One is that if a forger uses a lower quality factor in the second compression, applying antiforensics can both increase concealability and decrease the data rate. The other is that for any pairing of concealability and distortion values, achieved using a higher secondary quality factor, can also be achieved using a lower secondary quality factor at a lower data rate. As a result, the forger has an incentive to always recompress using a lower secondary quality factor.**

***Index Terms*— Concealability, anti-forensics, rate-distortion tradeoff, compression anti-forensics.**

I. Introduction

DUE to the wide availability of multimedia editing tools, the authenticity of multimedia content is often called into question. In order to verify the authenticity of this content, scientists have developed many forensic techniques to trace the processing histories of suspicious multimedia signals [1]–[11]. Among these techniques, tracing an images compression history has particular forensic significance. This is because detecting previous applications of JPEG compression in images that are currently stored in uncompressed formats can help the investigator to identify their origins [6], [7]. Furthermore, double or multiple compression may occur when a compressed image is manipulated, then re-saved in the same format. As a consequence, detecting double compression or multiple compression can imply that editing has possibly been applied to the image, thus calling its authenticity into question. There are many forensic tools to detect double and multiple compressions [12]–[22].

Given the forensic significance of an image's compression history, anti-forensic techniques have been developed in order to confuse forensic detectors [23]–[28]. These techniques enable a forger to fool forensic investigators through multiple ways. First, the forger can remove compression fingerprints completely so that the origin of the image cannot be detected. Furthermore, he/she can then recompress the anti-forensically modified image using another quantization table to mislead the identification of its origin [23]. When double compression occurs while editing a compressed image, modifying the compression history can also reduce the possibility of the forgery being detected via compression fingerprints. Additionally, other anti-forensic techniques have been developed to create forensically undetectable forgeries [29]–[32].

Studying anti-forensics and analyzing forgers' behavior are equally important for forensic purpose. Forensic investigators can use this information to improve existing detectors [33]. Furthermore, based on the specific fingerprints left by applying anti-forensics, investigators can develop new forensic detectors to reveal the use of anti-forensics [34]–[36]. Through either way, forensic invesitgators can make their detection system more robust by analyzing possible anti-forensic techniques.

Often, when anti-forensic techniques are applied, they introduce distortion to the multimedia content while concealing the fingerprints of manipulation [23]–[26]. For example, the authors in [23] remove JPEG compression fingerprints by adding anti-forensic dither to each DCT coefficient to eliminate quantization fingerprints. Thus, as the fingerprints are removed, distortion is also introduced to the DCT coefficients through the dither. In [24]–[26], the fingerprints are concealed by optimizing a certain cost function under some constraints. While achieving the anti-forensic performance, the distortion

Manuscript received August 22, 2014; revised November 12, 2014; accepted December 31, 2014. Date of publication January 8, 2015; date of current version February 11, 2015. This work was supported by the Division of Computing and Communication Foundations through the National Science Foundation under Grant CCF1320803. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Hitoshi Kiya.

X. Chu, Y. Chen, and K. J. R. Liu are with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park, MD 20742 USA (e-mail: cxygrace@umd.edu; yan@umd.edu; kjrliu@umd.edu).

M. C. Stamm is with the Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA 19104 USA (e-mail: mstamm@coe.drexel.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIP.2015.2390137

is also introduced to the content, the amount of which depends on the constraints. In these cases, the forger must balance between the amount that fingerprints have been concealed and the distortion introduced by anti-forensic modification.

Similarly, anti-forensics may also increase the size of the multimedia content while concealing the fingerprints of manipulation. For example, in order to conceal the fingerprints of video frame deletion/addition, the authors in [32] increase the P-frame prediction error to eliminate the periodic characteristic of the fingerprints. As a consequence, this technique enlarges the file size of the anti-forensically modified video. In such a case, the forger needs to balance between the degree to which fingerprints are concealed and the data rate.

While anti-forensic techniques may introduce the two kinds of tradeoffs discussed above, there is no existing work formally studying either of these tradeoffs. In fact, when compressing an anti-forensically modified forgery, there is a tradeoff among how much manipulation fingerprints can be concealed, the data rate, and distortion introduced into the signal. The forger must balance all three factors to appropriately decide the strength of his/her operation.

In this paper, we characterize the tradeoff discussed above. In order to measure the amount that manipulation fingerprints can be concealed, we define the effectiveness of concealing these fingerprints as *concealability*. To demonstrate this tradeoff in a real anti-forensic system, we introduce the concealability-rate-distortion (C-R-D) tradeoff in image double JPEG compression anti-forensics. In order to adjust concealability, we propose a flexible anti-forensic dither. To reduce the time and computational complexity associated with decoding a JPEG compressed image, applying anti-forensics, then recompressing it, we introduce an anti-forensic transcoder capable of efficiently performing these tasks in one step. Through a series of experiments, we have experimentally characterized the C-R-D tradeoff in JPEG anti-forensic systems. We have found that this tradeoff results in two distinct C-R-D surfaces; one for if the forger uses a lower JPEG quality factor during the second compression and another for if the forger uses a higher quality factor during the second compression. Furthermore, we observe two surprising phenomena from these experiments.

It is worth pointing out the implication of introducing the rate-distortion tradeoff in the field of multimedia forensics and anti-forensics. The rate-distortion tradeoff has been well studied for image and video compression [37], [38]. Both empirical and theoretical results have been derived to characterize the optimal achievable rate under a certain distortion constraint. Given this tradeoff, one can choose the optimal compression method according to his/her demands.

Since compression is a necessary signal processing for storage and transmission, rate-distortion tradeoff has been involved in the analysis of many systems in different fields. For example, when implementing compression, complexity is an essential factor, and the rate-distortion-complexity tradeoff was studied [39]. When transmitting the compressed multimedia content through wireless communication systems, energy consumption needs to be considered, where power-rate-distortion tradeoff was analyzed [40]. For multimedia attackers, there are works on studying the risk-distortion tradeoff for video collusion attacks [41]. Many anti-forensic schemes also try to maximize their concealability under some distortion constraint.

However, there is no existing work that considered the rate-distortion tradeoff when the attack or manipulation was applied on compressed multimedia content, while this is usually the case when the size of the multimedia signal is big. Thus, in this paper, we introduce the rate-distortion tradeoff to the field of multimedia forensics and anti-forensics and characterize the C-R-D tradeoff using the double image compression anti-forensics as an example. We believe that the C-R-D tradeoff also exists for other forensic and anti-forensic systems, like the video frame deletion/addition anti-forensic system.

The rest of the paper is organized as follows: first, we give an overview of image compression forensics and anti-forensics in Section II. Then, in Section III, we give the system model of double compression anti-forensics, and define the three tradeoff factors, concealability, rate and distortion. In Section IV, flexible anti-forensic dither is proposed for balancing the tradeoff between concealability, rate, and distortion. Section V introduces our anti-forensic transcoder, which combines decompression, flexible anti-forensic dither, and recompression into one process. Experimental results on the C-R-D tradeoff are shown and discussed in Section VI. Lastly, Section VII summarizes this paper.

II. Background

While our proposed C-R-D tradeoff exists in general image compression anti-forensic systems, we choose one of the most commonly used compression standards, JPEG, to characterize the tradeoff and show the effectiveness of our model. This section reviews the important concepts and techniques of JPEG compression forensics and anti-forensics which will be used in this case. Specifically, we start with a brief introduction of JPEG compression. Then, as an important set of fingerprints in forensics, double JPEG compression fingerprints are discussed. Among those double JPEG compression forensic detectors, without loss of generality, we choose one of the most popular and effective techniques to review in the next subsection. At last, we review the compression anti-forensic technique, which will be a special case in our proposed flexible anti-forensic scheme.

A. JPEG Compression

JPEG format is one of the most commonly used formats for images. We briefly overview the JPEG compression procedure as follows [42]: first, the image is separated into 8 by 8 blocks. Within each block, discrete cosine transform (DCT) is applied on the pixel values to obtain the DCT coefficients $x_{ij}, i, j = 0, 1, ..., 7$, where x_{ij} is the coefficient in subband (i, j). Then, quantization is applied on each DCT coefficient using a quantization table $\mathbf{Q}$, with each element denoted as q_{ij}. The quantized coefficients are

$$a_{ij} = \text{round}\left(\frac{x_{ij}}{q_{ij}}\right), \quad \text{for } i, j = 0, 1, \ldots, 7. \tag{1}$$

Finally, lossless entropy coding is applied on the quantized DCT coefficients to obtain the data ready for transmission or storage.

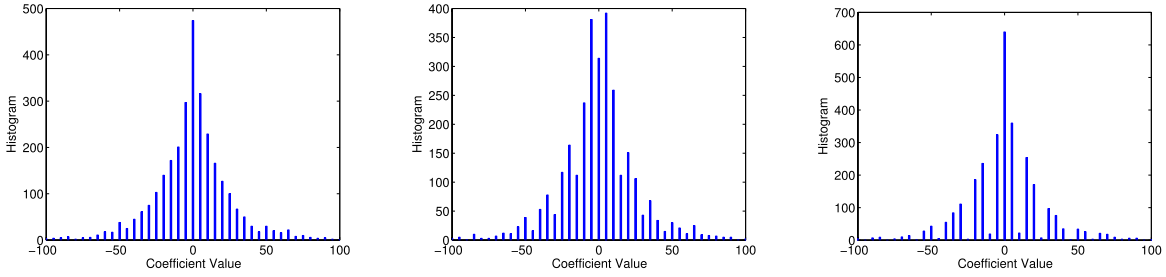


Fig. 1. Histograms of DCT coefficients subtracted from sub-band (0, 2) of a natural image been (a) single compressed with specific quantization step 5, (b) doubly compressed with quantization step 3 followed by 5, and (c) doubly compressed with quantization step 7 followed by 5.

Decompression has the reverse procedure of compression. Yet, it cannot recover the original image due to the lossy quantization process of JPEG compression. Specifically, during dequantization, the quantized DCT coefficients a_{ij} will be multiplied by its quantization steps q_{ij} to obtain the dequantized coefficients $y_{ij} = a_{ij}q_{ij}$, which is different from x_{ij}. These dequantized coefficients will instead only have values of integer multiples of the quantization step. We use the commonly applied model, Laplace distribution, to model the DCT coefficients in a certain subband of an uncompressed image [43]. Then, the histogram of the DCT coefficients from a JPEG compressed image can be modeled as a quantized Laplace distribution. Fig. 1(a) shows an example of the DCT coefficient histogram of a single JPEG compressed image.

B. Double JPEG Compression Fingerprints

If a forger modifies a JPEG image, it may be saved as JPEG again after modification. In such a case, the image has undergone two instances of JPEG compressions. If the quantization tables used in these two JPEG compressions are not exactly the same, double JPEG compression fingerprints will be left in the image. Since double JPEG compression happens in most forgeries, detecting its fingerprints is important in forensics to identify the existence of possible forgeries ever been applied on the image.

To see the double JPEG compression fingerprints, we examine the DCT coefficients of a double JPEG compressed image. Let $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$ denote the quantization tables used in the first and second JPEG compressions, respectively. Then the quantized DCT coefficients of this double JPEG compressed image is

$$b_{ij} = \text{round}\left(\frac{y_{ij}}{q_{ij}^{(2)}}\right) = \text{round}\left(\text{round}\left(\frac{x_{ij}}{q_{ij}^{(1)}}\right)\frac{q_{ij}^{(1)}}{q_{ij}^{(2)}}\right), \quad (2)$$

where $q_{ij}^{(1)}$ and $q_{ij}^{(2)}$ are elements of $\mathbf{Q}^{(1)}$ and $\mathbf{Q}^{(2)}$, respectively. If we decompress the image, the DCT coefficients observed are $w_{ij} = b_{ij}q_{ij}^{(2)}$.

Although we still observe quantized DCT coefficients with step size $q_{ij}^{(2)}$ from double JPEG compressed images, these coefficients cannot be modeled as quantized Laplace. During the second quantization, uneven numbers of bins of the single quantized histogram are collected into the new bins. Thus, the magnitudes of the double quantized bins will present periodic peaks or zeros [12], [13]. These periodic characteristics of the DCT coefficient histogram are identified as the fingerprints of double JPEG compression.

For illustration, let us take a DCT subband where the quantization steps in two compressions are different. Let q_1 and q_2 denote the quantization steps in this subband during the first and second JPEG compressions, respectively. Fig. 1(b) and 1(c) show the double JPEG compression fingerprints for $q_1 < q_2$ and $q_1 > q_2$, respectively.

C. Double JPEG Compression Detection

Due to the forensic significance of double JPEG compression fingerprints, there are many forensic techniques to detect such trace [12]–[18], [21], [22]. Various features are used to identify the double compression fingerprints, such as the DCT histograms and their Fourier transforms [12]–[14], [16], [18], the histograms of the first digit of DCT coefficients [22], and the number of DCT coefficients changed when recompressing with the same quantization table [21]. Among them, we choose one of the most popular and best performing detectors in [13] to review and use in this paper.

In [13], Pevný and Fridrich modeled the double JPEG compression detection problem as a classification of images between two classes:

$$C_1 : \text{The image is single compressed.} \quad (3)$$

$$C_2 : \text{The image is double compressed.} \quad (4)$$

Given the distinctive fingerprints of double JPEG compression in DCT coefficient histograms, they took the magnitudes of quantized bins in the histogram as the feature and fed them to a support vector machine.

Specifically, they chose the low frequency subbands where double JPEG compression fingerprints are most obvious. For each subband, the numbers of occurrences at integer multiples of q_2 were counted, where q_2 is the quantization step in the second compression. The feature vector was composed by concatenating the data from all chosen subbands:

$$\underline{v} = \left\{\frac{1}{c_{ij}}\big(h_{ij}(0), h_{ij}(1), \ldots, h_{ij}(15)\big)\,\middle|\,(i,j) \in \mathcal{L}\right\}, \quad (5)$$

where $h_{ij}(m)$ denotes the number of occurrences at $\pm mq_2$ in subband (i, j), and c_{ij} is a normalization constant,

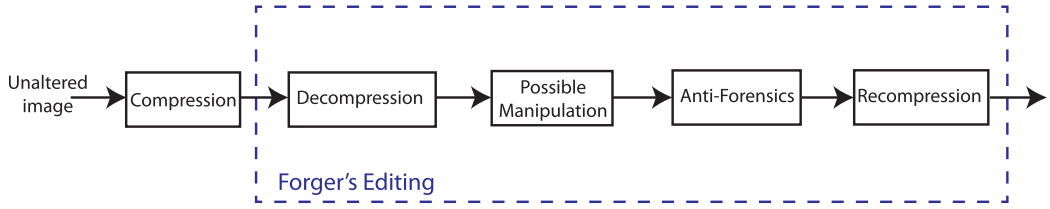


Fig. 2. The system model considered in this paper.

i.e., $c_{ij} = \sum_{m=0}^{15} h_{ij}(m)$. The set of low frequency subbands was chosen as

$$\mathcal{L} = \big\{(1,0),(2,0),(3,0),(0,1),(1,1),(2,1),(0,2),(1,2),(0,3)\big\}. \quad (6)$$

Given the feature vector $\underline{v}$ described above, the classification was done by using a soft-margin support vector machine with the Gaussian kernel [44] $k(x,y) = exp(-\gamma\,||x-y||^2)$. $k(x,y)$, also known as radial basis function, is a popular kernel function used in SVM classification. It can be interpreted as a similarity measure between two feature vector samples x and y. γ is a free parameter, which defaultly equals to 1/num_features in LIBSVM open source machine learning library.

D. JPEG Compression Anti-Forensics

There are also anti-forensic techniques that can falsify the image compression history and confuse the forensic detectors [23], [24], [26], [28]. Among them, we choose one of the most popular techniques in [23], which can successfully attack the forensic detector in [13], for illustration in this paper. Yet, the applicability of other anti-forensic techniques will also be discussed. In [23], single quantized DCT coefficients were added pre-designed dither so that the histogram will be smooth and look like the one from an uncompressed image. Then, when the forger modifies a JPEG image, as long as the traces of the first compression are removed, the recompressed image will only present single compression fingerprints. In this way, the forger can escape the forensic detection of double JPEG compression.

We briefly review the anti-forensic scheme proposed in [23] as follows: let random variable X denote the DCT coefficient of a certain sub-band (i,j) from an uncompressed image. $f(x,\lambda)$ is the modeled Laplace distribution of X with parameter λ, i.e.,

$$\mathbb{P}(X=x) = f(x,\lambda) = \frac{\lambda}{2}e^{-\lambda|x|}. \quad (7)$$

After JPEG compression, let Y denote the DCT coefficient of a JPEG compressed image and its distribution will be a quantized Laplace:

$$\mathbb{P}(Y=kq) = \begin{cases} 1-e^{-\lambda q/2} & \text{if } k=0, \\ e^{-\lambda|kq|}\sinh(\frac{\lambda q}{2}) & \text{otherwise,} \end{cases} \quad (8)$$

where q is the quantization step and $k \in \mathbb{Z}$. Then, in order to remove the fingerprints of JPEG compression, an anti-forensic dither, denoted as D, is added on the DCT coefficients of the JPEG compressed image. The resulting anti-forensically modified coefficients are $Z = Y + D$. Given a carefully designed anti-forensic dither, the distribution of Z can be equal to that of X. The distribution of the anti-forensic dither D in [23] is given by

$$\mathbb{P}(D=d|Y=kq) = \frac{f(kq+d,\hat{\lambda})}{\int_{(k-\frac{1}{2})q}^{(k+\frac{1}{2})q} f(x,\hat{\lambda})dx}\mathbb{1}(-\tfrac{q}{2} \le d < \tfrac{q}{2}), \quad (9)$$

where $\hat{\lambda}$ is the estimated parameter using coefficients Y and $\mathbb{1}(\cdot)$ is an indicator function.

III. Concealability-Rate-Distortion Tradeoff

In this paper, we assume that the forger wishes to recompress an image that has previously been JPEG compressed. This may happen under a variety of scenarios. For example, a forger may wish to falsify the content of the image. In this case, the forger must decompress the image, perform some manipulation, then recompress the image. Alternatively, if the forger does not wish to alter the content of the image but just wishes to falsify its origin, they must recompress the image using the quantization matrix used by the target camera [23]. In both scenarios, standard recompression will cause double JPEG fingerprints to occur.

To analyze both of these scenarios, we adopt the following system shown in Fig. 2. First, the forger receives a JPEG compressed image, which we refer to as the unaltered image. The forger will then decompress the image and perform any desired image manipulation. After this, they will apply anti-forensics to remove JPEG compression fingerprints, then recompress the image using their desired compression parameters. During this process, the forger is able to adjust the strength with which they apply anti-forensics, as well as the quality factor or quantization tables used during compression. Because we are interested primarily in characterizing the tradeoff among rate, distortion and the amount of double JPEG compression fingerprints that can be concealed, we neglect any effects caused by other possible manipulations for the purposes of this work.

Intuitively, when a forger applies anti-forensic techniques, he/she must balance a tradeoff between the amount of double JPEG compression fingerprints that can be concealed and the distortion introduced by anti-forensic modification. The forger can vary the anti-forensic strength to adjust the amount of modification caused by the anti-forensic technique, and thus balance this tradeoff. When recompressing the forgery, there is

a well-known tradeoff between the data rate and the distortion. In addition, since anti-forensics modifies the distribution of the DCT coefficients, it is possible that it can also affect the data rate during recompression. On the other hand, the performance of double JPEG compression detection depends on the relationship between the primary and the secondary quality factor. Thus, the secondary quality factor may also affect the possibility that the double JPEG compression will be detected. In other words, the amount of double JPEG compression fingerprints that can be concealed is also affected by the secondary quality factor.

Therefore, the amount of double JPEG compression fingerprints that can be concealed, the data rate, and the distortion are all related in the system. Adjusting either the strength of anti-forensics or the quality factor in recompression process will result in change of all three factors. Therefore, in order to achieve a certain requirement, the forger must balance the tradeoff among these three factors.

We note that, given the existence of many compression anti-forensic detectors, i.e., counter anti-forensic schemes, [34]–[36], our system model can be extended to include their effect in the following ways: 1) generalize the definition of concealability by including the amount of anti-forensic fingerprints that can be concealed 2) introduce another dimension in the tradeoff to reflect the detectability of anti-forensic techniques.

In order to characterize the tradeoff between how much the double JPEG compression fingerprints can be concealed, the data rate, and the distortion, we first define the term *concealability* as the measure of how much the fingerprints can be concealed. Since the accuracy of a detector is one measure of how well the fingerprints have been concealed, we define concealability in terms of the detection rate.

When detecting manipulation fingerprints, a simple hypothesis test is often used, where two hypotheses are defined as

H_0 : Manipulation fingerprints do not present.

H_1 : Manipulation fingerprints do present.

A forensic investigator will apply a certain decision rule to a suspicious signal to determine which hypothesis it belongs to. The decision rule results in a probability that the fingerprints are correctly detected, which is called the detection rate; and a probability that an unmanipulated signal is identified as a falsified one, which is called the false alarm rate. Different decision rules often results in different pairs of detection rates and false alarm rates. A receiver operating characteristic (ROC) curve plotting all reachable pairs of detection rates and false alarm rates characterizes the overall performance of the detector.

We define concealability as follows: let I denote the image edited by the forger. Let function $m(\cdot)$ be the modification made by the forger. Then, $m(I)$ is the forger modified image. In the system describe in Fig. 2, I represents the single compressed JPEG image and $m(I)$ represents the double JPEG compressed and anti-forensically modified image. For a given detector and a certain false alarm rate P_f, there is a corresponding decision rule $\delta_{P_f}(\cdot)$. Then the concealability of the forger edited image $m(I)$ is defined as

$$C(m, P_f) = \min\left(\frac{1-\mathbb{P}\left(\delta_{P_f}(m(I)) = H_1\right)}{1-P_f}, 1\right). \quad (10)$$

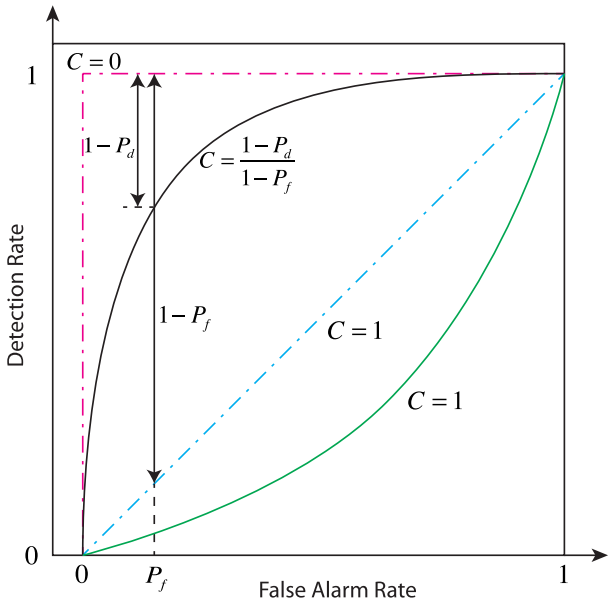


Fig. 3. Examples of concealabilities related to ROC curves. When the detector achieves perfect detection, the forger has concealability of the fingerprints as 0. When the ROC curve is at or below the random decision line, we say that the forger has achieved concealability as 1. Then for those ROC curves between perfect detection and random decision, the concealability ranges from 0 to 1 and depends on a certain false alarm rate.

We explain the definition of concealability by using ROC curves, as it is shown in Fig. 3. When no anti-forensics has been applied, the best performance of a forensic detector is perfect detection. That is, the detector can achieve detection rate of 100% at false alarm rate of 0%. Under this scenario, manipulation fingerprints can be detected without any error, and we say that the fingerprints have been fully exposed to the investigators. Thus, the concealability in this case will be its minimum value 0.

On the other hand, if anti-forensics are applied, it will reduce the accuracy of the forensic detector and increase the false alarm rate. Such degradation reaches its maximum when the detection rate becomes the same as the false alarm rate. In this case, the detector will act as an equal probability random decision process, i.e., the decision is made equivalently to randomly flipping a coin. Under this scenario, forger edited images will have no difference with those that have no been edited by the forger. Thus, we say that manipulation fingerprints have been fully concealed to the forensic investigators. We define the concealability in this case as its maximum value 1. We note that since the forensic detection strategy is determined regardless of the possible existence of anti-forensic technique, one may obtain a ROC curve below the random decision line, where detection rates equal to false alarm rates. However, because this scenario also implies that the forger has fully concealed the fingerprints, we define the concealability in such case also as 1.

For scenarios between these extreme cases, the concealability is defined as a measure dependent on the false alarm rate. Since it is inversely proportional to the detection rate and the value is limited between 0 and 1, we use a normalized decreasing function of the detection rate $\frac{1-P_d}{1-P_f}$ to characterize the concealability at a certain false alarm rate.

To evaluate the distortion, we define a measure that is based on the mean structural similarity (MSSIM) between the image that has not been edited by the forger and the one after the forger's editing [45]. MSSIM is a popular similarity measure between 0 and 1 that matches well with human perception. In order to let the distortion equal to zero when the two images are identical, i.e., when the similarity is 0, we define the distortion between I and $m(I)$ as

$$D(m) = 1 - \text{MSSIM}\big(I, m(I)\big). \tag{11}$$

We note that similar results can be obtained for other measures of distortion such as mean square error (MSE), which will be shown in simulation results.

Lastly, we use bits per pixel as the measure of rate. Specifically, the rate is calculated by examining the size of the forger edited image and dividing it by the number of pixels in that image:

$$R(m) = \frac{\text{number of bits of } m(I)}{\text{number of pixels in } m(I)}. \tag{12}$$

IV. Flexible Anti-Forensic Dither

In order to balance the tradeoff of concealability and distortion during the anti-forensic process, the forger needs to vary the strength of anti-forensics. Though there exists anti-forensic techniques to fully conceal the fingerprints of double JPEG compression [23]–[26], these techniques do not provide the flexibility to control the strength of anti-forensics. However, in order to characterize the C-R-D tradeoff and find the best choice, flexible anti-forensic schemes are necessary. In this section, we propose a *flexible anti-forensic dither* for the technique in [23] that enables the forger to adjust the strength of anti-forensics. Similar concept can be applied on other anti-forensic techniques, which we will discuss in the end of this section.

As we discussed in section II, double JPEG compression fingerprints are presented in DCT coefficients. Thus, in order to remove the fingerprints, our flexible anti-forensic dither will also be applied on DCT coefficients. To develop flexible dither, let us examine the procedure that a DCT coefficient in a certain subband of an image will go through during the whole process described in Fig. 2. First of all, the unaltered image will go through its first JPEG compression. Let q_1 denote the quantization step of the examined subband used in this compression. Then, the DCT coefficient of the single compressed image is obtained by

$$Y = q_1 \,\text{round}\,(X/q_1). \tag{13}$$

We assume that X obeys a Laplace distribution (7). Thus, Y will be distributed as a quantized Laplace distribution with quantization step size q_1.

Secondly, the flexible anti-forensic dither is applied on Y. Let α denote the *anti-forensic strength*. We define that $0 \leq \alpha \leq 1$. The corresponding flexible anti-forensic dither is denoted as D_α. Thus, the anti-forensically modified DCT coefficient becomes to

$$Z_\alpha = Y + D_\alpha. \tag{14}$$

Lastly, after recompressing Z_α with a quantization step q_2, the double JPEG compressed and anti-forensically modified DCT coefficient is

$$W_\alpha = q_2 \,\text{round}\,(Z_\alpha/q_2). \tag{15}$$

If no anti-forensics has been applied, which means that the anti-forensic strength is 0, then $W_0 = q_2 \,\text{round}(Y/q_2)$. The histogram of W_0 will present the fingerprints of double JPEG compression, as it is shown in Fig. 1(b) or Fig. 1(c). The periodic peaks or zeros in the histogram distinguish W_0 from those of single compressed images, who have quantized Laplace distribution shape as shown in Fig. 1(a). Thus, by measuring the distance between the normalized histogram of W_0 and the quantized Laplace distribution, forensic analysts can detect double JPEG compression.

If anti-forensics are fully applied, as it is the case in [23], the anti-forensic strength is 1, and the distribution of D_1 is the same as (9) with q substituted with q_1. Then, the distribution of Y will be the same as that of X. Consequently, the distribution of W_1 will be a quantized Laplace distribution. In such a case, the double JPEG compressed and anti-forensically modified image is hard to be distinguished from single JPEG compressed images through DCT coefficient histograms.

When anti-forensic strength is not applied in full, we can reduce the anti-forensic distortion by sacrificing the exposure of fingerprints to the forensic detector. That is, the histogram of W_α will be less like a quantized Laplace distribution when less anti-forensic strength is applied. By examining (9), we can see that the distribution of the dither D_1 has a bounded support $[-q_1/2, q_1/2)$. The shape of this distribution is a normalized and shifted version of the target distribution $f(x, \hat{\lambda})$ on support $\big[(k-1/2)q_1, (k+1/2)q_1\big)$ with left shifting of kq_1. Such design is to make the conditional probability $\mathbb{P}(Z_1 = z | Y = kq_1)$ be the same as $f(z, \hat{\lambda})$ normalized by $\mathbb{P}(Y = kq_1)$ with $z \in [kq_1 - q_1/2, kq_1 + q_1/2)$. Then, with Y taken all integer multiplies of q_1, the distribution of Z_1 will be the same as $f(z, \hat{\lambda})$.

When $\alpha < 1$, we shrink the support of the anti-forensic dither to decrease distortion. Meanwhile, the similarity between the distribution of Z_α and $f(z, \hat{\lambda})$ will be reduced. We note that because of the shrink of the dither's support, the anti-forensically dithered coefficients will not spread out the entire quantization interval. Consequently, the support of the histogram of the anti-forensically modified image before recompression will not match the support of the histogram of an uncompressed image. Nevertheless, the image will be recompressed, where all coefficients are requantized to integer multiples of the new quantization step. The use of anti-forensic dither can cause some coefficients that would normally get quantized to lq_2 to instead be mapped to $(l-1)q_2$ or $(l+1)q_2$.

In this way, the strength of the double compression fingerprints are weakened by the anti-forensic dither.

Let $S_\alpha^{(k)}$ denote the support of Z_α given $Y = kq_1$, which means that the support of D_α is $S_\alpha^{(k)}$ left shifted by kq_1. Then the range of $S_\alpha^{(k)}$ will be decreased when less anti-forensic strength is applied, i.e., α decreases. We will give the explicit expression of $S_\alpha^{(k)}$ in later paragraphs. We still take the shape of the dither's distribution to be a normalized and shifted version of $f(x, \hat{\lambda})$. The distribution of the flexible anti-forensic dither is proposed as

$$\mathbb{P}(D_\alpha = d|Y = kq_1) = \frac{f(kq_1 + d, \hat{\lambda})}{\int_{S_\alpha^{(k)}} f(x, \hat{\lambda})dx} \mathbb{1}\left(kq_1 + d \in S_\alpha^{(k)}\right). \tag{16}$$

We define $S_1^{(k)}$ as

$$S_1^{(k)} = \left\{t \in \mathbb{R} \middle| (k - \tfrac{1}{2})q_1 \le t < (k + \tfrac{1}{2})q_1\right\}, \tag{17}$$

then (9) becomes a special case of (16). By our definition, $S_0^{(k)}$ is the support of Z_0 given $Y = kq_1$, which results in W_0. However, due to the second compression described by (15), there are multiple choices of $S_0^{(k)}$ which can lead to the same W_0 after requantization. Specifically, let lq_2 be the quantized bin that $Y = kq_1$ will be mapped into during the second compression, i.e.,

$$l = \text{round}\left(\frac{kq_1}{q_2}\right). \tag{18}$$

Then, any dither within the range $\left[(l - 1/2)q_2, (l + 1/2)q_2\right)$ will be mapped into the same bin lq_2. We define $S_0^{(k)}$ as the one that has the largest range while any dither within this support will be mapped into the same $W_0 = lq_2$. In addition, the property of $S_\alpha^{(k)}$ needs to be satisfied, i.e., $S_0^{(k)} \subseteq S_1^{(k)}$. Thus, the expression of $S_0^{(k)}$ is given as

$$S_0^{(k)} = \left\{t \in S_1^{(k)} \middle| (l - \tfrac{1}{2})q_2 \le t < (l + \tfrac{1}{2})q_2\right\}. \tag{19}$$

Fig. 4 shows an illustration of how to find $S_0^{(k)}$ and $S_1^{(k)}$ for a certain quantized bin $Y = kq_1$. Four cases are listed in the figure regarding the relative positions of the quantization intervals of Y in the first compression and $W_0 = lq_2$ in the second compression. Basically, $S_0^{(k)}$ is the intersection between the intervals $\left[(k - \frac{1}{2})q_1, (k + \frac{1}{2})q_1\right)$ and $\left[(l - \frac{1}{2})q_2, (l + \frac{1}{2})q_2\right)$.

Given the extreme cases of $S_\alpha^{(k)}$ when $\alpha = 0$ and $\alpha = 1$, we pick up $S_\alpha^{(k)}, 0 < \alpha < 1$, from the convex hull of the supports of $S_0^{(k)}$ and $S_1^{(k)}$. Formally, let $b_{\alpha,1}$ and $b_{\alpha,2}$ be the lower and upper bounds of support set $S_\alpha^{(k)}$, respectively. We have the extreme cases

$$\begin{aligned} b_{0,1} &= \max\left((k - \tfrac{1}{2})q_1, (l - \tfrac{1}{2})q_2\right), \quad b_{1,1} = (k - \tfrac{1}{2})q_1, \\ b_{0,2} &= \min\left((k + \tfrac{1}{2})q_1, (l + \tfrac{1}{2})q_2\right), \quad b_{1,2} = (k + \tfrac{1}{2})q_1. \end{aligned} \tag{20}$$

Then, $S_\alpha^{(k)}, 0 < \alpha < 1$ is defined as

$$S_\alpha^{(k)} = \left\{t \in \mathbb{R} \middle| b_{\alpha,1} \le t < b_{\alpha,2}\right\},$$

where

$$b_{\alpha,j} = (1 - \alpha)b_{0,j} + \alpha b_{1,j}, \quad \text{for } j = 1, 2. \tag{21}$$

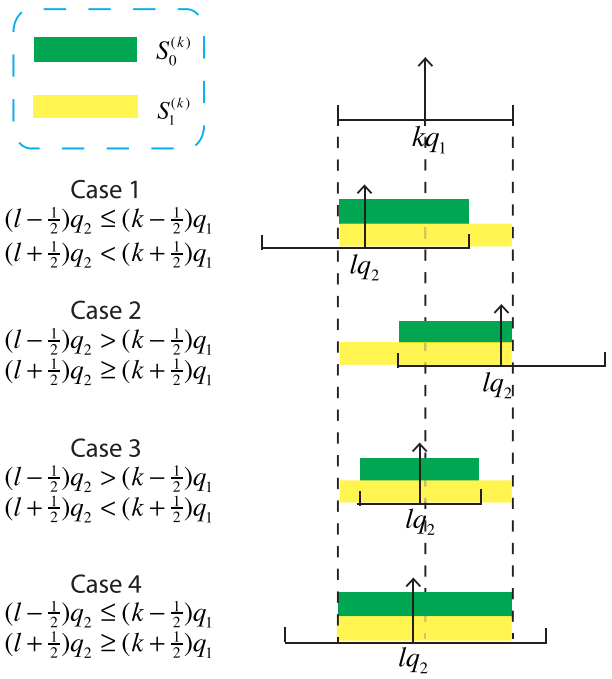


Fig. 4. An illustration of how to determine $S_0^{(k)}$ and $S_1^{(k)}$ for a certain value of $Y = kq_1$. The vertical arrows denote the position of a certain quantized bin in the coefficient histogram. The horizontal line segment at the bottom of each arrow represents the quantization interval where all values within this range will be mapped into the quantized bin indicated by the arrow. lq_2 is the quantized bin that kq_1 will be mapped into during the recompression. According to different positions of lq_2 and its quantization intervals, there are four cases for $S_0^{(k)}$, while $S_1^{(k)}$ keeps the same for the same kq_1.

Using (21) and (16), our flexible anti-forensic dither can be generated from this pre-determined distribution.

The flexible anti-forensic scheme can be summarized as follows:

1) Obtain DCT coefficients by decompressing the single compressed image for all subbands.
2) In each subband, estimate the parameter $\hat{\lambda}$ of the Laplace distribution function $f(x, \hat{\lambda})$ using Y statistics [23].
3) For a certain anti-forensic strength α, calculate $S_\alpha^{(k)}$ and $\mathbb{P}(D_\alpha = d|Y = kq_1)$ for each kq_1 using (21) and (16).
4) For each $Y = kq_1$, randomly generate a value of D_α from the distribution function (16), and add it to Y to obtain Z_α.
5) Obtain the anti-forensically modified image by modifying all coefficients in all subbands and mapping them to pixel domain.

We note that the concealability-distortion tradeoff also occurs in other anti-forensic techniques, where the forger can vary the anti-forensic strength to balance them [24]–[26], [28]. In [24], the authors modified pixel values of an image to conceal JPEG compression fingerprints. Specifically, they minimized the total variance and variance difference between boundary areas and interior areas of blocks while limiting the modified DCT coefficients in a distortion constraint set. The smaller the minimized function is, the higher the concealability will be. Then, by shrinking the range of the constraint set,

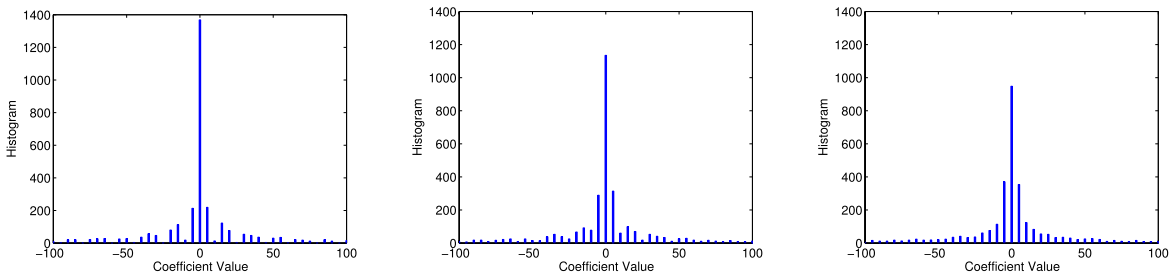


Fig. 5. Histograms of DCT coefficients of an anti-forensically modified and double compressed image with anti-forensic strength (a) $\alpha = 0$, (b) $\alpha = 0.4$, and (c) $\alpha = 1$.

less distortion is allowed to be introduced to the image, but a larger minimized function will be obtained, and thus concealability decreases. Techniques in [25] and [26] concealed manipulation fingerprints by modifying the manipulated histogram to one that is closest to an unaltered histogram under some distortion constraints. Similarly, by varying the distortion constraints, the forger is able to vary how close the anti-forensically modified histogram is to an unaltered one, and thus vary the concealability. Lastly, in [28], the fingerprints of double JPEG compression with the same quantization table were concealed by modifying the DCT coefficients in textural regions. Then, the less the DCT coefficients were modified, the less distortion it introduces to the image. However, the fingerprints are less concealed, and thus concealability becomes smaller. In all cases, the tradeoff between concealability and distortion exists and flexible anti-forensic techniques can be applied to characterize them.

V. Anti-Forensic Transcoder

As a post-processing technique, anti-forensic dither can be used whenever a forgery needs to be recompressed without leaving double JPEG compression fingerprints. Yet, there are some cases, for example when modifying the quantization table of the compressed image, where the forger simply wants to recompress the JPEG image without performing other manipulations. In such cases, the forger do not need to decompress the JPEG image, apply anti-forensic dither, and then recompress the image. Instead, the forger can use an integrated anti-forensic transcoder to directly falsifies the DCT coefficients from the JPEG file and transcodes them into the coefficients associated with another quantization table while no double compression fingerprints will be detected. In this section, we propose this anti-forensic transcoder to reduce the time and computational complexity associated with decompressing a JPEG image, applying anti-forensics, then recompressing it, and efficiently perform all these tasks in one step.

To propose this anti-forensic transcoder, let us review the modifications of DCT coefficients made by the anti-forensic dither and recompression. As described in Section IV, the decompressed DCT coefficient Y will be added with the anti-forensic dither D_α to obtain the anti-forensically modified coefficient Z_α. This modification dithers each $Y = kq_1$ to some nearby values. When we examine the coefficients' histogram, we will see that the anti-forensic dither spreads each quantized bin within a certain range. Then, Z_α will be mapped into pixel domain where recompression is applied. During recompression, Z_α is again transformed into DCT domain and then quantized. In quantization process, some of the dithered values will be mapped into one bin while some of them may be mapped into other bins. Thus, even though these dithered coefficients are all coming from the same value of $Y = kq_1$, they will be mapped into different values of $W_\alpha = jq_2$, $j_{\min} \le j \le j_{\max}$. If we figure out what portions of coefficients valued as $Y = kq_1$ will be mapped into $W_\alpha = jq_2$, $j_{\min} \le j \le j_{\max}$, we can then directly map some of the coefficients $Y = kq_1$ to one of W_α without the intermediate state of Z_α. Different anti-forensic strengths will affect these portions and also the range that kq_1 will be mapped into, i.e., $j_{\min}$ and $j_{\max}$.

Fig. 5 shows the transition of the histograms of W_α when increasing the anti-forensic strength. When no anti-forensics is applied, each $Y = kq_1$ can only be mapped into one bin valued as $W_0 = lq_2$ during the second quantization. Without loss of generality, we consider the case where $q_1 > q_2$. Then, some integer multiples of q_2 may even not have corresponding coefficients. This results in those nearly zero bins in Fig. 5(a). With anti-forensics applied, some of the coefficients valued as kq_1 can be mapped into nearby bins other than the lq_2 bin. Thus, those nearly zero bins can be gradually filled up by its neighboring bins to finally obtain the quantized Laplace shape histogram, as it is shown in Fig. 5(b) and Fig. 5(c).

We derive the direct map between Y and W_α using the intermediate state Z_α described in Section IV. First, we decide the range that kq_1 can be mapped into. Recall that $S_\alpha^{(k)}$ is the support of Z_α given $Y = kq_1$. Thus, when quantizing Z_α to obtain $W_\alpha = jq_2$, all candidates of j will be bounded by

$$j_{\min} = \text{round}\left(\frac{b_{\alpha,1}}{q_2}\right),$$
$$j_{\max} = \text{round}\left(\frac{b_{\alpha,2}}{q_2}\right). \tag{22}$$

Next, we let γ_{kj} denote the probability that the anti-forensic transcoder maps a coefficient valued as kq_1 to jq_2. Then, we can describe the mapping of the anti-forensic transcoder on DCT coefficients by using the following transition

probability function,

$$\mathbb{P}(W_\alpha = jq_2|Y = kq_1) = \begin{cases} \gamma_{kj} & \text{if } j_{\min} \le j \le j_{\max}, \\ 0 & \text{otherwise.} \end{cases} \quad (23)$$

The value of γ_{kj} depends on the extent that the anti-forensic dither spreads the single bin kq_1, which is also determined by the anti-forensic strength. From (16) and (14), we have

$$\mathbb{P}(Z_\alpha = z|Y = kq_1) = \frac{f(z,\hat{\lambda})}{\int_{S_\alpha^{(k)}} f(x,\hat{\lambda})dx}\mathbb{1}\left(z \in S_\alpha^{(k)}\right). \quad (24)$$

When quantizing Z_α, those values belonging to the range $\left[(j-\frac{1}{2})q_2, (j+\frac{1}{2})q_2\right)$ will be mapped to value $W_\alpha = jq_2$. Let R_j denote this quantization interval for $W = jq_2$, i.e.,

$$R_j = \left\{t \in \mathbb{R} | (j-1/2)q_2 \le t < (j+1/2)q_2\right\}. \quad (25)$$

Then, we have

$$\begin{aligned} \gamma_{kj} &= \mathbb{P}(W_\alpha = jq_2|Y = kq_1) \\ &= \int_{R_j} \mathbb{P}(Z_\alpha = z|Y = kq_1)dz \\ &= \frac{\int_{S_\alpha^{(k)} \cap R_j} f(z,\hat{\lambda})dz}{\int_{S_\alpha^{(k)}} f(x,\hat{\lambda})dx} \end{aligned} \quad (26)$$

Given $j_{\min}$, $j_{\max}$, and γ_{kj} well defined by (22) and (26), the anti-forensic transcoder can be described as follows: Let U be a uniformly distributed random variable within $[0, 1)$. Then, for a coefficient valued as kq_1, the anti-forensic transcoder with anti-forensic strength α will map it to

$$W_\alpha = \sum_{j=j_{\min}}^{j_{\max}} jq_2 \mathbb{1}\Big(\sum_{t=j_{\min}}^{j-1} \gamma_{kt} \le U < \sum_{t=j_{\min}}^{j} \gamma_{kt}\Big), \quad (27)$$

where $\sum_{t=j_{\min}}^{j-1} \gamma_{kt} = 0$ when $j = j_{\min}$.

We summarize the anti-forensic transcoder as follows:

1) Obtain DCT coefficients by directly reading the JPEG file.
2) In each subband, estimate the parameter $\hat{\lambda}$ of the Laplace distribution function $f(x,\hat{\lambda})$ using Y statistics [23].
3) For a certain anti-forensic strength α, calculate $j_{\min}$, $j_{\max}$, and γ_{kj} using (22) and (26).
4) For each $Y = kq_1$, transcode it to W_α according to equation (27).
5) Apply lossless entropy coding similar as that used in JPEG compression to obtain the undetectable double JPEG compressed file.

We note that, for a certain anti-forensic strength and recompression quantization table, by either applying the anti-forensic dither and then recompressing, or directly applying the anti-forensic dither, the forger can obtain the same double JPEG compressed and anti-forensically modified image file.

VI. Simulation Results and Analysis

In order to characterize the C-R-D tradeoff, we set up an experiment to obtain the reachable C-R-D values. We used the flexible anti-forensic dither to apply anti-forensics with adjustable strength. During the experiment, different strengths of anti-forensics and different quality factors of the recompression were used. Then, based on the data, we characterized the tradeoff using polynomial surfaces. Two surprising results were found during the analysis of the simulation results.

TABLE I

Numbers of Images in (A) Training Database and (B) Testing Database That Were Used in Our Experiment

(A)

	# of different image content	# of different Q_2	Total # of images
H_0	1000	31	31000
H_1	1000	31	31000

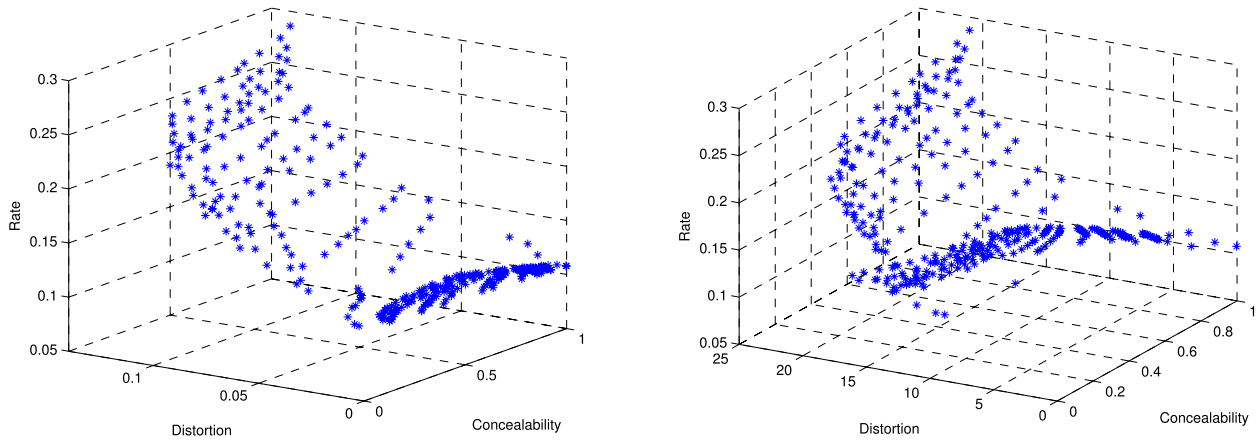
(B)

	# of different image content	# of different Q_2	# of different α	Total # of images
H_0	300	31	1	9300
H_1	300	31	11	102300

A. Two C-R-D Tradeoffs Revealed From Simulation

To experimentally characterize the C-R-D surface, we compressed, then anti-forensically modified and recompressed a set of images using a variety of JPEG quality factors and anti-forensic strengths. We then measured the concealability, rate, and distortion of each pairing of quality factor and anti-forensic strength, and used the resulting data to characterize the C-R-D surface.

We set up the simulation database based on the 1300 natural unaltered images from UCID database [46]. We examine the behavior of the forger, who can vary the anti-forensic strength and the quality factor of the recompression. So we fixed the first quality factor $Q_1 = 75$, and varied the secondary quality factor Q_2 from 60 to 90 with incremental interval 1. Then, we took 1000 unaltered images from the UCID database and JPEG compress each one using quality factors Q_2 to build the single compressed image database for training. The training database of double compressed images were obtained by compressing the same 1000 unaltered images using quality factor 75 and then recompressing them using secondary quality factors Q_2. Thus, the training database in our simulation contained $1000 \times 31 \times 2 = 62000$ images. Our testing database involved single compressed images, double compressed images and double compressed but anti-forensically modified images. The single compressed images for testing were composed by compressing the rest 300 unaltered images from the UCID database using quality factors Q_2. The double compressed images and double compressed but anti-forensically modified images were obtained by first compressing the same 300 unaltered images using quality factor 75, then applying anti-forensic dithers with strengths taken from range $[0, 1]$, and lastly recompressing them using secondary quality factors Q_2. We used 11 different anti-forensic strengths from $[0, 1]$ for each secondary quality factor. Therefore, we finally built up a testing database containing $300 \times (31 + 31 \times 11) = 111600$ images. The numbers of images used in our experiment are summarized in Table I.



(a) (b)

Fig. 6. Concealability, rate, and distortion triples for all tested anti-forensic strengths and secondary quality factors with distortion defined based on (a) MSSIM in (11) and (b) MSE.

In order to characterize the C-R-D tradeoff, we calculate the concealability, rate, and distortion for each pair of anti-forensic strength and secondary quality factor. The detection technique described in Section II-C developed by Pevný et al. was used to perform double JPEG compression detection. Different detectors were trained for each secondary quality factor using images from the training database described in the above paragraph. The false alarm rate is taken as 5%. Rate and distortion are calculated as the mean values of all the testing images with the same anti-forensic strength and secondary quality factor. Besides using (11) to calculate distortion, we also calculated mean square errors as an illustration of the results by applying other distortion measures. Based on the concealabilities, rates, and distortions obtained for different anti-forensic strengths and secondary quality factors, we plot each triple of concealability, rate, and distortion as a point in 3D figures in Fig. 6. Fig. 6(a) shows the tradeoff for using our definition of distortion in (11), and Fig. 6(b) is the tradeoff when we measure the distortion using the mean square error.

We find that, in both figures of Fig. 6, the points are separated into two surfaces. The lower surface is composed by the points where the secondary quality factor is lower than the primary quality factor. We call the tradeoff described by them as the lower quality factor tradeoff. The higher surface contains the points where the secondary quality factor is higher than the primary quality factor. This tradeoff is called the higher quality factor tradeoff. We note that the authors in [34] have found the similar phenomenon about separated cases for lower quality factors and higher quality factors when they studied the counter detector of the anti-forensic dither. Yet, they only considered the change on distortion, while our work characterizes the whole C-R-D tradeoff. We will study these two tradeoffs separately in the following two subsections. For the sake of space limitation, we only give the detailed analysis to Fig. 6(a), while the other one can be analyzed similarly.

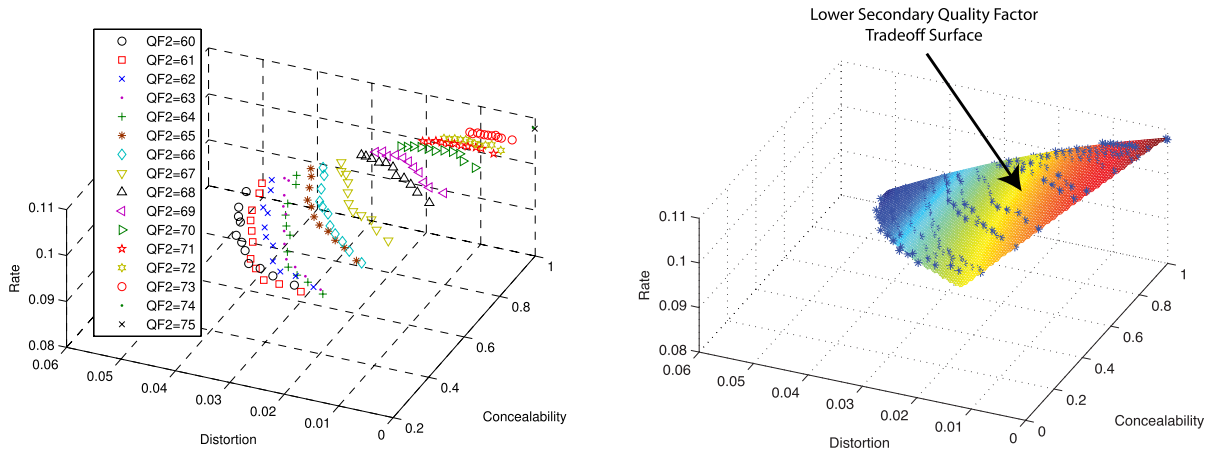
B. C-R-D Tradeoff for Lower Secondary Quality Factors

To characterize the C-R-D tradeoff for lower secondary quality factors, we plot those triple points obtained by using lower secondary quality factors in Fig. 7(a). Different markers represent different secondary quality factors. Each marker has several points obtained by using different anti-forensic strengths. Among them, the one with higher concealability implies that more anti-forensic strength has been applied to get this point. It is easy to see that increasing anti-forensic strength will increase concealability but also introduce more distortion.

Since anti-forensic dither adds noise to DCT coefficients, and typically a noisy signal is harder to be compressed, we would expect to get a higher rate when applying anti-forensics. However, we surprisingly find that, in the case of a lower secondary quality factor, applying anti-forensics will actually decrease the rate. We use a 2D figure to more explicitly present this surprising result in Fig. 8.

This phenomenon happens due to the entropy coding procedure of JPEG compression. When quantization table is fixed, the rate of the compressed image depends on the entropy of the DCT coefficients. Since the coefficient histogram describes its probability density function, we can use the normalized histogram to compare the entropy. Furthermore, when the normalized histogram is closer to the uniform distribution, it implies a higher entropy of the coefficient. With anti-forensics applied to the double compressed image, it gradually changes the coefficient histogram from a double compressed histogram to a single compressed one. Thus, we can compare the entropies of these two cases to see how does anti-forensics affect the rate. Recall the typical coefficient histograms for single compressed and double compressed images shown in Fig. 1. It is easy to see that the entropy of the single compressed coefficient (histogram is shown in Fig. 1(a)) is less than that of the double compressed one for lower quality factor case (histogram is shown in Fig. 1(b)), where $q_2 > q_1$, i.e., $Q_2 < Q_1$. Thus, when anti-forensics change the histogram from the double compressed one to the single compressed one, it decreases the rate. However, similar argument implies that the result will be reversed for higher secondary quality factor scenario.

Next, we characterize the lower secondary quality factor tradeoff using a polynomial surface, as it is shown in Fig. 7(b).



(a) (b)

Fig. 7. Tradeoff of concealability, rate, and distortion for the case where the second quality factor is smaller than the first one. (a) plots the reachable (C, R, D) points, where the points with the same marker and color are those who have the same secondary compression quality factor but have been applied different anti-forensic strengths. The higher the concealability, the more the anti-forensic strength. (b) is the polynominal fitting surface of (a).

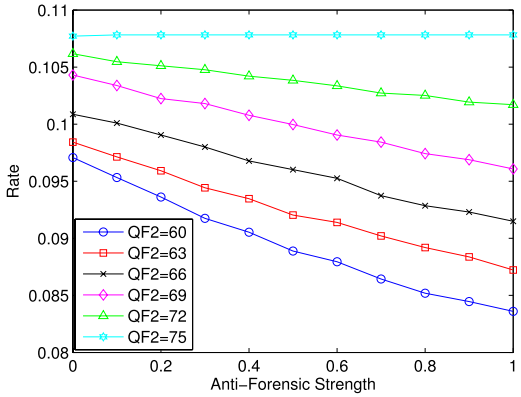


Fig. 8. Rate changes with anti-forensic strength for lower secondary quality factor case.

The expression for the surface is

$$R = 0.1018 + 0.0088C - 0.238D \\ -0.0025C^2 - 0.1037CD - 2.771D^2, \qquad (28)$$

where C, R, and D are concealability, rate, and distortion calculated from (10), (12), and (11), respectively. We obtain this equation by modeling R as a polynomial function of C and D. Then, we varied the degrees of freedom on both C and D to obtain the best fitting that yielding the minimum fitting error. We used the curve fitting toolbox in Matlab to implement this process. Similar approaches will be applied to obtain the tradeoff surfaces for the higher secondary quality factor case.

In (28), for a fixed C, R decreases with D, which matches the property of conventional $R-D$ curve. The $C-D$ tradeoff for a certain R is that increasing C will increase D. When D is fixed, by a little calculation on (28) we find that for most of the cases where $D < 0.037$, R increases with C. In this case, there exists a $R-C$ tradeoff, where increasing concealability will increase the rate. We note that this $R-C$ tradeoff is different from our previously mentioned surprising result, where increasing anti-forensic strength results in increase on the concealability and decrease on the rate. The former is a tradeoff for a certain distortion value, while the latter implies changes on distortion with the increase of anti-forensic strength.

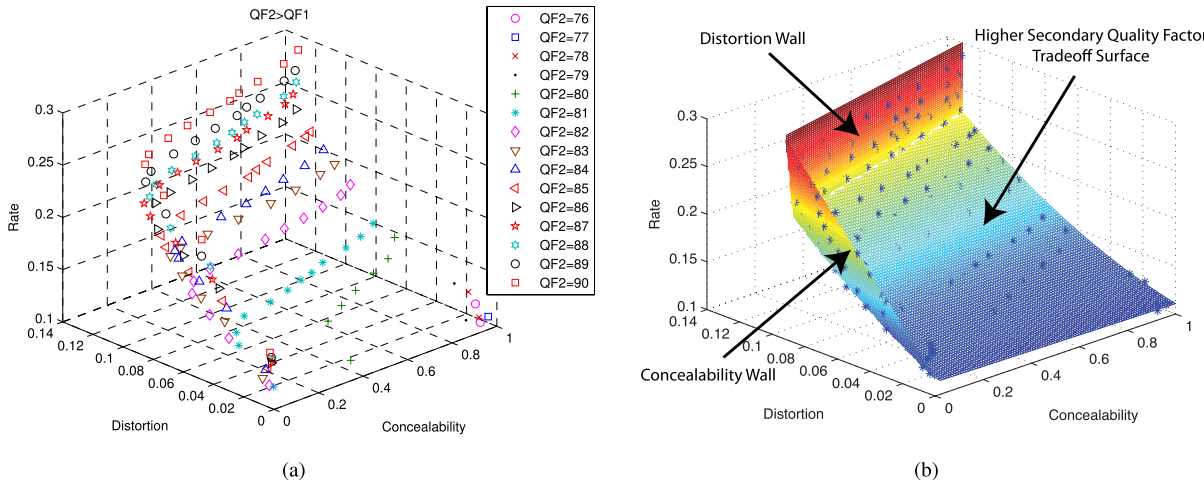
C. C-R-D Tradeoff for Higher Secondary Quality Factors

To characterize the C-R-D tradeoff for higher secondary quality factors, we plot the rest triple points obtained by using higher secondary quality factors in Fig. 9(a). Again, different markers represent different secondary quality factors. Each marker has several points obtained by using different anti-forensic strengths. Among them, the one with higher concealability implies that more anti-forensic strength has been applied to get this point. In this tradeoff, the reachable points of concealability, rate, and distortion depict three surfaces, which we use polynomial surfaces to fit.

As it is shown in Fig. 9(b), the main tradeoff surface for higher secondary quality factor is expressed as

$$R = 0.1146 - 0.0038C + 0.5474D - 0.15CD + 3.738D^2. \qquad (29)$$

In this tradeoff, the $R-D$ tradeoff for a certain C is that the increase rate will also increase distortion. It is inconsistent with the conventional $R-D$ tradeoff, where distortion is reduced by the increase of data rate. This phenomenon happens due to the fact that, in higher secondary quality factor case, anti-forensic modification introduces much more distortion than recompression. Specifically, when using higher secondary quality factors, as the quality factor increases, double compression fingerprints will be more obvious and harder to conceal. Thus, more anti-forensic modification is needed to achieve the expected concealability. This results in the increase of distortion for higher secondary quality factor and consequently higher rate. From the expression, we can



(a) (b)

Fig. 9. Tradeoff of concealability, rate, and distortion for the higher secondary quality factor case. (a) plots the R-D-C points. Points with the same marker and same color are those obtained by using the same secondary quality factor but different anti-forensic strengths. (b) is the polynominal fitting surfaces of (a).

find the $R-C$ tradeoff for a fixed D is that increasing C will decrease R. This is also a result due to the distortion of the anti-forensic modification: when C increases, it implies that more anti-forensic strength has been applied, and thus more distortion has been introduced by anti-forensic modification. Then, in order to keep D unchanged, the distortion from recompression must be reduced, which means the secondary quality factor should be closer to the first quality factor. Since $Q_2 > Q_1$, it results in a lower R. Additionally, when we fix R, D will increase with higher C.

Besides the higher secondary quality factor tradeoff surface, there are two walls along the concealability axis and distortion axis. Which we call the concealability wall:

$$R = 0.1378 - 2.0084C + 2.9504D, \tag{30}$$

and the distortion wall:

$$R = 39.7255 + 118.4314C - 392.1569D. \tag{31}$$

The concealability wall is generated for small anti-forensic strengths. Specifically, because the double compression fingerprints for $Q_2 > Q_1$ is very distinctive, when anti-forensic strength is small, the increase on anti-forensic strength hardly changes C. However, the distortion introduced by anti-forensic modification increases proportionally with the strength, and thus it leads to the increase of R and D. Therefore, while R and D are increasing, the little change on C results in the concealability wall. The distortion wall happens for much higher quality factors, where recompression distortion decreases with finer quantization, i.e., higher quality factor, but anti-forensics distortion increases with higher quality factor. Thus, the summation of these two distortions results in the little change on overall distortion and the distortion wall appears.

When comparing the higher secondary quality factor tradeoff with the lower secondary quality factor tradeoff, we notice that the lower secondary quality factor tradeoff locates entirely below the higher secondary quality factor tradeoff, as it is shown in Fig. 6. This implies that using a lower secondary quality factor can achieve the same concealability and distortion as the one obtained by using a higher quality factor, while the rate is lower. Note that we consider the data rate in this paper, which is inversely proportional to the compression rate. Thus, such phenomenon induces the forger to choose a lower secondary quality factor rather than a higher one to obtain a lower rate without increasing the distortion or decreasing the concealability. This surprising behavior happens because that the anti-forensic modification introduces much more distortion in higher secondary quality factor case than in lower secondary quality factor case. Since double compression fingerprints are more obvious in higher secondary quality factor case than in the lower one, in order to achieve the same concealability, anti-forensic modification will introduce much more distortion when the forger decides to use a higher secondary quality factor. Thus, to achieve a certain concealability, using higher secondary quality factors will not only results in more distortion but also higher rate than the case of using lower secondary quality factors. As a consequence, the forger will always tend to use a lower secondary quality factor rather than a higher one.

VII. Conclusion

In this paper, we proposed a concealability-rate-distortion tradeoff in anti-forensic systems. Specifically, we defined concealability and characterized the C-R-D tradeoff in double JPEG compression anti-forensics. To obtain the tradeoff, we proposed a flexible anti-forensic dither to vary the strength of anti-forensics. We also provided an anti-forensic transcoder to more efficiently accomplish the tasks of anti-forensics and recompression. We then experimentally characterized the C-R-D tradeoff by polynomial surfaces regarding whether the secondary quality factor is lower or higher than the first one. From the experimental results, we found two surprising results. The first one is that if the forger recompresses using a lower secondary quality factor, applying anti-forensics with greater

strength will decrease the data rate. The second one is that the forger is always incentivized to recompress using a lower secondary quality factor. This is because our results have shown that, for any pairing of concealability and distortion values achieved by a higher secondary quality factor, the forger can choose a lower secondary quality factor that will achieve the same concealability and distortion values yet at a lower data rate.

REFERENCES

[1] M. C. Stamm, M. Wu, and K. J. R. Liu, "Information forensics: An overview of the first decade," *IEEE Access*, vol. 1, pp. 167–200, May 2013.

[2] X. Chu, M. C. Stamm, W. S. Lin, and K. J. R. Liu, "Forensic identification of compressively sensed images," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2012, pp. 1837–1840.

[3] A. Swaminathan, M. Wu, and K. J. R. Liu, "Component forensics," *IEEE Signal Process. Mag.*, vol. 26, no. 2, pp. 38–48, Mar. 2009.

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

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

[6] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," *IEEE Trans. Image Process.*, vol. 12, no. 2, pp. 230–235, Feb. 2003.

[7] H. Farid, "Digital image ballistics from JPEG quantization," Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2006-583, 2006.

[8] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 758–767, Feb. 2005.

[9] M. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 492–506, Sep. 2010.

[10] M. Kirchner and J. Fridrich, "On detection of median filtering in digital images," *Proc. SPIE*, vol. 7541, p. 754110, Jan. 2010.

[11] H. Farid, "Image forgery detection," *IEEE Signal Process. Mag.*, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[12] A. C. Popescu and H. Farid, "Statistical tools for digital forensics," in *Proc. 6th Int. Workshop Inf. Hiding*, Toronto, ON, Canada, 2004, pp. 128–147.

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

[14] J. Lukáš, and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. Digital Forensic Res. Workshop*, Cleveland, OH, USA, Aug. 2003, pp. 5–8.

[15] D. Fu, Y. Q. Shi, and W. Su, "A generalized Benford's law for JPEG coefficients and its applications in image forensics," *Proc. SPIE*, vol. 6505, pp. 65051L-1–65051L-11, Feb. 2007.

[16] X. Feng and G. Doërr, "JPEG recompression detection," *Proc. SPIE*, vol. 7541, pp. 75410J-1–75410J-10, Feb. 2010.

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

[18] B. Mahdian and S. Saic, "Detecting double compressed JPEG images," in *Proc. 3rd Int. Conf. Crime Detection Prevention*, Dec. 2009, pp. 1–6.

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

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

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

[22] S. Milani, M. Tagliasacchi, and S. Tubaro, "Discriminating multiple JPEG compression using first digit features," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2012, pp. 2253–2256.

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

[24] W. Fan, K. Wang, F. Cayre, and Z. Xiong, "A variational approach to JPEG anti-forensics," in *Proc. IEEE ICASSP*, May 2013, pp. 3058–3062.

[25] M. Barni, M. Fontani, and B. Tondi, "A universal technique to hide traces of histogram-based image manipulations," in *Proc. Multimedia Security*, 2012, pp. 97–104.

[26] P. Comesana-Alfaro and F. Perez-Gonzalez, "Optimal counterforensics for histogram-based forensics," in *Proc. IEEE ICASSP*, May 2013, pp. 3048–3052.

[27] Z. Qian and X. Zhang, "Improved anti-forensics of JPEG compression," *J. Syst. Softw.*, vol. 91, pp. 100–108, May 2014.

[28] H. Li, W. Luo, and J. Huang, "Anti-forensics of double jpeg compression with the same quantization matrix," in *Multimedia Tools and Applications*. New York, NY, USA: Springer-Verlag, 2014, pp. 1–16.

[29] Z.-H. Wu, M. C. Stamm, and K. J. R. Liu, "Anti-forensics of median filtering," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, May 2013, pp. 3043–3047.

[30] 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.

[31] G. Cao, Y. Zhao, R. Ni, and H. Tian, "Anti-forensics of contrast enhancement in digital images," in *Proc. 12th ACM Workshop Multimedia Security*, 2010, pp. 25–34.

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

[33] M. Goljan, J. Fridrich, and M. Chen, "Sensor noise camera identification: Countering counter-forensics," *Proc. SPIE*, vol. 7541, pp. 75410S-1–75410S-12, Jan. 2010.

[34] G. Valenzise, M. Tagliasacchi, and S. Tubaro, "Revealing the traces of JPEG compression anti-forensics," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 2, pp. 335–349, Feb. 2013.

[35] S. Lai and R. Böhme, "Countering counter-forensics: The case of JPEG compression," in *Information Hiding* (Lecture Notes in Computer Science), vol. 6958, T. Filler, T. Pevný, S. Craver, and A. Ker, Eds. Berlin, Germany: Springer-Verlag, 2011, pp. 285–298. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-24178-9_20

[36] H. Li, W. Luo, and J. Huang, "Countering anti-JPEG compression forensics," in *Proc. 19th IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2012, pp. 241–244.

[37] A. Ortega and K. Ramchandran, "Rate-distortion methods for image and video compression," *IEEE Signal Process. Mag.*, vol. 15, no. 6, pp. 23–50, Nov. 1998.

[38] G. J. Sullivan and T. Wiegand, "Rate-distortion optimization for video compression," *IEEE Signal Process. Mag.*, vol. 15, no. 6, pp. 74–90, Nov. 1998.

[39] B. Foo, Y. Andreopoulos, and M. van der Schaar, "Analytical rate-distortion-complexity modeling of wavelet-based video coders," *IEEE Trans. Signal Process.*, vol. 56, no. 2, pp. 797–815, Feb. 2008.

[40] Z. He, Y. Liang, L. Chen, I. Ahmad, and D. Wu, "Power-rate-distortion analysis for wireless video communication under energy constraints," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 15, no. 5, pp. 645–658, May 2005.

[41] Y. Chen, W. S. Lin, and K. J. R. Liu, "Risk-distortion analysis for video collusion attacks: A mouse-and-cat game," *IEEE Trans. Image Process.*, vol. 19, no. 7, pp. 1798–1807, Jul. 2010.

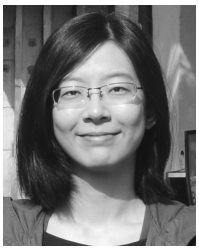
[42] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still Image Data Compression Standard*. New York, NY, USA: Van Nostrand, 1993.

[43] E. Y. Lam and J. W. Goodman, "A mathematical analysis of the DCT coefficient distributions for images," *IEEE Trans. Image Process.*, vol. 9, no. 10, pp. 1661–1666, Oct. 2000.

[44] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Mining Knowl. Discovery*, vol. 2, no. 2, pp. 121–167, 1998.

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

[46] G. Schaefer and M. Stich, "UCID: An uncompressed color image database," *Proc. SPIE*, vol. 5307, pp. 472–480, Dec. 2004.



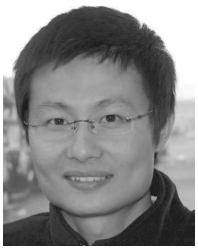
Xiaoyu Chu (S'11) received the B.S. degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2010. She is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of Maryland at College Park, College Park, MD, USA. Her research interests are in the area of information security, multimedia forensics, and antiforensics.

Ms. Chu received the First Prize in the 22nd Chinese Physics Olympiad, the Best Thesis Award of Shanghai Jiao Tong University, the Honor of Excellent Graduate of Shanghai Jiao Tong University, and the University of Maryland at College Park Future Faculty Fellowship in 2013.

Matthew Christopher Stamm (S'08–M'12) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the University of Maryland at College Park, College Park, MD, USA, in 2004, 2011, and 2012, respectively.

He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA, USA. His research interests include signal processing and information security with a focus on digital multimedia forensics and antiforensics.

Dr. Stamm was a recipient of the Dean's Doctoral Research Award from the A. James Clark School of Engineering, University of Maryland at College Park, in 2012. From 2004 to 2006, he was a Radar Systems Engineer with the Johns Hopkins University Applied Physics Laboratory, Laurel, MD, USA.



Yan Chen (SM'14) received the bachelor's degree from the University of Science and Technology of China, Hefei, China, in 2004, the M.Phil. degree from the Hong Kong University of Science and Technology, Hong Kong, in 2007, and the Ph.D. degree from the University of Maryland at College Park, College Park, MD, USA, in 2011. His current research interests are in data science, network science, game theory, social learning and networking, and signal processing and wireless communications.

Dr. Chen was a recipient of multiple honors and awards, including the best paper award from the IEEE GLOBECOM in 2013, the Future Faculty Fellowship and the Distinguished Dissertation Fellowship Honorable Mention from the Department of Electrical and Computer Engineering in 2010 and 2011, respectively, the Finalist of Dean's Doctoral Research Award from the A. James Clark School of Engineering, University of Maryland at College Park, in 2011, and the Chinese Government Award for outstanding students abroad in 2011.

K. J. Ray Liu (F'03) was named as a Distinguished Scholar-Teacher with the University of Maryland at College Park, College Park, MD, USA, in 2007, where he is currently a Christine Kim Eminent Professor of Information Technology. He leads the Maryland Signals and Information Group, where he conducting research encompassing broad areas of signal processing and communications with recent focus on cooperative and cognitive communications, social learning and network science, information forensics and security, and green information and communications technology.

He was a recipient of the IEEE Signal Processing Society Award in 2014, the IEEE Signal Processing Society Technical Achievement Award in 2009, and best paper awards from various IEEE societies and EURASIP. He received teaching and research recognitions from the University of Maryland at College Park, including the university-level Invention of the Year Award, and the college-level Poole and Kent Senior Faculty Teaching Award, the Outstanding Faculty Research Award, and the Outstanding Faculty Service Award, all from the A. James Clark School of Engineering. He recognized by Thomson Reuters as an ISI Highly Cited Researcher. He is a fellow of the American Association for the Advancement of Science.

Dr. Liu was the President of the IEEE Signal Processing Society (2012–2013), where he has served as the Vice President-Publications and Board of Governor. He was the Editor-in-Chief of the *IEEE Signal Processing Magazine* and the Founding Editor-in-Chief of the *EURASIP Journal on Advances in Signal Processing*.