Detection and information theoretic measures for quantifying the distinguishability between multimedia operator chains

Pedro Comesaña #1

Signal Theory and Communications Department, University Vigo
E. E. Telecomunicación, Campus-Lagoas Marcosende, Vigo 36310, Spain
[1] pcomesan@gts.uvigo.es

***Abstract*—Despite the large number of contributions on forensics in the recent years, there is still a lack of fundamental limits on how easily two signal processing operators (or operator chains) can be distinguished. We take a first step in this direction by proposing the use of some detection and information theoretic measures that are suitable for assessing those fundamental limits. The optimality and the links between those measures are discussed; they are used for quantifying the distinguishability between different operator chains, considering the different prior knowledge that could be available at the forensics analyst. Although this work is mainly a theoretical motivation to the use of those measures in forensic applications, its particularization to three practical scenarios is illustrated.**

I. Introduction

Passive multimedia forensics has rapidly evolved in the last few years to face the challenge imposed by the quick spread of digital acquisition devices and the development of powerful editing tools, which allow even unskilled users to easily modify contents, with a dramatic general decline of trust in digital multimedia objects. Despite the flurry of forensic methods, in most cases the proposed solutions focus on very specific problems, such as the estimation of the resampling factor in resizing operations, or learning the quantization table in compressed images. As a consequence of this disparity, there is currently a lack of a general theory which would uncover the common grounds of forensic algorithms, and assess their fundamental performance limits. This lack has been recognized in the context of the European Project REWIND [1], which aims at developing a framework for the forensic analysis of signal processing operator chains in order to unveil the full topology (meaning the way in which elementary operators are interconnected) of operators a content has gone through.

The objective of this paper is to answer the following key question: to which extent the traces of a certain operator (or operator chain) can be reliably found in a given content? Related to this, is the following: what is the probability of success when trying to detect a processing operator chain? We address these two questions through the concept of *distinguishability* which is approached from both information-theoretic and detection-theoretic perspectives. Moreover, the framework here proposed has the advantage of including the prior (but not necessarily correct) assumptions on both the statistics of the contents and the possible operator chains made by the forensic analyst.

WIFS'2012, December, 2-5, 2012, Tenerife, Spain. 978-1-4244-9080-6/10/$26.00

To the best of our knowledge, the only other work that tackles a forensic problem from a fundamental perspective is [2], where source identification is treated as a game between the analyst and an adversary who modifies the content as little as possible to make it look as if it were produced by a different source. In our work, we are interested in estimating the operator processing chain instead of identifying the source; this requires a different approach where the possible existence of a meaningful game is secondary to being able to correctly learning the operator topology.

Even though our approach is fundamental in spirit, we will illustrate how it can be particularized to practical scenarios. By no means we try to propose practical algorithms for such cases, but simply assess the difficulties that the development of those algorithms would entail, which are adequately summarized by our measures. However, the properties (e.g., multimodality, gradient) of the proposed measures provide useful clues for designing practical forensic estimation and detection methods.

The remaining of this paper is organized as follows: previous approaches to multimedia forensics problems, paying special attention to JPEG and double JPEG quantization, are summarized in Sect. II; the proposed measures, and the links between them are presented in Sect. III. Sect. IV introduces the use of such measures to deal with different frameworks depending on the knowledge available to the forensics analyst; the links between those strategies and maximum likelihood operator parameter estimation are also highlighted there, while Sect. V presents some experimental results on three relevant practical scenarios. Finally, Sect. VI summarizes the main conclusions of this work and discusses future lines.

II. Previous multimedia forensics proposals

In this section we give a brief overview of some state-of-the-art forensics methods dealing with quantization; our interest in that operator is related to the scenarios analyzed in Sect. V, which in turn are just an example of the applicability of the measures we propose to use in forensics: a) Quant. + AWGN (additive white Gaussian noise), b) Quant. + Quant., c) Quant. + Quant. + Quant.. In any case, by no means we try to be exhaustive, but simply provide a rough picture of some of the solutions that have been proposed in the last years, emphasizing their ad-hoc and/or heuristic nature.

One of the first works in the literature dealing with the single quantization detection and estimation is due to Fan and Queiroz [3], where the detection statistic depends on the difference between the histogram of the pixel differences across blocks and within blocks. Once the quantization is detected, a Maximum Likelihood (ML) estimator, based on assuming that the AC DCT coefficients follow a Laplacian distribution, is used for estimating the quantization step. A completely different approach was proposed by Lin *et al.* in [4], where in order to check the suitability of a candidate transform, the authors try to estimate the pdf of the original (unquantized) coefficients by interpolating the histogram of the observed coefficients, and then compute the normalized correlation between this pdf approximation and the observed histogram; if the obtained value is high, then the considered transform will likely be the one used in coding. In another relevant work [5], the variability of the integral of the AC DCT coefficients in different intervals is exploited in order to detect the quantization artifacts; the same idea is then used to determine the transform encoder.

Concerning double quantization, in [6] Lukas and Fridrich propose a method for estimating the first quantization matrix; they study some characteristic features that appear in DCT coefficient histograms when those coefficients are quantized; although several strategies are proposed, the most successful one is based on neural networks. An alternative approach is proposed by Fu *et al.* in [7], where a generalized version of Benford's law is exploited for JPEG detection and estimation, and double JPEG detection. In another proposal, Luo *et al.* [8] study the blocking artifacts introduced by mis-aligned double JPEG coding; with the help of a SVM that information is used to determine if an image is a JPEG original or it was cropped from other JPEG image and re-saved as JPEG. The non-aliged double JPEG artifacts on the pdf of the DCT coefficients is exploited in [9] for locating image forgeries.

III. Distinguishability measures

The target of this work is to defend the use of some already known measures (although so far not exploited in forensics) for dealing with a wide range of chains of operators, i.e., reliably determining if a multimedia content has gone through an arbitrary chain of operators which are arranged in a particular ordering and topology. We also want to quantify how easily two different chains of operators (characterized by their ordering and topology, and where in some circumstances additional knowledge on the operator parameters is assumed) can be distinguished; the dual question to this problem can be written in terms of how many samples of multimedia contents are required to reliably determine the processing a test content has gone through. Furthermore, we want our proposal to follow some optimality criterion, as for example minimizing the false positive probability (i.e., determining that the considered content has gone through a given operator chain, when it has not) for a given false negative probability (i.e., saying that the content has not undergone a given operator chain, when indeed it has). Finally, it is also desirable the detection scheme to be blind, meaning that deterministic knowledge of the original multimedia content should not be required, although some kind of *a priori* information about the original statistical distribution will typically be assumed to be known.

Based on these requirements, the use of two different measures is proposed for distinguishing operator chains.

A. Detection theoretic measure

From a detection theory point of view the problem of determining which distribution out of two possible candidates produced a given observation, is modeled as a binary hypothesis test; it is well known that the most powerful test (i.e., that one minimizing the probability of false positive for a given false negative probability) in that scenario is given by the Neyman-Pearson Lemma, which uses the likelihood-ratio between the so-called null hypothesis (denoted by θ_0) and the alternative hypothesis (denoted by θ_1), i.e., $\Lambda(\mathbf{x}) = \frac{p(\theta_0|\mathbf{X})}{p(\theta_1|\mathbf{X})}$, where $\mathbf{x}$ denotes the n-dimensional signal under test. Assuming that *a priori* information about the different hypothesis is not available, the former ratio is equivalent to $\text{LLR}(\mathbf{x}) = \log\left(\frac{p(\mathbf{X}|\theta_0)}{p(\mathbf{X}|\theta_1)}\right)$, for the case where $\mathbf{x}$ belongs to a discrete alphabet and $\text{LLR}(\mathbf{x}) = \log\left(\frac{f(\mathbf{X}|\theta_0)}{f(\mathbf{X}|\theta_1)}\right)$, for the continuous scenario, where $p(\cdot)$ is used for denoting probability mass functions (pmfs), and $f(\cdot)$ for probability density functions (pdfs). For the sake of notational simplicity we will use $f(\mathbf{x}|\theta_i) = f_i(\mathbf{x})$, and $p(\mathbf{x}|\theta_i) = p_i(\mathbf{x})$.

Be aware that θ_0 and θ_1 define the considered operator chain topology (i.e., how the operators are linked, in parallel or series) and ordering, as well as the specific parameters characterizing each operator. Therefore, the generality objective is achieved by this measure, as it can be useful, among others, for detecting:

- the ordering and topology of the operator chain whenever a fixed set of operators, each of them using fixed parameters, is considered;
- the presence of different operators in chains sharing the same topology;
- the use of different operator parameters in processing chains using the same operators with common ordering and topology;
- combinations of the previous scenarios.

B. Information theoretic measure

Concerning information theoretic measures devoted to quantify the differences between two different pdfs/pmfs, probably the most used choice is the Kullback-Leibler divergence (a.k.a. Kullback-Leibler distance and relative entropy). This measure was proposed, for example, for quantifying the statistic detectability of the watermark embedding in steganographic applications [10]. For the discrete case it is defined as,

$$D(p_0||p_1) = \sum_{\mathbf{x}\in\mathcal{X}} p_0(\mathbf{x}) \log\left(\frac{p_0(\mathbf{x})}{p_1(\mathbf{x})}\right),$$

where $\mathcal{X}$ is the discret alphabet where $\mathbf{x}$ takes values, and

$$D(f_0||f_1) = \int_{\mathbb{R}^n} f_0(\mathbf{x}) \log\left(\frac{f_0(\mathbf{x})}{f_1(\mathbf{x})}\right) d\mathbf{x},$$

for the continuous case. It is worth pointing out that the KLD is non-negative, being null if and only if the two considered distributions are the same almost everywhere.

The intuitive interpretation of this measure is very clear: the closer two distributions are, the smaller their KLD is. In the context of our problem a small but positive KLD implies that it will be difficult to distinguish the compared operator chains, or alternatively, that a large number of observations will be required in order to reliably determine the operator chain undergone by the content. Indeed, if the KLD were null, then the two operator chains could not be distinguished at all. Of course, the same considerations made about the generality of the LLR also apply here.

C. Links between the two proposed measures and error probabilities

Since the use of two different measures is proposed, one may wonder how they are linked, if at all. It is a well-known result that the relative entropy version of the Asymptotic Equipartition Property establishes that if $\mathbf{X}$ is a sequence of random variables drawn i.i.d. according to $p_0(\mathbf{x})$, then $\frac{1}{n}\log\left(\frac{p_0(\mathbf{X})}{p_1(\mathbf{X})}\right) \to D(p_0||p_1)$, where convergence takes place in probability [11]. In plain words, this result shows that when the contents produced under the null hypothesis are i.i.d. and the dimensionality of the considered problem goes to infinity, then the two measures we have proposed in the previous sections to be used in forensic applications are asymptotically equivalent. This confirms that both measures are good candidates for quantifying the distinguishability between different operator chain topologies, and/or operator chains with different operator parameters, providing a coherent framework.

Additionally, the Chernoff-Stein Lemma [11] states that the false positive probability error exponent achievable for a given non-null false negative probability asymptotically converges to $D(p_0||p_1)$ (as long as that measure takes a finite value) when the dimensionality of the problem goes to infinity. Therefore, the intuitive idea behind the application of this lemma to our problem is straightforward: the larger the differences between the considered pdfs/pmfs, the smaller the probability of confusing the related operator chains.

IV. Using the Proposed Measures

In this work the systematic use of the two (asymptotically equivalent) measures mentioned above in forensics applications is proposed. In this section we describe how these measures can be used for dealing with a number of different forensic scenarios; the links with estimation criteria in the literature, specifically with ML, are also discussed.

Based on the characteristics of the proposed measures, we will look for that operator chain providing a theoretical pdf of its output which is at a minimal distance (the LLR or the KLD) of the empirical pdf (i.e., the histogram of the considered content, which is the null hypothesis pdf). This framework also allows to deal with knowledge that is *assumed* by the forensics analyst, although he/she could be wrong. Specifically, if we denote by $\xi \in \Xi$ the operator chain topology and parameter values which are *assumed true* by the forensics analyst, by $\psi \in \Psi$ the operator chain topology and parameter values which are unknown by the analyst, by $\gamma \in \Gamma$ the original signal characteristics assumed by the analyst, and by $\phi \in \Phi$ the unknown ones, then the task of estimating the processing may be formalized as

$$\hat{\psi}_0 = \arg\min_{\psi_1\in\Psi_1}\min_{\phi_1\in\Phi_1} D(f(\mathbf{x}|\xi_0,\psi_0,\gamma_0,\phi_0)||f(\mathbf{x}|\xi_1,\psi_1,\gamma_1,\phi_1)), \quad (1)$$

where the subindex 0 stands for the null hypothesis, meaning the distribution parameters which have actually produced the content under analysis, and 1 stands for the alternative hypothesis, which in our problem is the test distribution. Note that whenever $\psi_0 \in \Psi_1$, $\phi_0 \in \Phi_1$, $\xi_0 = \xi_1$, and $\gamma_0 = \gamma_1$, at least one point exists where the theoretical KLD and the LLR are null (and the KLD with the histogram, asymptotically null).

For the sake of illustration we introduce a JPEG quantization table estimation problem. The forensics analyst tries to reduce the search computational cost by making some assumptions that allow him/her to reduce the search space. Specifically, the forensics analyst assumes that the non-quantized DCT coefficients follow a Laplacian distribution with unknown variance, and that YC_BC_R color transformation was used. Nevertheless, the non-quantized DCT coefficients of the considered content truly follow a Generalized Gaussian Distribution (GGD) with shaping parameter 0.7 (consequently, the forensics analyst will use mismatched knowledge, as he/she is assuming those coefficients to follow a Laplacian distribution) and variance 10, and it was quantized using the color space YIQ; the used quantization table corresponds to a Quality Factor (QF) of 70. In this case

- $\xi_1 =$ color space YC_BC_R
- $\xi_0 =$ color space YIQ
- $\gamma_1 =$ Laplacian-distributed DCT coefficients
- $\gamma_0 =$ GGD-distributed DCT coefficients with shaping parameter 0.7
- $\Psi_1 =$ the set of all possible quantization tables
- $\psi_0 =$ quantization table QF$= 70$
- $\Phi_1 = \mathbb{R}^+$
- $\phi_0 =$ variance of DCT coefficients $= 10$

Therefore, $\psi_0 \in \Psi_1$, $\phi_0 \in \Phi_1$, $\xi_0 \neq \xi_1$, and $\gamma_0 \neq \gamma_1$.

The forensics analyst could also assume a kind of operator (Ψ_1) completely different from that truly used to process the content (e.g., JPEG quantization, whenever $\psi_0 =$ average

3×3 filtering), or a wrong search space for the content parameters (e.g., he/she could assume that the input signal is GGD-distributed with shaping parameter in the interval $[1,2]$, so he/she will focus his/her search in that interval, while the shaping parameter truly modeling the input signal is 0.5). The price to be paid for avoiding the use of wrong input signal characteristics and/or operator chain parameters is to skip the use of those *supposedly known* values if a reliable proof that they were indeed used is not available. In other words, a trade-off between computational cost and detection performance must be faced; the better the achievable performance (by avoiding the use of possibly wrong input signal and/or operator chain parameters), the larger the required computational cost.

Similarly to (1), if the LLR is used as target function, then the estimation of the operator chain can be formalized as

$$\hat{\psi}_0 = \arg \min_{\psi_1 \in \Psi_1} \min_{\phi_1 \in \Phi_1} \log \left(\frac{f(\mathbf{x}|\xi_0, \psi_0, \gamma_0, \phi_0)}{f(\mathbf{x}|\xi_1, \psi_1, \gamma_1, \phi_1)} \right). \quad (2)$$

Although both the optimizations in (1) and (2) seem to make sense from a rather heuristic point of view, as one is trying to find the closest distribution (in the set of feasible alternative distributions) to that corresponding to the null hypothesis, one aspect that deserves our attention is the relationship between the proposed estimators and classical strategies in estimation theory. Interestingly, (2) describes the ML estimation criterion, i.e., since the null hypothesis is fixed, one is trying to find the parameters that maximize the probability of the observed content. Moreover, as the KLD and the LLR are asymptotically equivalent when the dimensionality of the problem goes to infinity, in this case the parameter estimation based on the KLD will be also equivalent to the ML criterion. If *a priori* information about the parameters to be estimated were available, then (2) could be replaced by its MAP counterpart.

Finally, note that

$$\min_{\psi_1 \in \Psi_1} \min_{\phi_1 \in \Phi_1} D(f(\mathbf{x}|\xi_0, \psi_0, \gamma_0, \phi_0) || f(\mathbf{x}|\xi_1, \psi_1, \gamma_1, \phi_1)),$$

and

$$\min_{\psi_1 \in \Psi_1} \min_{\phi_1 \in \Phi_1} \log \left(\frac{f(\mathbf{x}|\xi_0, \psi_0, \gamma_0, \phi_0)}{f(\mathbf{x}|\xi_1, \psi_1, \gamma_1, \phi_1)} \right),$$

are useful tools for quantifying how easy it will be to separate the operator chain corresponding to the null hypothesis from the class of distributions defined by the parameters ξ_1 and γ_1, and the classes Ψ_1 and Φ_1; an application scenario of these measures is the case where one wants to discard the use of a given operator chain, for example, how easily one can discard the use of a linear filter when the observed image was really JPEG compressed with $QF = 80$.

Similarly, one can be interested in quantifying the distinguishability between two classes of operator chains defined by the parameters (ξ_0, γ_0) and (ξ_1, γ_1), and the classes (Ψ_0, Φ_0) and (Ψ_1, Φ_1) (denoted in general by $\mathcal{C}(\Psi_i, \Phi_i, \xi_i, \gamma_i)$) by using,

$$d_1(\mathcal{C}(\Psi_0, \Phi_0, \xi_0, \gamma_0), \mathcal{C}(\Psi_1, \Phi_1, \xi_1, \gamma_1)) \triangleq \min_{(\psi_0, \phi_0) \in \Psi_0 \times \Phi_0} \min_{(\psi_1, \phi_1) \in \Psi_1 \times \Phi_1} D(f(\mathbf{x}|\xi_0, \psi_0, \gamma_0, \phi_0) || f(\mathbf{x}|\xi_1, \psi_1, \gamma_1, \phi_1)), \quad (3)$$

or

$$d_2(\mathcal{C}(\Psi_0, \Phi_0, \xi_0, \gamma_0), \mathcal{C}(\Psi_1, \Phi_1, \xi_1, \gamma_1)) \triangleq \min_{(\psi_0, \phi_0) \in \Psi_0 \times \Phi_0} \min_{(\psi_1, \phi_1) \in \Psi_1 \times \Phi_1} \log \left(\frac{f(\mathbf{x}|\xi_0, \psi_0, \gamma_0, \phi_0)}{f(\mathbf{x}|\xi_1, \psi_1, \gamma_1, \phi_1)} \right). \quad (4)$$

In this case these measures can be used, for example, for quantifying how easily a linear filtering processing (Ψ_1) can be distinguished from a JPEG quantization (Ψ_0), for a given input signal model ($\Phi_0 = \Phi_1$).

It is worth noting that these measures resemble the definition of the distance between two sets as the minimum distance between any pair of points belonging to each of those sets. Be also aware that most of works in the literature deal with the distinguishability among operators in a same class, so this powerful possibility of distinguishability between classes is, to the best of authors knowlege, proposed for the first time.

Clearly, the criteria in (3) and (4) are different of those in

$$\max_{(\psi_0, \phi_0) \in \Psi_0 \times \Phi_0} \min_{(\psi_1, \phi_1) \in \Psi_1 \times \Phi_1} D(f(\mathbf{x}|\xi_0, \psi_0, \gamma_0, \phi_0) || f(\mathbf{x}|\xi_1, \psi_1, \gamma_1, \phi_1)), \quad \text{or}$$

$$\max_{(\psi_0, \phi_0) \in \Psi_0 \times \Phi_0} \min_{(\psi_1, \phi_1) \in \Psi_1 \times \Phi_1} \log \left(\frac{f(\mathbf{x}|\xi_0, \psi_0, \gamma_0, \phi_0)}{f(\mathbf{x}|\xi_1, \psi_1, \gamma_1, \phi_1)} \right).$$

In the latter case we are comparing the probabilities of the considered observations according to the probability distributions using the ML estimators in both classes (namely, $\mathcal{C}(\Psi_0, \Phi_0, \xi_0, \gamma_0)$ and $\mathcal{C}(\Psi_1, \Phi_1, \xi_1, \gamma_1)$). This last measure would be of interest when one wishes to compare the most probable cases of those two classes. For the KLD case, the same interpretation may be asymptotically done when the dimensionality of the problem goes to infinity.

V. Analyzed Scenarios

In this section the operator parameters used for generating the considered samples (i.e., those corresponding to the null hypothesis) will be denoted by the subindex 0, while 1 will refer to the tested values (corresponding to the alternative hypothesis). In case that a subindex were already used for denoting the corresponding parameter (e.g., Δ_i), a second subindex will be added for denoting the null or alternative hypothesis (i.e., $\Delta_{i,j}$). In all the three considered scenarios the variance of the content is equal to 200. Theoretical expressions for the considered pdfs/pmfs have been derived, although they are not included here due to the lack of space.

A. Scenario 1: Quantization and AWGN

- Operator chain description: a scalar quantizer followed by the addition of AWGN.
- Application scenarios: detecting quantization in the transformed domain whenever the pixels of the quantized image are rounded; characterizing full-frame filtering of blockwise quantized images. The AWGN models the pixel rounding noise in the transformed domain, and the contributions of the pixels of the surrounding blocks, respectively
- Known/unknown parameters: since the quantization is assumed to be performed in a transformed domain known

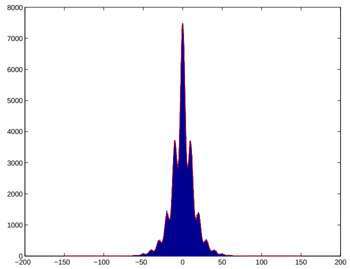

Fig. 1. Theoretical pdf vs. Histogram for Scenario 1. $\Delta_0 = 10$, $(\sigma_N^2)_0 = 10$, $n = 10^6$.

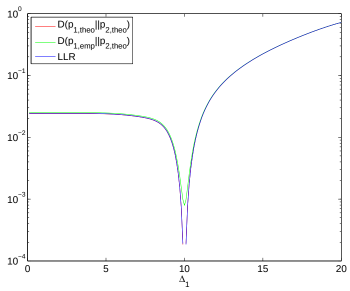

Fig. 2. Theoretical and empirical KLD and LLR for Scenario 1. $\Delta_0 = 10$, $(\sigma_N^2)_0 = (\sigma_N^2)_1 = 10$, $n = 10^7$.

by the forensics analyst (e.g., the 8×8 DCT domain for JPEG quantization), the original signal will be modeled by a zero-mean Laplacian. Although in the results reported in this paper we will assume its variance to be known, it could be also estimated by using (1) or (2). The operator chain parameters to be estimated will be the quantization step Δ and the AWGN variance σ_N^2.

- Obtained results: Fig. 1 compares the theoretical pdf (red line) and the sample histogram (for $n = 10^6$). Then, Fig. 2 ($n = 10^7$) compare $D(f_0||f_1)$ and $\text{LLR}(\mathbf{x})$ when $(\sigma_N^2)_1 = (\sigma_N^2)_0$, i.e., only variation with respect to Δ_1 is considered. For the Kullback-Leibler Divergence, the results for both the theoretical pdf (which is indeed quantized in order to compute this measure, so a pmf is really used) and the histogram (i.e., p_{emp}) for the null hypothesis are plotted. As expected, the minimum of the considered measures will be located at $\Delta_1 = \Delta_0$, being zero for the Kullback-Leiber Divergence when the theoretical pdf of the null hypothesis is considered, and for $\text{LLR}(\mathbf{x})$. Figs. 3, 4, and 5 show, respectively, the KLD between the theoretical pdf under the null hypothesis and the theoretical pdf under the alternative hypothesis, the KLD between the *empirical pdf* (the histogram) under the null hypothesis and the theoretical pdf under the alternative hypothesis, and the LLR. As expected, all the figures are similar, and they have the corresponding minimum located at $\Delta_1 = \Delta_0$ and $(\sigma_N^2)_1 = (\sigma_N^2)_0$.

B. Scenario 2: Double quantization

- Operator chain description: the considered content is scalar-quantized twice, and the latter quantization stepsize is known by the forensics analyst. Therefore, the target is

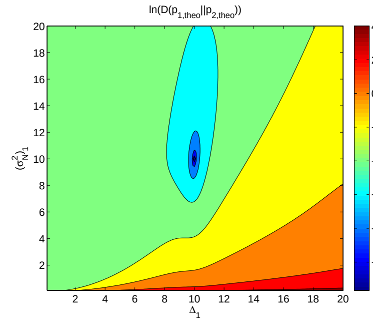

Fig. 3. Theoretical KLD for Scenario 1. $\Delta_0 = 10$, $(\sigma_N^2)_0 = 10$, $n = 10^7$.

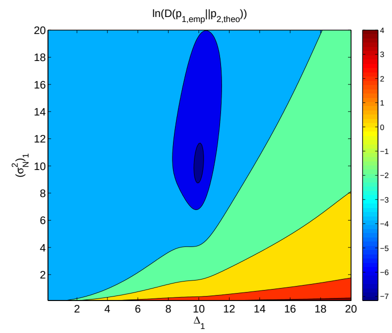

Fig. 4. Empirical KLD for Scenario 1. $\Delta_0 = 10$, $(\sigma_N^2)_0 = 10$, $n = 10^7$.

estimate the first quantization stepsize, similarly to [6].

- Application scenarios: double JPEG quantization estimation.
- Known/unknown parameters: due to the similarities with the previous scenario, we will model the content coefficients by a known-variance Laplacian. The first quantization step (Δ_1) is not available, so it is estimated following the proposed approach. The second quantization step (Δ_2) is assumed to be known; this is a realistic assumption, as the input format to the forensics analyst will typically be the result of the latter quantization.
- Obtained results: Fig. 6 shows the 3 measures already used in Fig. 2 for this scenario when $\Delta_{2,0} = \Delta_{2,1} = 9$ and $\Delta_{1,0} = 5$. As expected, the minimum of the considered target is located at $\Delta_{1,1} = \Delta_{1,0}$. Special attention should be paid to the discontinuities on the

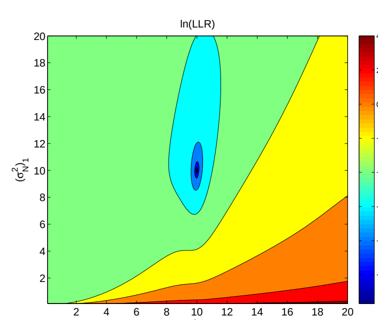

Fig. 5. LLR for Scenario 1. $\Delta_0 = 10$, $(\sigma_N^2)_0 = 10$, $n = 10^7$.

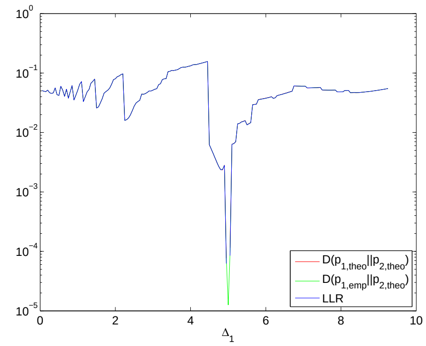

Fig. 6. Theoretical and empirical KLD and LLR for Scenario 2. $\Delta_{1,0} = 5, \Delta_{2,0} = \Delta_{2,1} = 9$, $n = 10^6$.

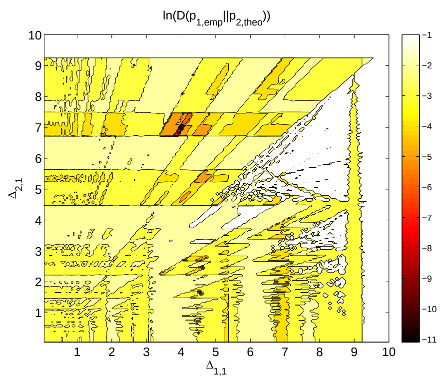

Fig. 7. Empirical KLD for Scenario 3. $\Delta_{1,0} = 4$, $\Delta_{2,0} = 7$, $\Delta_{3,0} = \Delta_{3,1} = 9$, $n = 10^6$.

target functions, due to the quantization effect.

C. Scenario 3: Triple quantization

- Operator chain description: the content goes through three scalar quantizers connected in series. The last quantization stepsize is known.
- Application scenarios: this is a generalized version of the typically studied double JPEG quantization. The real target of this scenario is to illustrate the power of the proposed distinguishability measures.
- Known/unknown parameters: similarly to the two previous scenarios, the input signal is assumed to be Laplacian of known variance. The first two quantization steps (respectively Δ_1 and Δ_2) are not known, but the third one (Δ_3) is available at the forensics analyst.
- Obtained results: the results for this case are shown in Fig. 7, where the KLD using the empirical pdf under the null hypothesis and its alternative hypothesis theoretical counterpart are plotted. Again, the minimum of the considered target function is located at $\Delta_{1,1} = \Delta_{1,0}$ and $\Delta_{2,1} = \Delta_{2,0}$. Similarly to scenario 2, the discontinuities due to quantization can be clearly observed.

Other signal processing scenarios are studied in [12], where some examples of undetectable manipulations within a class of manipulations are presented.

VI. Conclusions and future work

In this work the use of two measures is proposed to determine the fundamental limits on the distinguishability between processing operator chains, as well as between classes of processing operator chains. Based on those criteria, optimal or simplified near-optimal detectors can be defined. Additionally, in game theoretic frameworks the proposed measures may be used by attackers for designing smart attacks where constraints (for instance, on the introduced distortion) can be introduced [2]. Future lines include the summarization of the plots shown in this paper in a kind of ROC curve (false negative vs. false positive error probabilities), the consideration of *a priori* information about the original signal and system parameters, the consideration of more operator chain scenarios, and performing experiments with real images, comparing the achieved results with those of existing schemes in the literature.

Acknowledgments

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

References

[1] http://www.rewindproject.eu/.

[2] M. Barni, “A game theoretic approach to source identification with known statistics,” in *Proc. of the IEEE ICASSP*, Kyoto, Japan, March 2012.

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

[4] W. S. Lin, S. K. Tjoa, H. V. Zhao, and K. J. R. Liu, “Digital image source coder forensics via intrinsic fingerprints,” *IEEE Transactions on Informations Forensics and Security*, vol. 4, no. 3, p. 460, September 2009.

[5] W. Luo, Y. Wang, and J. Huang, “Detection of quantization artifacts and its applications to transform encoder identification,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 810–815, December 2010.

[6] J. Lukas and J. Fridrich, “Estimation of primary quantization matrix in double compressed JPEG images,” in *Proc. of DFRWS*, 2003.

[7] D. Fu, Y. Q. Shi, and W. Su, “A generalized Benford’s law for JPEG coefficients and its applications in image forensics,” in *Proc. SPIE 6505*, vol. 6505, San Jose, CA, January 2007, p. 65051L.

[8] W. Luo, Z. Qu, J. Huang, and G. Qiu, “A novel method for detecting cropped and recompressed image block,” in *Proc. of the IEEE ICASSP*, Honolulu, HI, April 2007, pp. 217–220.

[9] T. Bianchi and A. Piva, “Analysis of non-aligned double JPEG artifacts for the localization of image forgeries,” in *Proc. of the IEEE WIFS*, Iguacu Falls, Brasil, December 2011.

[10] C. Cachin, “An information-theoretic model for steganography,” in *Information Hiding International Workshop*, ser. Lecture Notes in Computer Science, D. Aucsmith, Ed., vol. 1525. Portland, OR, USA: Springer, April 1998, pp. 306–318.

[11] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley, 2006.

[12] P. Comesaña and F. Pérez-González, “Multimedia operator chain topology and ordering estimation based on detection and information theoretic tools,” in *IWDW 2012 proceedings*, accepted.