Journal of Real-Time Image Processing (2019) 16:741–750
https://doi.org/10.1007/s11554-019-00860-3

SPECIAL ISSUE PAPER

Real-time detecting one specific tampering operation in multiple operator chains

Shangde Gao[1] · Xin Liao[1,2] · Xuchong Liu[2]

Received: 1 December 2018 / Accepted: 20 February 2019 / Published online: 2 March 2019

Abstract
Currently, many forensic techniques have been developed to determine the processing history of given multimedia contents. However, because of the interaction among tampering operations, there are still fundamental limits on the determination of tampering order and type. Up to now, a few works consider the cases where multiple operation types are involved in. In these cases, we not only need to consider the interplay of operation order, but also should quantify the detectability of one specific operation. In this paper, we propose an efficient information theoretical framework to solve this problem. Specially, we analyze the operation detection problem from the perspective of set partitioning and detection theory. Then, under certain detectors, we present the information framework to contrast the detected hypotheses and true hypotheses. Some constraint criterions are designed to improve the detection performance of an operation. In addition, Maximum-Likelihood Estimation (MLE) is used to obtain the best detector. Finally, a multiple chain set is examined in this paper, where three efficient detection methods have been proposed and the effectiveness of our framework has been demonstrated by simulations.

Keywords Image forensics · Operation chains · Resizing · Contrast enhancement · Median filter · Information theory

1 Introduction

Nowadays, digital images have been the main carriers transmitting and acquiring multimedia contents. With the rapid development of image editing software, digital multimedia contents can be easily manipulated and falsified. As a result, lots of tampered images have appeared in various fields such as news publication, scientific experiments, legal evidences, etc. Thus, it is hard to know whether the given multimedia content is trustful or maliciously tampered [1].

To combat this situation, digital forensics has emerged as an important research field with the applications of authenticity integrality verification for digital data. Digital forensics technology can be divided into active and passive types. By pre-embedding digital watermarks [2–4] or generating perceptual hashes [5], active forensics can prevent and verify possible image tampering. Passive forensics, also known as blind forensics, can be directly based on the digital image itself for authenticity discrimination, which has a better adaptability. Recently, many passive forensic techniques have been proposed to identify the use of different manipulation operations, such as scaling [6–9], contrast enhancement [10, 11], median filtering [12, 13], and so on [14, 15]. Furthermore, some researchers proposed the concept of universal forensics, i.e., identifying one specific operation of certain operation sets [16–18]. In [16], the authors used the difference histogram to structure the features set which can detect scaling, JEPG compression, and blurring operation effectively. By extracting statistical features of image in residual domain, Li et al. [17] achieved to determine some multiple single-operations. Different from the previous ones, authors in [18] proposed a method to distinguish JEPG compression, Gauss blurring, gamma correction, median filtering, and resampling in terms of image steganalysis.

Considering multiple manipulation operations may be used to create a forgery in reality, some state-of-art methods have been proposed for identifying one operation in a certain processing chain [19, 20]. Authors in [19] considered a scenario where linear contrast enhancement was interleaved with two compressions, then zero-height gaps are used to determine the trace left by contrast enhancement. In [20],

✉ Xin Liao
xinliao@hnu.edu.cn

[1] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China

[2] Key Laboratory of Network Crime Investigation of Hunan Provincial Colleges, Changsha 410138, China

an improved double compression detector was proposed for the processing chain of two compressions with resizing in between. Specifically, two hypotheses were considered: whether the image was single JPEG compressed, or it was double JPEG compressed with resizing applied in the middle.

While these techniques considered multiple operations, their goal is to identify the existence of one specific operation in a certain processing chain. Actually, by combining with each other in any ordering or topology, different operations will generate a wide-range operator chains [21]. Considering the interaction between multiple operator chains, Stamm et al. [22] focused on a scenario that the image was altered by contrast enhancement and resizing. To determine the order of those two operations, zero-height gaps and prediction residual are used for detecting contrast enhancement and resizing. Moreover, conditional fingerprint is proposed to distinguish their tampering order. In [23], the authors considered a similar situation that the testing image suffered the manipulations of blurring and sharpening. In [24], Chu et al. proposed an information theoretical framework to quantify the detectability of the order of operations. Specially, they first formulated the order detection problem as a multi-hypotheses test problem. Then, an information theoretical framework was proposed to model the relationship between the detected hypothesis and the true hypothesis. In addition, conditional fingerprints were defined to measure the detection performance. Similarly, our previous works [25, 26] also focused on the detection of binary operation chains. In [25], we achieved the order detection of contrast enhancement and resizing. In [26], we considered a scenario that the image was altered by upsampling and median filter; a certain conditional fingerprint was designed to determine their tampering order.

However, considering the ambiguous processing artifacts (i.e., when applying tamper operations on multimedia content, subsequent operations can weaken or even erase the traces of previous ones), it is hard to determine the trace of multiple manipulation history which digital content has gone through. There is no work to answer this question, "how to quantify the detectability of one specific operator in multiple operations?" For example, if a given image is tampered by resizing, contrast enhancement, and median filter, there will be 16 different operator chains, how to identify one specific operation? It remains an open challenge.

In this paper, an information theoretical framework is proposed to answer the question how to quantify the detectability of one specific operation in multiple chains. To accomplish this, we analyze the operation identification problem from the perspective of set partitioning and detection theory. Based on a certain of detectors, conditional probability criterions are used to quantify the detectability of one specific operation. Furthermore, two main constraints are designed to improve the detection performance. In our experiments, we evaluated our information theoretical framework performance by detecting the operations of contrast enhancement, resizing, and median filter in a certain chain set.

The remaining of this paper is organized as follows. Section 2 proposes the information framework and constraints. Section 3 presents our proposed detection methods for the operations contrast enhancement, resizing, and median filter. To demonstrate the effectiveness of our proposed framework and constraints, simulation results are examined in Sect. 4. Finally, Sect. 5 concludes our work.

2 Information theoretical framework

To identify and quantify the detectability of one specific operation, we analyze the operation detection problem from the perspective of set partitioning and detection theory. First, in terms of set partitioning, we need to separate the considered multiple operator chains into binary chains set. One set contains the topologies of detected operation, the other is not. Furthermore, to quantify the detectability, we model the operation quantification problem as a multiple hypotheses testing problem. Specially, based on the intrinsical fingerprint, features can be extracted from the image contents. Then, after modeling the distribution of features, detectors with tunable parameters will be used to obtain the detection performance. The process is shown in Fig. 1.

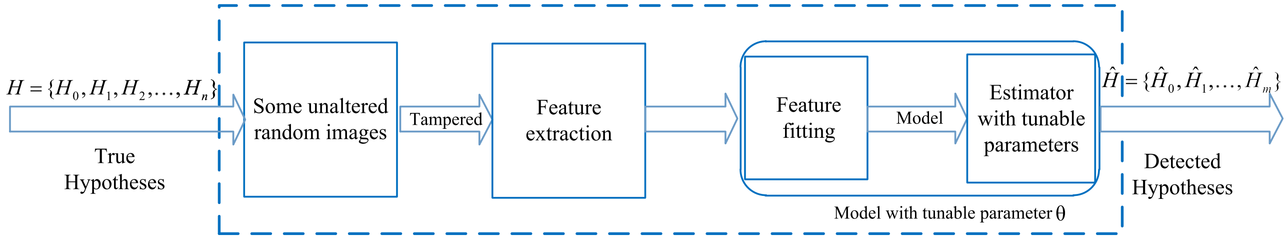
$H = \{H_0, H_1, H_2, \ldots, H_n\}$
True Hypotheses
Some unaltered random images
Tampered
Feature extraction
Feature fitting
Model
Estimator with tunable parameters
Model with tunable parameter θ
$\hat{H} = \{\hat{H}_0, \hat{H}_1, \ldots, \hat{H}_m\}$
Detected Hypotheses

Fig. 1 A typical process of detecting one specific operation in multiple operator chains

Let $O = (O_1, O_2, \dots, O_m)$ denote the set of manipulation operations. In terms of set partitioning, we need to separate the considered multiple operator chains into binary chain sets. To obtain those two sets, we first use $S = (S_0, S_1, \dots, S_m)$ to denote the set of operator chains containing all the considered topologies, among them, $S_i (i = 0, 1, \dots, m)$ denotes the set generated by full permutation of i operations. S_0 denotes empty chain, it means that the detecting image content is unaltered. Then, divide S into two parts, denote as (D_i^0, D_i^1). D_i^1 is the set that contains all the topologies of the detected operation O_i, D_i^0 is the complementary set, they are incompatible with each other. To measure the separation result, we use $\mathrm{Num}(S)$ to denote the topologies number containing all the considered operator chains. It is computed by the equation:

$$\mathrm{Num}(S) = \sum_{i=0}^{m} A_m^i. \tag{1}$$

$\mathrm{Num}(D_i^1)$ denotes the topologies number of D_i^1, as formulated by the following:

$$\mathrm{Num}(D_i^1) = \sum_{j=1}^{m} C_j^1 A_{m-1}^{j-1}, \tag{2}$$

where A and C are symbols of permutation and combination.

Then, we can use the equation to calculate the proportion set containing O_i in the whole, that is

$$P(\hat{H}_{O_i}) = P(D_i^1/S) = \frac{\sum_{j=1}^{m} C_j^1 A_{m-1}^{j-1}}{\sum_{i=0}^{m} A_m^i}. \tag{3}$$

To further quantify and improve the detection performance, we model the operation identification problem as a multiple hypotheses testing problem. Specially, define the true hypotheses as a set containing all the considered multiple operator chains, denote as $H = (H_0, H_1, \dots, H_n)$, where $n = \sum_{i=0}^{m} A_m^i$. Define the detected hypotheses as a set containing all the topologies of one specific operation, denote as $\hat{H} = (\hat{H}_0, \hat{H}_1, \dots, \hat{H}_m)$. For example, suppose to detect two operations A and B, i.e., $m = 2$, there are five operator chains to be considered, i.e., $\emptyset, A, B, AB, BA$. Thus, $n = 5, H = (\emptyset, A, B, AB, BA)$. Similarly, $\hat{H} = (\emptyset, (A, AB, BA), (B, AB, BA))$. Given the true hypotheses, our destination is to measure the information entropy between H and $\hat{H}$.

Specially, via modeling the distribution of certain feature contents, detectors with tunable parameters $\underline{\theta}$, denoted as $d_{\underline{\theta}}$, which can be developed to contrast different hypotheses. For each choice of $\underline{\theta}$, we represent the performance of its detector using the conditional probability of a detected hypothesis given a true hypothesis, i.e., $P_{\underline{\theta}}(\hat{H}, H)$. Based on set partitioning and hypothesis test, we novelly propose a Theorem to quantify the detectability, that is:

Theorem 1 Calculate the detectability of null operation $\hat{H}_0$ and one specific operation $\hat{H}_j$ as the following equations:

$$P_{\underline{\theta}}(\hat{H}_0, H) > \frac{1}{\sum_{i=0}^{m} A_m^i} + \epsilon \tag{4}$$

$$P_{\underline{\theta}}(\hat{H}_j, H) > P(\hat{H}_j, H) + \epsilon, \quad \forall j = 1, 2, \dots, m, \tag{5}$$

where $P(\hat{H}_j, H) = P(\hat{H}_{O_j})$, calculated by Eq. (3). $\epsilon \geq 0$ are confidence factors indicating how well the hypothesis can be distinguished from others.

According to Theorem 1, we can achieve quantifying the detectability of one specific operation in operator chains. However, in the actual process of operation detection, there are many factors that may affect the performance of operation identification, such as different parameters of tampering operation, tunable parameters during modeling the distribution of features, and so on. Therefore, we further design two main constraints to improve the detection performance, they are as follows.

Constraint 1 To minimum the average decision error P_e, minimize the false-positive rate for a given false-negative rate, that is:

$$\arg\min_{P_{FP}} (P_e) = \arg\min_{P_{FP}} \frac{1}{2}\left(P_{FP} + P_{FN}\right), \tag{6}$$

where P_{FP} and P_{FN} denote the false-positive and false-negative rates, respectively. In our scenario, the false-positive rate means detecting a specific operation which the considered content has gone through when it has not. The false-negative rate indicates that the content has not undergone a given operator chain, when, indeed, it has.

Constraint 2 For detectors $d_{\underline{\theta}_1}$ and $d_{\underline{\theta}_2}$, detector $d_{\underline{\theta}_1}$ is better than $d_{\underline{\theta}_2}$, with respect to the conditional probability, when

$$P_{\underline{\theta}_1}(\hat{H}, H) > P_{\underline{\theta}_2}(\hat{H}, H). \tag{7}$$

According to Constraint 2, different detectors yield different detection performance. To obtain the best detector $d_{\underline{\theta}^\star}$, we next use Maximum-Likelihood Estimation (MLE) method to estimate those tunable parameters affecting the detection probability. That is:

$$\underline{\theta}^\star = \arg\max_{\underline{\theta}} P_{\underline{\theta}}(\hat{H}, H). \tag{8}$$

Based on the information theoretical framework, by examining the Theorem 1, we can answer whether an operation can be detected or not. If the operation can be detected, MLE can be used to obtain the best detector. So far, using the designed constraints, we can further optimize the information theoretical framework detection performance.

3 Detecting one specific operation in multiple operation chains

In this section, we consider a multiple case that the image is tampered by three different operations, i.e., contrast enhancement, resizing and median filter. Based our information theoretical framework and constraints, we first theoretically analyze how to quantify the detectability of one specific operation. Then, three detection methods are proposed to extract the features of those tampering operations.

3.1 Specific operation identification based on information theoretical framework

To demonstrate the effectiveness of our framework, we consider a scenario that a given image content is altered by contrast enhancement, resizing, or median filter. In this problem, $O = (O_1, O_2, O_3)$, $m = 3$. We use org, rs, ce, and mf to denote null operation, resizing, contrast enhancement, and median filter, respectively. According to Eq. (1), there are 16 different operation chains to be considered, and thus, $n = 16$. Suppose to detect contrast enhancement, in terms of set partitioning, the given image can be divided into two sets, D_1^0 and D_1^1. D_1^0 contains 5 elements (calculated by Eqs. (2, 3)), i.e., org, rs, mf, rsmf, and mfrs. To implement the separation of those two sets, we then analyze the problem in terms of detection theory.

According to the typical detection process of Fig. 1, we can first obtain the true hypotheses $H = (H_0, H_1, \dots, H_{16})$. Similarly, $\hat{H} = (\hat{H}_0, \hat{H}_1, \dots, \hat{H}_3)$ denote the detected hypotheses, where $\hat{H}_0$, $\hat{H}_1$, $\hat{H}_2$ and $\hat{H}_3$ denote the detected hypothesis of null operation, contrast enhancement, resizing, and median filter, respectively. To contrast H and $\hat{H}_1$, we first extract the fingerprint left by contrast enhancement. Then, using the model of distribution fitting and estimation, a detector d_θ with fixed parameters can be obtained. According to the Theorem 1, we can quantify the detectability of contrast enhancement. Furthermore, considering the fact that detection performance varies on different detectors, MLE method is used to obtain the best detector, as shown in Eq. (8).

3.2 Contrast enhancement detection based on residual histogram

Contrast enhancement works by applying a non-decreasing nonlinear mapping to the pixel values of an image. After nonlinear mapping, there will be sudden zero-height gaps in a contrast enhanced image's pixel value histogram. In our previous work [21], we have proposed a detection algorithm by measuring the difference of each pixel value in the histogram. However, the feature dimension is too small.

To overcome this shortcoming, we directly extract residual information of the histogram in this paper. The process can be formalized as follows:

$$\mathrm{Hist}(i) = \frac{\mathrm{Hist}(i) - \mathrm{Hist}_{\mathrm{mean}}}{\mathrm{Hist}_{\mathrm{std}}}, \tag{9}$$

where $\mathrm{Hist}_{\mathrm{mean}}$ and $\mathrm{Hist}_{\mathrm{std}}$ denote the mean and standard deviation of the histogram, respectively.

Calculated by Eq. (9), we can obtain different residual histograms of tampered images. As shown in Fig. 2, the zero-height gaps still remain in the residual histogram of an contrast enhanced image; they can be used to identify the operation of contrast enhancement.

3.3 Resizing detection based on the integral projection of p-map

Image resizing is performed by first determining a new image sampling grid and then by interpolating values on this grid that are not directly observed. The state-of-art work [3] in resizing detection mainly estimates the p-map (i.e., a set of probabilities measure the correlation of a pixel and its neighbors), which can be calculated as formula:

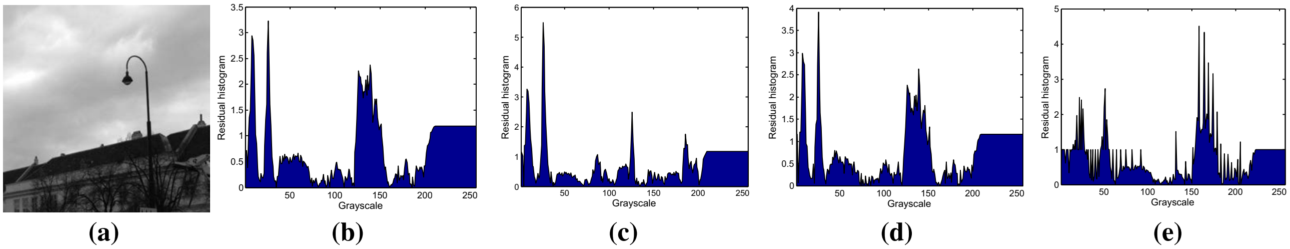

Fig. 2 A gray image (**a**) and its residual histogram (**b**), the residual histogram of a resized image (**c**), median filtered image (**d**), and contrast enhanced image (**e**)

$$p_{i,j} = \lambda \exp(-\left|e_{i,j}^{\mu}\right|/\sigma), \tag{10}$$

where $\lambda, \mu > 1$, and $\sigma > 0$ are controlling parameters. If an image has been resampled, distinct spectral peaks will be present in the 2D DFT of p-map. Then, the cumulative periodogram C is used to detect resizing:

$$\rho = \max_{k_1,k_2} \|\nabla C(k_1, k_2)\|, \tag{11}$$

where ρ is a detection statistic. Via analyzing each element of p-map, we find that there are a large difference between some values of p in the vertical or horizontal directions. Considering the complexity of cumulative periodogram, we propose a new method to calculate p-map. We first standardize the p-map using z scores, and then calculate the integral projection of p-map in the vertical or horizontal directions (i.e., sum each row or column of p-map). Because we only calculate the vertical integral projection, the process can be formalized as follows:

$$\bar{P}(1,j) = \bar{P}(1,j) + \sum_{i=2}^{L} \bar{P}(i,j), \tag{12}$$

where L is the length of matrix p-map, and $\bar{P}(i,j)$ is the element of normalized p-map, which is calculated using the following equation:

$$\bar{P}(i,j) = \frac{P(i,j) - P_{\text{mean}}}{P_{\text{std}}}. \tag{13}$$

The above detection scheme can not only highlight the feature traces, but also reduce the feature dimension. According to Eqs. (12, 13), we can obtain p-map integral projections of different tampered images. The details are shown in Fig. 3, where horizontal axis represents frequency and vertical axis represents the integral projection values of p-map. In the bottom right figure of Fig. 3, the dotted read line shows that some elements of $\bar{P}$ changes a lot than others. Meanwhile, distinct spectral peaks are present in resized image. Thus, we can use them to determine resizing.

3.4 Median filter detection based on difference histogram

Median filtering is a nonlinear smoothing technique that sets each pixel value to the median values of all the pixels in a neighborhood window at that point. As is known, the distribution function of natural image is hard to model. On the contrary, the distribution of difference image can be precisely characterized by the generalized Gaussian distribution (w.r.t, GGD) or Laplace distribution. To detect median filter, we first define the difference image (in vertical direction) of gray image D as $\bar{D}$, with

$$\bar{D}(i,j) = D(i,j) - D(i+1,j) \tag{14}$$

Moreover, the 2D DFT of difference histogram (i.e, the histogram of difference image) takes both spital and frequency correlations into consideration and can reflect most image information. Thus, we next calculate the energy of difference histogram in frequency domain using the equation:

$$E(x,y) = \sum_{u=-l_d}^{l_d} \sum_{v=-w_d}^{w_d} F(u,v)^2, \tag{15}$$

where $F(u, v)$ means the histogram of difference image $\bar{D}$ in frequency domain. E remains the energy presenting in the power spectrum, in a window of dimension $(2l_d \times 2w_d)$.

Calculated by Eqs. (14, 15), we can obtain difference-histogram energy curves of different operations, as shown in Fig. 4. While this approach can be used to trace the fingerprint of median filter, there are great difference between elements of $E(x, y)$.

To overcome this shortcoming, we novelly do logarithmic operation for each element of normalized energy, that is:

$$\bar{E}(x,y) = -\log_{10} \frac{E(x,y)}{\sum_x \sum_y E(x,y)}. \tag{16}$$

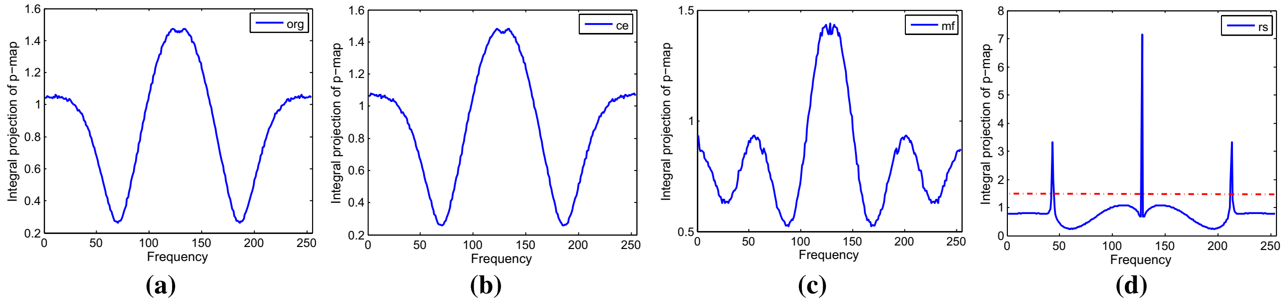

Fig. 3 Integral projection of p-map in the vertical direction. Unaltered images (**a**), contrast enhanced images (**b**), median filtered images (**c**), and resized images (**d**). The curves are averaged over 1000 images from the BOSS database [27]

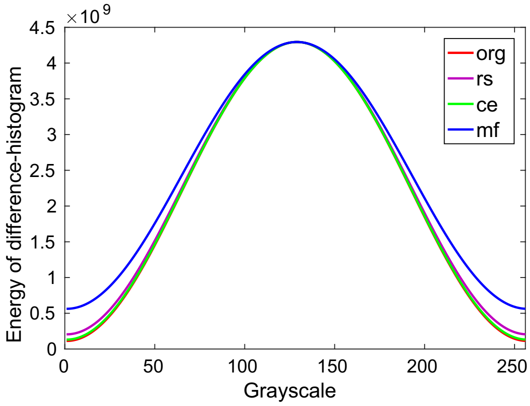

Fig. 4 Difference-histogram energy curves of different operations, averaged over 1000 images from the BOSS database [27]

From Fig. 5, we can see all the curves which precisely present in the distribution of GGD. Moreover, because different distribution parameters correspond to certain distribution curves, by the processing of distribution fitting and parameters estimation, we can achieve the detection of median filter.

4 Simulation results

In this section, we conduct several simulations to demonstrate our framework. Based on the theoretical analysis of quantifying the detection of one specific operation, experiment results are used to verify the correctness and effectiveness of our framework.

4.1 Image set

Considering that when the test image database and the training image database are derived from the same data set, it is possible to make the test and training image have similar statistical characteristics. Thus, we choose 10000 images from BOSS database [27] to generate the training images, and 1338 images from UCID database [28] to generate the test images. The fore-mentioned feature representation is based on gray image, and thus, we first convert each color image to gray image. Now, we generate a number of tampered images. Let $\bar{I}_i = H_i(I)$, where $i = \{1, 2, \dots, 16\}$. H_i denotes the ith operator chain. In this problem, we use γ, α, and β which denote the parameters of contrast enhancement, resizing, and median filter, respectively.

To verify the robustness of our proposed features, we tamper the images with different parameter pairs (see Table 1 for details). Then, we crop them to [256 × 256] which are the most meaningful parts of original ones. Finally, we totally get 160000 tampered images to train and every 10000 tampered images are derived from one specific operator chain. Similarly, there are 21408 images constructing different test databases.

4.2 Real-time detecting three different operations

As known from the constraints 1 and 2 in Section II, there are three aspects affecting the tunable parameters $\underline{\theta}^{\star}$ in this problem, they are as follows:

- the ordering and topology of the operator chain whenever a fixed set of operators, each of them using fixed parameters;
- the use of different operator parameters in chains which share the same topology;
- different proportions of training and testing image set using the same operators, denoted as n.

Thus, there are four tunable parameters, i.e., $\underline{\theta} = \left(\gamma, \alpha, \beta, n\right)$.

Specially, considering the effect of the size of image set, we select training and testing sample in a certain scale n, where $n = \{1, 2, \dots, 5\}$. If $n = 2$, we randomly select 1000 sample from each database $\bar{I}_i$ generated by the BOSS database for training, and 500 sample from each testing set

Table 1 Parameter sets used to generate tampering images

parameter	Set 1	Set 2
γ	0.7	1.2
α	1.25	1.5
β	3 × 3	5 × 5

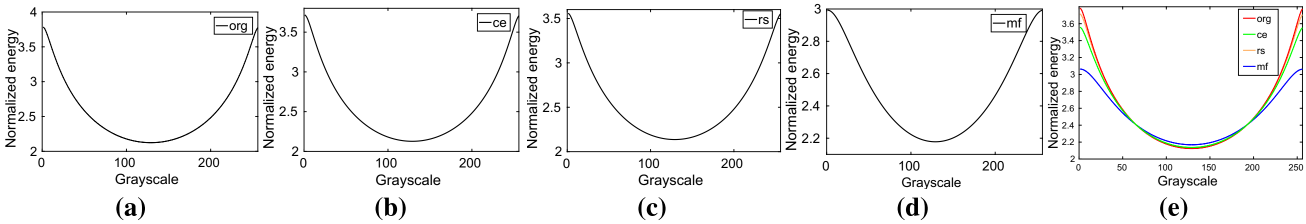

Fig. 5 Normalized energy curves of difference histograms, averaged over 1000 images from the BOSS database. Unaltered images (**a**), contrast enhanced images (**b**), resized images (**c**), median filtered image (**d**), and the contrast of those different operations (**e**)

Table 2 Average detecting accuracies with $\underline{\theta} = \left(0.7, 1.5, 3 \times 3\right)$ (%)

Scale	C_0	C_1	C_2	C_3
1:1	98.237	90.025	86.316	82.750
2:1	98.566	91.600	87.195	82.745
3:1	98.916	92.591	87.429	82.712
4:1	99.012	93.504	87.500	82.733
5:1	99.056	94.079	87.704	82.775

Table 3 Average detecting accuracies with $\underline{\theta} = \left(0.7, 1.5, 5 \times 5\right)$ (%)

Scale	C_0	C_1	C_2	C_3
1:1	98.566	90.225	80.850	85.625
2:1	98.825	92.008	81.183	86.125
3:1	98.995	92.716	80.941	86.016
4:1	99.054	93.129	81.083	86.079
5:1	99.108	93.508	81.487	86.041

Table 4 Average detecting accuracies with $\underline{\theta} = (0.7, 1.25, 3 \times 3)$ (%)

Scale	C_0	C_1	C_2	C_3
1:1	98.395	91.087	81.886	82.925
2:1	98.725	92.518	82.407	82.915
3:1	98.914	93.518	82.418	83.412
4:1	97.973	93.975	82.956	83.356
5:1	98.014	94.637	83.150	83.275

Table 5 Average detecting accuracies with $\underline{\theta} = (0.7, 1.25, 5 \times 5)$ (%)

Scale	C_0	C_1	C_2	C_3
1:1	98.350	91.425	78.954	83.812
2:1	98.750	92.500	79.175	85.275
3:1	98.904	93.775	79.512	85.112
4:1	98.975	93.612	79.912	86.637
5:1	99.117	94.425	80.125	86.650

for testing. Then, we employ SVM to learn a multi-class classifier with grid-search parameter optimization. The radial basis function (RBF) is used as kernel function, where the kernel function parameters are initialized to: $C = 10, \gamma = 0.0032$. The procedure is repeated three times for fivefold cross-validation, and finally, we get the average accuracies.

Denote null operator chain as C_0, the operator chains containing contrast enhancement as C_1, the operator chains containing resizing as C_2, and the operator chains containing median filter as C_3, they correspond to each element of the detected hypotheses $\hat{H}$. According to our framework, we first extract features from training set. Specially, we cascade the feature sets of those detection methods proposed above to detect the empty operator chain. When extracting the integral projection feature of resizing, we initialize the parameters in Eq. (10) to $\lambda = 1$, $\sigma = 1$, $\mu = 2$. Then, via the procedures of feature fitting and estimation, the training model with different tunable parameters will be obtained.

Based on different detectors with tunable parameters $\underline{\theta} = (\gamma, \alpha, \beta, n)$, we can use information theoretical framework and constraints to obtain the best tunable parameters. Specially, testing images are first used to obtain different detection probability. Then, MLE is used to obtain the estimate the best tunable parameter $\underline{\theta}$. The experiment results with different tunable parameters are shown in Tables 2, 3, 4, 5, 6, 7, 8, 9.

By analyzing all of average detection accuracies shown above, we can obtain that:

Table 6 Average detecting accuracies with $\underline{\theta} = \left(1.2, 1.5, 3 \times 3\right)$ (%)

Scale	C_0	C_1	C_2	C_3
1:1	98.250	87.487	86.237	82.850
2:1	98.675	89.200	87.387	82.700
3:1	98.718	91.075	85.575	82.800
4:1	98.025	91.075	87.837	82.687
5:1	98.174	91.850	87.775	82.762

Table 7 Average detecting accuracies with $\underline{\theta} = (1.2, 1.5, 5 \times 5)$ (%)

Scale	C_0	C_1	C_2	C_3
1:1	97.435	88.587	80.737	85.375
2:1	98.077	90.025	80.912	85.837
3:1	98.545	90.675	81.987	85.937
4:1	98.900	91.137	81.362	85.662
5:1	99.124	92.025	81.587	85.700

Table 8 Average detecting accuracies with $\underline{\theta} = (1.2, 1.25, 5 \times 5)$ (%)

Scale	C_0	C_1	C_2	C_3
1:1	98.135	89.662	78.877	86.750
2:1	98.375	90.187	79.125	86.900
3:1	98.697	91.587	79.975	86.675
4:1	98.875	91.937	80.125	87.012
5:1	98.756	92.400	80.364	86.812

- When the values of γ, α, and β are constant, the larger the scale n between training and testing set, the better detection performance.
- In the case where only γ can be tunable, the farther γ is from 1, the better the detection performance of contrast enhancement.

Table 9 Average detecting accuracies with $\underline{\theta} = (1.2, 1.25, 3 \times 3)$ (%)

Scale	C_0	C_1	C_2	C_3
1:1	97.575	88.537	79.875	83.275
2:1	97.837	90.575	80.437	83.350
3:1	98.128	91.387	80.775	83.262
4:1	98.350	92.187	80.837	83.462
5:1	98.750	92.437	81.175	83.250

- In the case where only α can be tunable, the larger resizing scale factor α, the better the detection performance of resizing.
- In the case where only β can be tunable, the larger filer window β is, the better the detection performance median filter gains.

4.3 Comparison analysis

In this section, we compared the detection method based on information theoretical framework and that without framework. To accomplish this, we first used the same experimental database that we created in the previous set of experiments for the three operations detection scenario using the theoretical framework. Next, we directly achieve detecting specific operations with SVM.

To do this, we first use detection methods proposed in Sect. 3 to extract the tampering traces of contrast enhancement, resizing, and median filter, respectively. Then, based on RBF kernel function, we employ SVM to learn a multi-class classifier with grid-search parameter optimization.

Table 10 shows the results of our experiments using the information theoretic framework and not, the parameters of RBF are: $C = 10, \gamma = 0.0032$. From Table 10, one can notice that our approaches can typically achieve higher than 82% detection accuracy with different types of image manipulations. Furthermore, the average detection accuracies using information framework can 4% higher than that not.

Tables 11, 12 also show the comparison results of our experiments under different tunable parameters. All these results demonstrate the effectiveness of using our information theoretic framework.

4.4 Complexity analysis

In this section, we mainly analyze the effectiveness of our theoretical framework from two aspects, i.e., the time complexity and space complexity. All of the detection methods are implemented with MATLAB R2013b and run on a computer with following configuration. The processor is a quad-core Intel core i7-4790k CPU with 4.00 GHz, the

Table 10 Average detection accuracies with and without the information theoretical framework under $\underline{\theta} = (0.7, 1.5, 3 \times 3)$ (%)

Scale	C_0	C_1	C_2	C_3
(a) Detection results with the information theoretical framework				
1:1	98.237	90.025	86.316	82.750
2:1	98.566	91.600	87.195	82.745
3:1	98.916	92.591	87.429	82.712
4:1	99.012	93.504	87.500	82.733
5:1	99.056	94.079	87.704	82.775
(b) Detection results without the information theoretical framework				
1:1	93.970	87.913	78.400	77.713
2:1	94.021	88.725	78.613	78.218
3:1	94.269	89.725	79.375	78.650
4:1	94.154	90.050	79.525	79.013
5:1	94.975	90.437	79.600	79.188

Table 11 Average detection accuracies with and without the information theoretical framework under $\underline{\theta} = (1.2, 1.5, 3 \times 3)$ (%)

Scale	C_0	C_1	C_2	C_3
(a) Detection results with the information theoretical framework				
1:1	98.250	87.487	86.237	82.850
2:1	98.675	89.200	87.387	82.700
3:1	98.718	91.075	85.575	82.800
4:1	98.025	91.075	87.837	82.687
5:1	98.174	91.850	87.775	82.762
(b) Detection results without the information theoretical framework				
1:1	93.895	84.250	79.875	78.400
2:1	93.984	84.500	80.438	78.613
3:1	94.032	84.425	80.725	79.375
4:1	94.875	84.575	80.838	79.525
5:1	95.160	84.463	81.175	79.600

Table 12 Average detection accuracies with and without the information theoretical framework under $\underline{\theta} = (1.2, 1.5, 5 \times 5)$ (%)

Scale	C_0	C_1	C_2	C_3
(a) Detection results with the information theoretical framework				
1:1	97.435	88.587	80.737	85.375
2:1	98.077	90.025	80.912	85.837
3:1	98.545	90.675	81.987	85.937
4:1	98.900	91.137	81.362	85.662
5:1	99.124	92.025	81.587	85.700
(b) Detection results without the information theoretical framework				
1:1	93.895	85.112	77.187	79.987
2:1	93.984	85.550	77.612	80.425
3:1	94.032	85.937	77.725	80.575
4:1	94.875	86.012	78.400	80.700
5:1	95.160	86.512	78.525	81.053

RAM capacity is 16 GB, and the operating system is Windows 7. The detailed analyses are as following.

First, we analyze the time complexities of those three detection methods,

- The core of contrast enhancement detection is to normalize the histogram with z score method. To achieve that, we need calculate histogram's mean and standard deviation. Thus, the time complexity is $O(n)$.
- The core of resizing detection is to calculate p-map and its integral projection. Therefore, the time complexity is $O(n^2)$.
- The main time consuming of median filter detection is the stage of calculating energy of histogram, and thus, the time complexity is $O(n^2)$.

Second, in terms of space complexity, it takes 65 kb to store an [256 × 256] image. From Sect. 4, we can know that there are 181408 images may be used, and thus, over 12.25GB memory is used to store those image databases.

Finally, we calculate the average consuming time for training a model and that testing an image. Table 13 presents computational time comparison, where the first column is the scale of training and testing set, the second column is the average time cost to train a model of each image, and the last four columns are the average testing time of different operation detecting methods. It is observed that our average time of training an image is fast and efficient.

To further save training and testing time, we use MATLAB parallel tool to accelerate computational time of our detection methods, the details are shown in Table 14. Compared with the first column of Table 13, we can see that the average training time of Table 14 is greatly shortened. For example, when the scale of training and testing data set is 3 : 1, the average training time is shorten by 52.8%.

Table 13 Computational time comparison among different scales between training and testing databases with single core

Scale	Average training time (s)	Average testing time			
		C_0 (s)	C_1 (s)	C_2 (s)	C_3 (s)
1:1	0.185	0.001	0.002	0.004	0.002
2:1	0.185	0.005	0.007	0.007	0.005
3:1	0.191	0.011	0.014	0.026	0.011
4:1	0.190	0.017	0.025	0.059	0.020
5:1	0.189	0.028	0.039	0.093	0.035

Table 14 Computational time comparison among different scales between training and testing databases based on MATLAB parallel tools

Scale	Average training time (s)	Average testing time			
		C_0 (s)	C_1 (s)	C_2 (s)	C_3 (s)
1:1	0.121	0.001	0.003	0.004	0.002
2:1	0.095	0.004	0.007	0.011	0.006
3:1	0.090	0.008	0.017	0.031	0.012
4:1	0.114	0.012	0.028	0.053	0.019
5:1	0.112	0.021	0.041	0.089	0.027

5 Conclusion

In this paper, we focus on the question how to quantify the detectability of one specific operation in multiple chains. The main contributions of the paper can be summarized in the following three aspects:

1. Via the perspective of set partitioning and detection theory, we novelly analyze the operation identification problem and propose an operation identification information theoretical framework.
2. Based on a certain of detectors, conditional probability criterions are used to quantify the identification of one specific operation. Moreover, considering the main constraints affecting the detection performance, a strategy based on MLE is proposed to obtain the best detectors.
3. For a case study, we examine the problem of detecting one specific operation in a certain multiple chain set. Simulations show that our proposed framework and constraints are useful and efficient for operation detection.

Acknowledgements This work is supported by National Natural Science Foundation of China (Grant nos. 61402162, 61772191), Hunan Provincial Natural Science Foundation (Grant no. 2017JJ3040), Open Project Program of National Laboratory of Pattern Recognition (Grant no. 201900017), Open Research Fund of Key Laboratory of Network Crime Investigation of Hunan Provincial Colleges (Grant no. 2017WL-FZZC001), the Key Lab of Information Network Security and the Ministry of Public Security of China (Grant no. C17606), and CERNET Innovation Project (Grant no. NGII20180412).

References

1. Stamm, M.C., Wu, M., Liu, K.J.R.: Information forensics: an overview of the first decade. IEEE Access **1**, 167–200 (2013)
2. Liao, X., Qin, Z., Ding, L.: Data embedding in digital images using critical functions. Signal Process. Image Commun. **58**, 146–156 (2017)

3. Qin, C., Ji, P., Chang, C., Dong, J.: Non-uniform watermark sharing based on optimal iterative BTC for image tampering recovery. IEEE Multimed. **25**(3), 36–48 (2018)
4. Liao, X., Yu, Y., Li, B., Li, Z.: A new payload partition strategy in color image steganpgraphy. IEEE Trans. Circuits Syst. Video Technol. https://doi.org/10.1109/TCSVT.2019.2896270 (2019)
5. Qin, C., Chen, X., Luo, X., Zhang, X.: Perceptual image hashing via dual-cross pattern encoding and salient structure detection. Inf. Sci. **423**, 284–302 (2018)
6. Popescu, A.C., Farid, H.: Exposing digital forgeries by detecting traces of resampling. IEEE Trans. Signal Process. **53**(2), 758–767 (2008)
7. Kirchner, M., Bohme, R.: Hiding traces of resampling in digital images. IEEE Trans. Inf. Forensics Secur. **3**(4), 582–592 (2008)
8. Boroumand, M., Fridrich, J.: Scalable processing history detector for JPEG images. Electron. Imaging **10**, 128–137 (2017)
9. Feng, X., Cox, I., Doerr, G.: Normalized energy density-based forensic detection of resampled images. IEEE Trans. Multimed. **14**(3), 536–545 (2012)
10. Stamm, M.C., Liu, K.J.R.: Forensic detection of image manipulation using statistical intrinsic fingerprints. IEEE Transactions on Information Forensics and Security **5**(3), 492–506 (2010)
11. Singh, N., Gupta, A., Jain, R.C.: Global contrast enhancement based image forensics using statistical features. Adv. Electric. Electron. Eng. **15**(3), 509–516 (2017)
12. Chen, C., Ni, J., Huang, J.: Blind detection of median filtering in digital images: a difference domain based approach. IEEE Trans. Image Process. **22**(12), 4699–4710 (2013)
13. Kang, X., Stamm, M.C., Peng, A., Liu, K.J.R.: Robust median filtering forensics using an autoregressive model. IEEE Trans. Inf. Forensics Secur. **8**(9), 1456–1468 (2013)
14. Su, B., Lu, S., Tan, C.L.: Blurred image region detection and classification. In: ACM International Conference on Multimedia, pp. 1397–1400 (2011)
15. Li, J., Li, X., Yang, B., Sun, X.: Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. **10**(3), 507–518 (2015)
16. Cai, K., Lu, X., Song, J., Wang, X.: Blind image tampering identification based on histogram features. In: International Conference on Multimedia Information Networking and Security (MINES), pp. 300–303 (2011)
17. Li, H., Luo, W., Qiu, X.: Identification of various image operations using residual-based features. IEEE Trans. Circuits Syst. Video Technol. **28**(1), 31–45 (2018)
18. Qiu, X., Li, H., Luo, W.: A universal image forensic strategy based on steganalytic model. In: ACM workshop on Information hiding and multimedia security, pp. 165–170 (2014)
19. Cao, G., Zhao, Y., Ni, R.: Contrast enhancement-based forensics in digital images. IEEE Trans. Inf. Forensics Secur. **9**(3), 515–525 (2014)
20. Chen, Z., Zhao, Y., Ni, R.: Detection of operation chain: JPEG-resampling-JPEG. Signal Process. Image Commun. **57**, 8–20 (2017)
21. Comesa*ñ*a, P.: Detection and information theoretic measures for quantifying the distinguishability between multimedia operator chains. In: IEEE International Workshop on Information Forensics and Security, pp. 211–216 (2012)
22. Stamm, M. C., Chu, X., Liu, K. J. R.: Forensically determining the order of signal processing operations. In: IEEE International Workshop on Information Forensics and Security, pp. 162–167 (2013)
23. Liu, Y., Zhao, Y., Ni, R.: Forensics of image blurring and sharpening history based on NSCT domain. In: Signal and Information Processing Association Annual Summit and Conference, pp. 1–4 (2014)
24. Chu, X., Chen, Y., Liu, K. R.: An information theoretic framework for order of operations forensics. In: IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 2049–2053 (2016)
25. Gao, S., Liao, X., Guo, S.: Forensic detection for image operation order: resizing and contrast Enhancement. In: International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, pp. 570–580 (2017)
26. Li, J., Liao, X., Hu, R., Liu, X.: Detectability of the image operation order: upsampling and mean filtering. In: IEEE Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, pp. 1544–1549 (2018)
27. Patrick, B., Filler, T., Pevn*ý*, T.: Break our steganographic system: the ins and outs of organizing BOSS. In: International Workshop on Information Hiding, pp. 59–70 (2011)
28. Schaefer, G., Stich, M.: UCID: an uncompressed color image database. Storage Retr. Methods Appl. Multimed. **5307**(1), 472–481 (2004)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Shangde Gao received the Bachelor's degree in College of Computer Science and Electronic Engineering, Hunan University, China. Currently, he is pursuing the Master's degree in College of Computer Science and Electronic Engineering, Hunan University, China. His research interests include image forensics and machine learning.

Xin Liao received the B.E. degree and Ph.D. degree in information security from Beijing University of Posts and Telecommunications, Beijing, China, in 2007 and 2012, respectively. He is currently an associate professor with Hunan University, China, where he joined in 2012. His research interests include image steganography, watermarking, and multimedia forensic.

Xuchong Liu received the Ph.D. degree in computer applied technology from Central South University in 2010. He is currently a professor with Hunan Police Academy and director of Hunan Key Laboratory of Network Investigation Technology. His research interests include digital forensics, network investigation, and big data intelligent police.