Signal Processing: Image Communication 95 (2021) 116287

Contents lists available at ScienceDirect

Signal Processing: Image Communication

journal homepage: www.elsevier.com/locate/image

Identifying tampering operations in image operator chains based on decision fusion

Jiaxin Chen [a], Xin Liao [b,a,*], Zheng Qin [a]

[a] College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[b] Key Lab of Forensic Science, Ministry of Justice, Academy of Forensic Science, Shanghai 200063, China

ARTICLE INFO

Keywords:
Image forensics
Image operator chain
Tampering operations identification
Decision fusion

ABSTRACT

There has been great interest in image forensics in recent years. However, most of the existing research focuses on detecting a certain tampering operation, which means that the introduced features usually depend on the investigated operation and only binary classification is considered. Given the case where the image tampering process involves diverse processing operations, we propose a decision fusion method for identifying tampering operations in operator chains in this work. The proposed method permits the integration of knowledge provided by available image forensic algorithms. Under this method, a similarity coefficient function is introduced to assign the weight of the output of each forensic classifier. Then, we utilize a combination rule based on local conflict management to merge these outputs. Comparison with the previous works shows an improvement in operations identification accuracy when an image has experienced multiple falsifications.

1. Introduction

Since an image is a representation of an objective object and contains information about the object being described, it has played an important role in information transmission. However, with the popularity of image editing tools, images are facing a serious crisis of public trust. Image forensics [1], whose purpose is to verify the authenticity of an image, has become a possible solution to the above crisis.

Image processing operations usually leave some imperceptible artifacts into the falsified images, therefore, the presence of these artifacts can be used as evidence to detect whether the suspected image has undergone manipulations or not [2]. In recent years, many state-of-art image forensic methods for image forgery detection have been designed, such as resampling [3–5], sharpening [6–8], contrast enhancement [9], and JPEG compression [10,11]. These methods are utilized for identifying the existence of a specific processing operation. In a realistic scenario, when performing a single tampering operation on an image, there are usually more than one manipulation options available. Thus, forensic technology for one operation may not perform well when used to detect another operation. Several universal forensic approaches [12–14] have been proposed to identify different kinds of manipulations in the past few years.

Generally, image forgery involves the application of multiple operations. Therefore, a variety of tampering artifacts will be left in the image. Considering that most existing image forensic methods (which assume the investigated image has undergone only a single tampering operation) applied in the scenario of multiple manipulations may give uncertain answers or the results would be far from ideal, nature thought would be to employ more than one forensic method to identify the types of operations when an image is altered by multiple operations.

Some efforts have been made to develop feature fusion schemes [15–17]. Nevertheless, If the dimension of the selected feature is large, then the feature fusion will have a greater computational cost. Thus, we consider fusing the output of the image forensic methods and then make a comprehensive decision. This choice delegates the task of selecting features and training the classifier to every single forensic algorithm. We can directly obtain the integrated identification result, while avoid retraining the whole detector each time a new method is added. In this paper, we concentrate on the tampering operations identification problem when an image has continuously undergone multiple operations. The main contributions of the paper are as follows:

(1) On the assumption that the forensic analyst has knowledge of multiple image forensic algorithms to identify certain tampering operations, we propose an image operations identification method based on decision fusion to detect different tampering operations in an operator chain. The method integrates forensic information obtained by several forensic algorithms. Notice that these algorithms are based on the hypothesis of images undergoing a single operation. To the best of our knowledge, this is the first attempt to introduce this fusion idea into the image forensics of image operator chains.

(2) We present a credibility calculation strategy to measure whether a piece of forensic evidence is in great conflict with other evidence. We use the similarity coefficient to characterize the degree of conflict

[*] Corresponding author at: College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China.
E-mail address: xinliao@hnu.edu.cn (X. Liao).

https://doi.org/10.1016/j.image.2021.116287
Received 20 October 2020; Received in revised form 7 April 2021; Accepted 11 April 2021
Available online 18 April 2021
0923-5965/

between forensic information obtained by different forensic methods and assign credibility to each evidence, which could achieve better tampering operations identification performance.

(3) We evaluate the effectiveness of our proposed method in the case of image operator chain forensics. The experimental results show that exploiting decision fusion to integrate the information of multiple forensic algorithms has better operations identification performance against state-of-the-art forensic methods.

The remainder of this paper is organized as follows. Section 2 reviews the related works. In Section 3, we explain the fact that the forensic method based on the single operation tampering assumption is not effective to identify operations in operator chains. The decision fusion-based operations identification method is proposed in Section 4. Section 5 presents investigative experiments aimed at comparing the identification performance among some state-of-the-art methods and our method in the case of multiple falsifications. Section 6 provides the corresponding discussions. Finally, the conclusions and future works are made.

2. Related works

In this section, we briefly review the related works about single operation forensics and multiple operations forensics. We then review the works about forgery detection relied on the fusion method.

2.1. Single operation forensics

Nowadays, various single operation forensic methods are designed, including specific operation identification and universal forensics.

Specific operation identification attempts to determine whether an image has undergone a certain tampering operation, which is a binary classification problem. Specifically, an earlier resampling forensic method [3] utilized the specific periodic correlations that can be observed in the image pixels. These correlations are measured based on an expectation–maximization algorithm and can be used to identify a broad range of resampling rates. Feng et al. [4] developed a resampled imagery detector where the normalized energy density characteristic is learned and applied to train an SVM classifier. Cao et al. [6] combined the gradient aberration of the gray histogram and ringing artifacts to capture trails of sharpening operation. In [7], the authors detected sharpening manipulation based on the overshoot artifacts that appear around the side edges in the sharpened images.

Universal forensics assumes that an image is altered by one of the various tampering operations. It aims at distinguishing which operation the image has experienced. Qiu et al. [12] analyzed the similarity between universal forensics and image steganography, and then they identified six kinds of typical manipulations with the help of some universal steganalytic features. Moreover, inspired by steganalytic algorithms, Li et al. [13] exploited the spatial rich model (SRM) features and designed a classification scheme for detecting different image operations. In [14], the authors employed the histogram features extracted from the difference images to train an SVM classifier, which can efficiently realize universal forensics.

2.2. Multiple operations identification

Consider the situation where an image is falsified by multiple operations. These operations collectively constitute an image operator chain in a certain order. Peng et al. [18] analyzed median filtering artifacts via a group of different residuals and constructed a feature set on these residuals to detect the operator chain composed of median filtering and JPEG compression. Chu et al. [19,20] formulated the order of operations detection problem as a multiple hypotheses testing problem. Then, they designed a set of features and proposed an information theoretical framework to determine whether or not the considered hypotheses can be distinguished. In [21], to quantify the detectability of one specific operation in operator chains, Gao et al. first analyzed the operation detection problem based on set partitioning and detection theory. Then, they presented an information theoretical framework and conditional probability criteria.

2.3. Forgery detection based on fusion method

Since using a single forensic tool may not achieve better results when detecting multiple tampering, several fusion methods have been developed to improve detection performance by integrating multiple aspects of information. Fusion methods can be divided into two categories: feature fusion and decision fusion.

Hsu et al. [15] proposed a fusion method based on Discriminative Random Fields [16] where different physical features are integrated to classify spliced images from four types of cameras. In [17], the authors presented a fuzzy fusion of image residue characteristics to detect tampering in video sequences. These works mainly focus on fusion at the feature level. Although being promising in terms of performance, the priority of feature fusion is less than that of decision fusion. The main reason is that feature fusion needs to re-integrate all features extracted from selected forensic algorithms and retrain a new classifier to achieve identification when a new forensic algorithm is added or deleted. Compared with decision fusion, which directly integrates forensic results, feature fusion pays more computational cost. Fontani et al. [22,23] presented a decision fusion strategy based on the Dempster–Shafer Theory of Evidence [24] for coping with image splicing classification under different compression situations. However, the authors only considered a certain operation and then studied how to distinguish between the original images and the tampered images, which is a binary classification and not suitable for multi-operation classification problem in image operator chains.

3. The tampering operations identification in operator chains

In this section, the motivation for the proposed work is investigated first. Then, we give an example to illustrate that the operations in an image operator chain may not be detectable by using a single operation forensic method.

3.1. Motivation

In a realistic scenario, it is inevitable to apply multiple tampering operations to forge an image. For instance, if a forger wants to weaken the details of an image, he or she may need to apply an upsampling operation to insert new elements between pixels on the basis of the original image pixels. This operation may lose the high-frequency part of the interpolated image, making the image blurred. To make the new image more realistic, the forger may also utilize median filtering to filter out the noise caused by upsampling. This purposeful image forgery will change the authenticity of an objective object. Therefore, it is necessary to verify the authenticity of the image and correctly identify the tampering operations, hoping to restore the original image.

However, multiple manipulations would affect and disguise the tampering artifacts of the previously applied operations. What is more, two chains of the same p tampering operations using different orders will leave behind different traces, making the tampering operations more difficult to distinguish. Therefore, the forensic method which supposes an image is altered by a single operation would not be able to effectively detect multiple tampering operations in operator chains. We propose an image operations identification method based on decision fusion, which integrates information obtained by multiple different forensic algorithms and makes comprehensive decisions on multiple tampering operations experienced by images from disparate perspectives. Then, the accuracy of operation recognition in an operator chain could be improved.

3.2. An example of operations may not be identified

Forensic investigators not only need to detect the type of each tampering operation but also to distinguish different tampering orders, so that the complete tampering history and the image forger can be determined. However, the existing forensic method which supposes the image is altered by a single operation may not effectively detect multiple tampering operations in operator chains. For example, considering an image operator chain that may contain two tampering operations: A and B, the following five possible processing histories of an investigated image need to be identified.

$$\begin{aligned} H_0 &: \text{It is unaltered,} \\ H_1 &: \text{It is altered by A only,} \\ H_2 &: \text{It is altered by B only,} \\ H_3 &: \text{It is altered by A then B,} \\ H_4 &: \text{It is altered by B then A.} \end{aligned} \tag{1}$$

We suppose A and B are median filtering and upsampling, and then a universal forensic algorithm [14] has been used to identify these tampering operations in the image operator chain. Fig. 1 shows the different features of each possible processing history, we would observe that the features of images with various processing histories by using this method are similar, especially for H_3 and H_4 classes, which makes these tampering operations unrecognizable. The reason for this result is that the forensic algorithm is designed based on the assumption that the image has only undergone a tampering operation, and does not consider the changes in traces caused by multiple operations.

The combination rule based on local conflict management [25] can be utilized to merge different evidence to calculate the probability of an event. Therefore, the uncertainty of the event will be reduced. Given the tampering operations identification problem in image operator chains we studied in this paper, if we only use a single existing image forensic method based on the assumption that the image has only undergone one processing operation, the identification effect cannot be ideal. To improve manipulations detection accuracy, we intend to exploit the local conflict management-based decision fusion for combining the forensic results of several image forensic methods.

4. The decision fusion in image operations identification

In this section, we first describe the assumptions of our method. Then, a similarity coefficient function is introduced for credibility calculation. Finally, we illustrate the combination process of operations identification results obtained from two or more forensic algorithms.

4.1. Assumptions

Our decision fusion method relies on the basic assumptions listed below:

(1) We consider a case in which we want to investigate the possible processing histories experienced by an image, and assume that two or more forensic methods are available for detecting certain operations;

(2) Each forensic method outputs a set of numbers in [0,1], where each number represents the probability of a certain processing history that the image may experience, and higher values indicate higher confidence about the analyzed image undergoing the processing history;

(3) Each forensic method gathers information independently of other methods. Note that the definition of independence mentioned in decision fusion is not strictly. To put it in another way, different (independent) image forensic methods that rely on a different principle or effect are needed to determine different tampering evidence.

These assumptions are very reasonable in the forensics scenario where an image is forged by several operations with a certain order. It is also worth noting that assumption 3 means that if we observe two different forensic algorithms supporting the same hypothesis, we are more confident than observing only one.

4.2. Credibility calculation strategy based on similarity coefficient

Let $O = \{o_1, o_2, \dots, o_p\}$ represent the set of possible manipulation operations, where $p \geq 1$. If these p operations are applied to falsify an original image, q falsified images will be generated.

$$q = \sum_{k=1}^{p} A_p^k, \tag{2}$$

where A_p^k represents the number of all permutations of k operations selected from p different operations.

Then, a hypotheses set can be denoted as $H = \{H_0, H_1, \dots, H_q\}$, where $H_i (i = 0, 1, \dots, q)$ represents a hypothesis for possible processing history of an image I. Note that the set H includes the classes of an unaltered image H_0 and images altered by A_p^k kinds of tampering operations. For example, suppose $O = \{o_1, o_2\}$, and then we can find that the hypotheses set is $H = \{H_0, H_1, H_2, H_3, H_4\}$ corresponding to the description of Eq. (1).

Definition 1. Let $H = \{H_0, H_1, \dots, H_q\}$ be a frame. A Basic Belief Assignment (BBA) function [26] over the frame H is denoted as follows,

$$m^H : 2^H \rightarrow [0, 1]. \tag{3}$$

Note that the BBA function satisfies:

$$\begin{cases} m(\phi) = 0, \\ m(H_i) \geq 0, \\ \sum\limits_{H_i \subset H} m(H_i) = 1, \end{cases} \tag{4}$$

where the summation is performed on every possible subset H_i of H.

Because the operations identification in an image operator chain is a multi-classification problem, we consider p manipulation operations, so $q + 1$ numbers in $[0, 1]$ will be output when using a forensic method c_i to identify the possible processing history of an image. These $q + 1$ numbers can be expressed as $m_i = \{m_i(H_0), m_i(H_1), \dots, m_i(H_q)\}$, which is the BBA function as described in Definition 1.

Supposing that we have two BBAs defined on the same frame, which are derived from two different forensic algorithms. We can utilize the decision fusion method to merge them into a single one. Note that the confusion and concealment of the operation traces caused by multiple falsifications will make some forensic results contrary to reality. These results often conflict with the correct information output by other algorithms, nevertheless, there are also certain similarities. We use the similarity coefficient to characterize the similarity between the forensic methods, which also reflects the degree of conflict between them.

Definition 2. Let m_i and m_j be BBA functions over the same frame $H = \{H_0, H_1, \dots, H_q\}$, for $\forall H_k$, the basic mass assignments are $m_i(H_k)$ and $m_j(H_k)$, respectively. Then the similarity coefficient of the two evidences with respect to hypothesis H_k is

$$Sim_{i,j}(H_k) = \frac{cos(\pi \cdot |m_i(H_k) - m_j(H_k)|) + 1}{2}. \tag{5}$$

Fig. 2 provides an illustration of the similarity coefficient function. The x-axis and y-axis are the basic mass assignments of different pieces of forensic evidence about a certain hypothesis over the same frame, and the z-axis calculates their similarity coefficient. When $m_i(H_k) = m_j(H_k)$, the similarity coefficient is 1, indicating that the two forensic methods hold the same opinion on the tampering history H_k experienced by the image. When the difference between $m_i(H_k)$ and $m_j(H_k)$ is large, that is, one forensic result supports the hypothesis H_k to a certain extent and the other evidence denies H_k, the similarity coefficient decreases, implying that there is a high degree of conflict between the two forensic results.

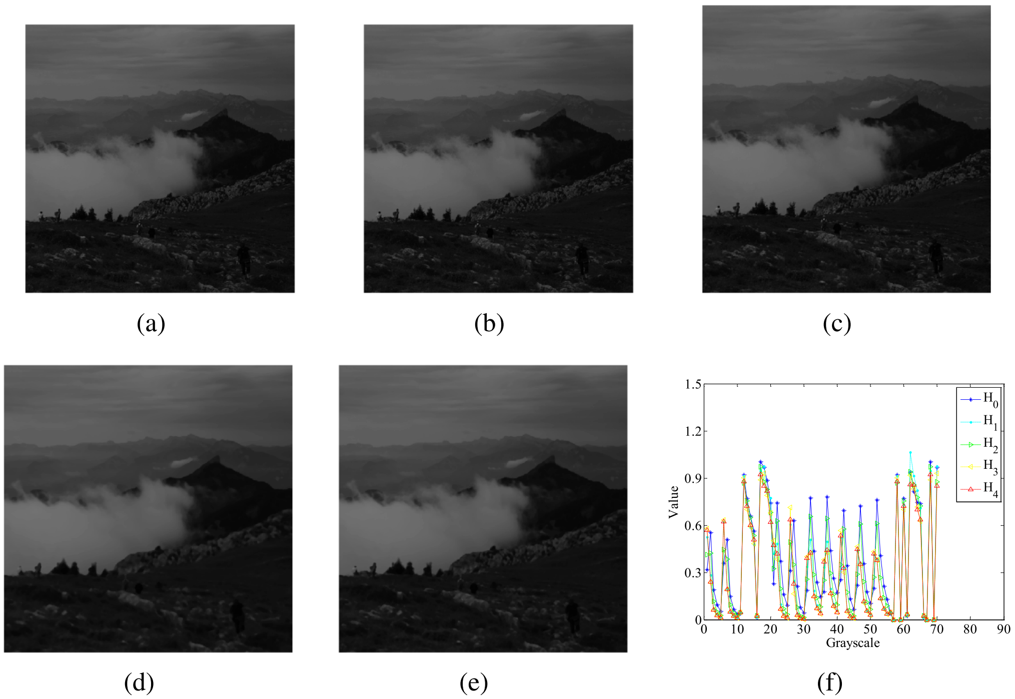


Fig. 1. An example that we might not be able to identify operations in an operator chain. (a) is the original image, (b) is the median filtered image, (c) is the upsampled image, (d) is the median filtered then upsampled image, (e) is the upsampled then median filtered image and (f) is the features of the image experienced different processing histories as described in Eq. (1).

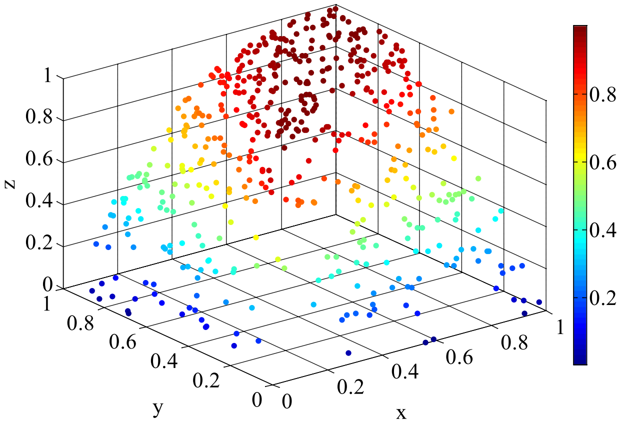


Fig. 2. An example of the similarity coefficient of two forensic evidence on the hypothesis H_k.

If we have n forensic results, according to the similarity coefficient between the n results calculated, we can get the similarity matrix of hypothesis H_k,

$$\boldsymbol{Sim} = \begin{bmatrix} 1 & Sim_{1,2} & \cdots & Sim_{1,n} \\ Sim_{2,1} & 1 & \cdots & Sim_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ Sim_{n,1} & Sim_{n,2} & \cdots & 1 \end{bmatrix}. \tag{6}$$

This matrix shows the degree of mutual support between the forensic evidences output by two forensic algorithms. The higher the degree of one evidence supported by other evidence, the higher the credibility of the evidence. For hypothesis H_k, calculate the degree of support for evidence m_i,

$$Sup_i(H_k) = \sum_{j=1, i\neq j}^{n} Sim_{i,j}(H_k). \tag{7}$$

When each forensic result is highly unified with other results, the similarity coefficient between the results is 1, so the ideal similarity is n. The credibility of evidence m_i with respect to H_k can be calculated as follows,

$$Crd_i(H_k) = \frac{Sup_i(H_k)}{n-1}. \tag{8}$$

Taking the credibility $Crd_i(H_k)$ as the weight of the evidence m_i corresponding to hypothesis H_k, and then redistributing the basic belief assignment function for subsequent forensic results fusion.

4.3. Fusion of forensic results using combination rule

In our work, we merge the pieces of evidence through the combination rule based on local conflict management [25] to get a more credible forensic result.

Definition 3. Combination rule: For the two BBAs m_1 and m_2 under the same frame $H = \{H_0, H_1, \ldots, H_q\}$, if $m_1(H_i) > 0$ and $m_2(H_j) > 0$, there will be conflict $m_1(H_i)m_2(H_j)$ during the combination. It should be noted that this conflict should be managed locally and allocated to the combination of H_i and H_j instead of other hypotheses. The combination of $m(H_k)$ based on local conflict management [25] is calculated in the following way.

- If $m_\cap(H_i) = 0$ and $m_\cap(H_j) = 0$,

$$m(H_k) = m_\cap(H_k) + \sum_{\substack{H_k \subseteq H_i \text{ or } H_k \subseteq H_j \\ H_i \cap H_j = \phi}} \frac{m_\cap(H_k)}{2} \cdot m_1(H_i)m_2(H_j); \tag{9}$$

- If $m_\cap(H_i) \neq 0$ or $m_\cap(H_j) \neq 0$,

$$m(H_k) = m_\cap(H_k) + \sum_{\substack{H_k \subseteq H_i \text{ or } H_k \subseteq H_j \\ H_i \cap H_j = \phi}} \frac{m_\cap(H_k)}{\sum_{D \subseteq H_i \text{ or } D \subseteq H_j} m_\cap(D)} \cdot m_1(H_i)m_2(H_j). \tag{10}$$

It should be noted that $m_{\cap}(H_i)$ represents the product sums of the basic mass assignments where the elements in the hypotheses frame intersect as H_i. In addition, $\frac{m_{\cap}(H_k)}{\sum_{D\subseteq H_i \text{ or } D\subseteq H_j} m_{\cap}(D)} \cdot m_1(H_i)m_2(H_j)$ is the part of a specific conflict value assigned to hypothesis H_k.

According to the Eqs. (9), (10), the combined result $m = \{m(H_0), m(H_1), \cdots, m(H_q)\}$ can be obtained after decision fusion, where $m(H_k)$ represents the fused mass assignment of the hypothesis H_k. The hypothesis corresponding to the maximum value of $m(H_k)$ is the possible processing history experienced by the suspected image.

Since decision fusion can provide a more credible forensic result by integrating the knowledge of various forensic algorithms, we perform the multiple tampering operations identification based on the decision fusion method in image operator chains, which is illustrated in Fig. 3. Specifically, we suppose there are p tampering operations that may be employed to alter the N investigated testing image. For detecting the possible processing history of the testing images, there are n image forensic methods to reveal image tampering, which can feed n forensics classifiers $\{c_1, c_2, c_3, \ldots, c_n\}$. The calculation of operations identification accuracy based on decision fusion can be divided into four steps:

(1) Obtaining the forensic result $\{m_1, m_2, \ldots, m_n\}$ from n image forensic classifiers. According to Eq. (2), p tampering operations will generate $q+1$ possible processing history hypotheses $\{H_0, H_1, \cdots, H_q\}$. The result of classifier c_i can be denoted as a basic belief assignment function $m_i = \{m_i(H_0), m_i(H_1), \ldots, m_i(H_q)\}$;

(2) Calculating the credibility of each evidence relies on Eqs. (5)–(8) and redistributing the basic belief assignment function for each piece of evidence, we will obtain a new forensic result $m_i' = \{m_i'(H_0), m_i'(H_1), \cdots, m_i'(H_q)\}$;

(3) Exploiting the combination rule in turn to fuse the forensics results to obtain the final identification result $m = \{m(H_0), m(H_1), \ldots, m(H_q)\}$;

(4) Determining whether the identification result is the same as the true result. Concretely, the highest value of $m(H_i)$ indicates that the image may be forged in the manner described by H_i. If the result is consistent with the actual tampering history of the image, it is judged that the operations in the image operator chain have been correctly identified. The accuracy of each class is the number of images whose identification result is the same as the true result in N testing images.

5. Experimental results

In this section, taking the image operator chain composed of two different tampering operations as an example, we validate the performance of tampering operations identification. Specifically, three typical image manipulation operations (i.e., median filtering, sharpening, and upsampling) are chosen. Every two different operations are used to collectively constitute an image processing chain:

- The operator chain consists of median filtering and upsampling.
- The operator chain consists of upsampling and sharpening.
- The operator chain consists of median filtering and sharpening.

Given that the median filtering will affect the distribution of differences between neighboring pixels, the image upsampling operation may alter spatial correlations among neighboring pixels, and the image sharpening is an image enhancement operation that will enhance image contrast and sharpen the edges. Applying these tampering operations will destroy the authenticity and integrity of an image. We exploit two universal forensic methods for detecting median filtering, one is to use histogram features of difference images [14] and the other is to analyze the conditional joint distribution of first-order difference images [27]. The specific periodic correlations based method [3] and the normalized energy density-based approach [4] are utilized to identify upsampling. For sharpening detection, we observe the overshoot artifacts around the side edges [7]. In our experiments, we apply our proposed method to fuse the outputs obtained from these methods, hoping to achieve the purpose of improving recognition performance by merging multi-perspective information.

Table 1
The operations identification accuracies (%) of the forensic methods based on the single operation tampering assumption, the SVM-based method and our method in operator chain consists of median filtering and upsampling. “w/out CC” means that the credibility calculation is not used. “w/CC” is to utilize the credibility calculation. “AVG” calculates average accuracy.

Parameter	Method	H_0	H_1	H_2	H_3	H_4	AVG
$w = 3, s = 1.5$	Popescu et al. [3]	91.80	61.90	95.00	91.20	71.10	82.20
	Feng et al. [4]	90.00	87.00	80.80	88.70	61.70	81.64
	Cai et al. [14]	97.20	81.40	80.90	87.70	82.20	85.88
	SVM-based	97.80	77.70	79.10	85.00	75.40	83.00
	Fusion w/out CC	**99.40**	91.00	97.30	95.60	**86.60**	93.86
	Fusion w/CC	**99.40**	**91.30**	**97.60**	**95.80**	**86.60**	**94.14**
$w = 5, s = 1.3$	Popescu et al. [3]	98.20	51.20	96.70	93.30	46.60	77.20
	Feng et al. [4]	89.20	76.70	83.80	24.00	**69.40**	68.62
	Cai et al. [14]	94.60	69.10	75.90	90.10	51.40	76.22
	SVM-based	93.40	74.60	90.10	96.30	62.70	83.42
	Fusion w/out CC	**99.20**	79.90	97.70	98.10	67.50	88.48
	Fusion w/CC	**99.20**	**80.20**	**97.80**	**98.50**	69.20	**88.98**

In order to verify the effectiveness of our decision fusion method, we compare it with an SVM-based framework, where tampering manipulations are identified by training an SVM classifier and utilizing the output of a single algorithm as input features. The reason for this comparison is all referenced methods end up employing a classifier (usually an SVM) and the SVM-based framework uses the obtained forensic results for re-training, which is equivalent to transferring knowledge from the learned tasks to improve the learning of new tasks, improving the accuracy of operations recognition. It is the best way to compare our decision fusion method. What is more, in the case of ignoring the computational complexity, we consider a comparison with the feature fusion method [17] to discuss the difference between the feature fusion method and the decision fusion method in the accuracy of tampering operations identification in image operator chains.

5.1. Image manipulations identification of median filtering and upsampling

In the experiment, tampered images are generated with different parameters by combining the factors of median filtering and upsampling. Namely, the median filtering with window sizes $w = \{3, 5\}$ and the upsampling with scaling factors $s = \{1.3, 1.5\}$. For a given image, the five hypotheses about possible processing history are considered as Eq. (1), where A and B represent median filtering and upsampling.

According to Fig. 3, to detect operations that images may undergo, we should choose some forensic methods based on the single operation tampering hypothesis. In this case, the methods mentioned in [3,4,14] are used. Notice that these methods all obtain forgery results by training a classifier, that is, there are three different classifiers utilized to identify manipulations in the image operator chain consisting of median filtering and upsampling. For each classifier, we use 2000 unaltered images from the BOSSbase image set [28] to generate a training database, and 1000 unaltered images from the UCID image set [29] to generate a testing database. These images are converted into gray-scale images and altered as described in Eq. (1). Hence, we will get 10,000 training images and 5000 testing images.

The classifier can output the assignment of the hypothesis of each testing image. Specifically, for a testing image I, we will derive forensics results $m_i = \{m_i(H_0), m_i(H_1), m_i(H_2), m_i(H_3), m_i(H_4)\}$ from classifier c_i. Then, the final identification result $m = \{m(H_0), m(H_1), m(H_2), m(H_3), m(H_4)\}$ can be calculated according to our decision fusion method. The hypothesis with the highest probability value corresponds to the hypothesis to which the predicted testing image belongs.

Table 1 shows the classification results of image forensic methods that suppose the image has only undergone tampering with a single

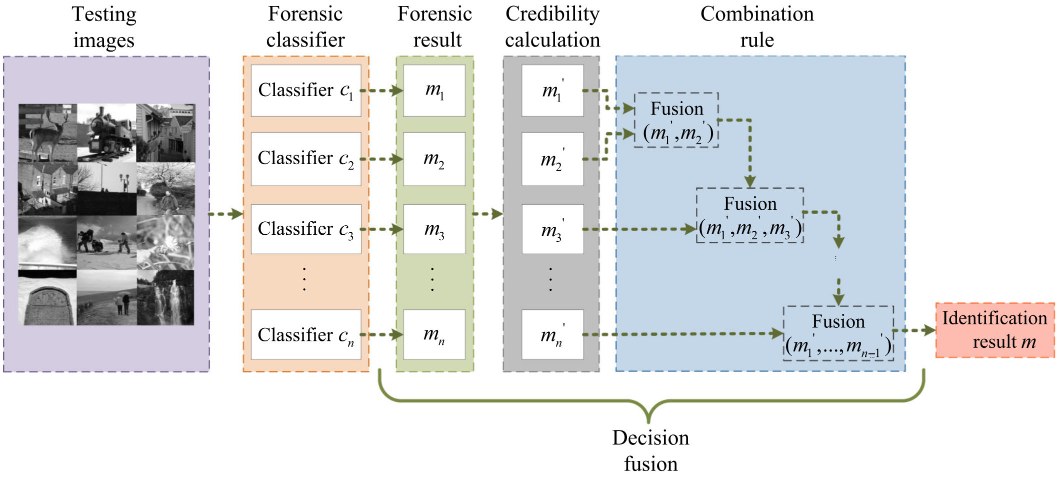


Fig. 3. Block diagram illustrating the tampering operations identification based on decision fusion.

Table 2
The operations identification accuracies (%) of the forensic methods based on the single operation tampering assumption, the SVM-based method and our proposed method in operator chain consists of upsampling and sharpening. "w/out CC" means that the credibility calculation is not used. "w/CC" is to utilize the credibility calculation. "AVG" calculates average accuracy.

Parameter	Method	H_0	H_1	H_2	H_3	H_4	AVG
$s = 1.3$ $\sigma = 0.8, \lambda = 1.5$	Popescu et al. [3]	51.50	55.90	71.40	94.90	72.10	69.16
	Cao et al. [7]	38.30	56.60	31.80	38.50	35.30	40.1
	Pevný et al. [27]	73.50	69.50	97.70	82.70	92.30	83.14
	SVM-based	68.60	69.20	96.80	67.50	87.30	77.88
	Fusion w/out CC	79.30	76.20	**99.30**	**97.00**	93.30	89.02
	Fusion w/CC	**85.10**	**84.80**	98.50	**97.00**	**93.60**	**91.80**
$s = 1.5$ $\sigma = 1.3, \lambda = 1$	Popescu et al. [3]	49.10	45.90	32.10	93.60	72.20	58.58
	Cao et al. [7]	40.90	61.50	26.90	45.40	49.60	44.86
	Pevný et al. [27]	72.10	63.50	99.10	93.30	88.30	83.26
	SVM-based	65.00	60.50	97.10	91.20	82.20	79.20
	Fusion w/out CC	79.20	77.90	**99.20**	**98.90**	95.30	90.10
	Fusion w/CC	**89.60**	**89.90**	97.90	97.90	**95.90**	**94.24**

operation, the SVM-based method, our proposed fusion method without calculating the credibility and fusion method via credibility calculation respectively. From this table, we can see that after merging the forensic results of three existing forensic methods via our methods, identification accuracy has improved significantly. This result indicates that our decision fusion method can be applied to identify manipulations in this operator chain.

In order to prove that our proposed method is superior to other methods when identifying tampering operations in an image operator chain, four comparison experiments are conducted. The first experiment is compared to Peng et al. [18], which designed a group of different residuals features to detect the operator chain composed of median filtering and JPEG compression. The second experiment is compared to Chu et al. [19], which formulated the order of operations detection problem as multiple hypotheses testing problem and proposed an information theoretical framework to determine whether or not the considered hypotheses can be distinguished. The third experiment is compared to Gao et al. [21], which proposed an information theoretical framework to quantify the detectability of one specific operation in image operator chains. The fourth experiment is compared to Chetty et al. [17], where forgery is detected by exploiting a feature fusion method. It should be pointed out that we did not compare with Fontani et al. [23], because the authors researched a binary classification problem of whether an image has undergone splicing. However, our issue is the detection of image processing history, which is a multi-classification problem. The hypotheses frames of the two works are different, so it is not appropriate to compare the two methods.

In these comparison experiments, we forge 2000 original images from the BOSSbase dataset with median filtering and upsampling to generate five kinds of training images. Besides, to build the testing dataset, 1000 original images from the UCID image set are chosen and altered in the same way. Fig. 4 provides the comparison of tampering operations identification performance in the image operator chain composed of median filtering and upsampling by applying the proposed method and comparative methods respectively. From this figure, we can find that the proposed decision fusion method could obtain improvements in the identification performance than other comparison methods.

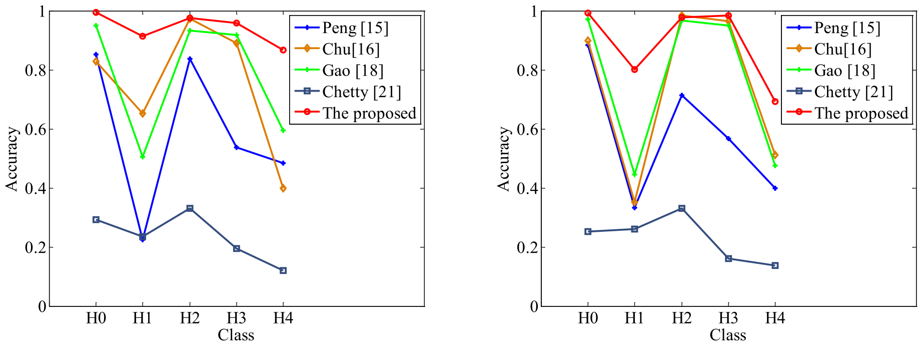
5.2. Image manipulations identification of upsampling and sharpening

In this experiment, tampered images are generated with different parameters by combining the factors of upsampling and sharpening. Namely, the upsampling with scaling factors $s = \{1.3, 1.5\}$ and sharpening with the radius and strength values $(\sigma = 0.8, \lambda = 1.5)$ and $(\sigma = 1.3, \lambda = 1)$. Generally, when setting the sharpening parameter σ, a value greater than 1 and a value less than 1 will be selected to test the detection effect of the sharpening operation under different ranges. We have selected the more commonly used parameter values [7,8,13] for experimental testing. For an investigated image, we consider five hypotheses for possible processing history of the image based on Eq. (1), where A and B are upsampling and sharpening respectively.

As described in Fig. 3, we employ three forensic methods [3,7,27] to identify manipulations in operator chains. For each method, to build the training dataset, 2000 original images are selected from the BOSSbase dataset and forged according to Eq. (1). We also select 1000 unaltered images from the UCID dataset and forge them to create a set of testing images.

Table 2 demonstrates the manipulations identification accuracies when applying the selected forensic methods, the SVM-based method and our methods. What is worth pointing out is that, compared with the recognition performance of the selected single operation forensic algorithms, the average operation identification accuracy of our proposed method with credibility calculation is improved by at least 8.50%. From these results, we find that the proposed identification method is useful to identify manipulations in the operator chain.

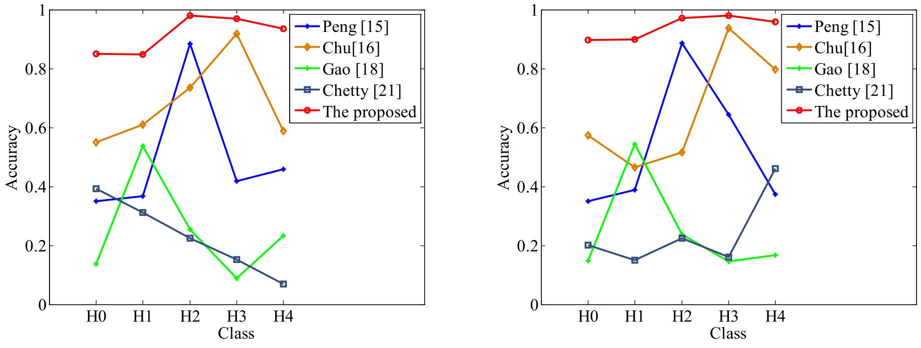
Moreover, we compare our method with the method proposed by Peng et al. [18], Chu et al. [19], Gao et al. [21] and Chetty et al. [17]. Fig. 5 illustrates the comparison results. It is indicated that our proposed method has a great advantage over the comparison methods when detecting tampering operations in the image operator chain consists of upsampling and sharpening.



(a) $w = 3, s = 1.5$

(b) $w = 5, s = 1.3$

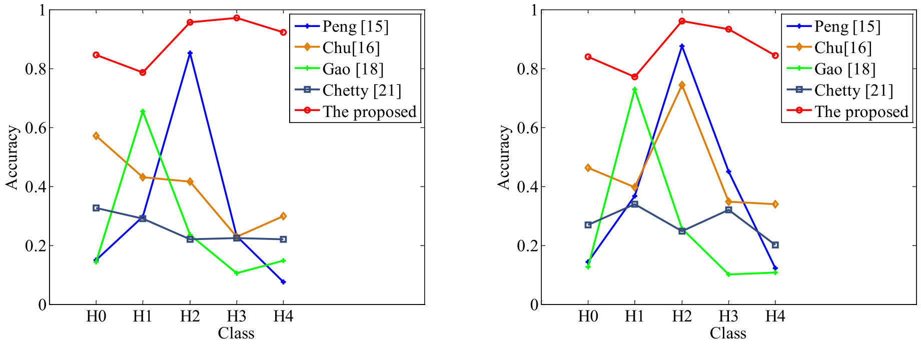
Fig. 4. Comparison of the identification performance of four state-of-the-art forensic methods and the proposed method under different median filtering and upsampling parameters.



(a) $s = 1.3, \sigma = 0.8, \lambda = 1.5$

(b) $s = 1.5, \sigma = 1.3, \lambda = 1$

Fig. 5. Comparison of the identification performance of four state-of-the-art forensic methods and the proposed method under different upsampling and sharpening parameters.



(a) $w = 3, \sigma = 1.3, \lambda = 1$

(b) $w = 5, \sigma = 0.8, \lambda = 1.5$

Fig. 6. Comparison of the identification performance of four state-of-the-art forensic methods and the proposed method under different median filtering and sharpening parameters.

5.3. Image manipulations identification of median filtering and sharpening

In the experiment, tampered images are generated with different parameters by combining the factors of median filtering and sharpening. Namely, the median filtering with window sizes $w = \{3, 5\}$, while the radius and strength values of sharpening are $(\sigma = 0.8, \lambda = 1.5)$ and $(\sigma = 1.3, \lambda = 1)$. For a suspected image, the following five hypotheses for possible processing history are considered as described in Eq. (1), where A and B are median filtering and sharpening.

In this case, three image forgery detection algorithms [4,7,27] are used. We alter 2000 images from the BOSSbase image set by median filtering and sharpening to create the training image set. The testing dataset is composed of 1000 original images from the UCID dataset and 4000 falsified images created as described in Eq. (1). The results of the multi-class classification are displayed in Table 3. From this Table, the results show that the proposed identification method can identify manipulations in the operator chain with great accuracy.

In addition, to evaluate the effectiveness of our decision fusion method, four comparative experiments are performed with the methods of Peng et al. [18], Chu et al. [19], Gao et al. [21] and Chetty et al. [17]. Fig. 6 provides the comparative identification accuracies. Obviously, our method is superior to the comparative methods when detecting manipulations in the image operator chain consisting of median filtering and sharpening.

5.4. Compressed image operations identification in an operator chain

Because several images are stored in JPEG format, the proposed method has been carried out for the manipulations identification when the image is JPEG compressed. In this subsection, two kinds of image

Table 3
The operations identification accuracies (%) of the forensic methods based on the single operation tampering assumption, the SVM-based method and our method in operator chain consists of median filtering and sharpening. "w/out CC" means that the credibility calculation is not used. "w/CC" is to utilize the credibility calculation. "AVG" calculates average accuracy.

Parameter	Method	H_0	H_1	H_2	H_3	H_4	AVG
$w = 5$ $\sigma = 0.8, \lambda = 1.5$	Feng et al. [4]	75.20	**83.90**	77.10	90.10	50.10	75.28
	Cao et al. [7]	64.00	38.60	75.40	63.60	29.60	54.24
	Pevný et al. [27]	76.30	69.70	**97.50**	88.50	83.90	83.18
	SVM-based	72.00	71.80	96.50	82.60	79.10	80.40
	Fusion w/out CC	80.20	75.90	96.40	91.10	**84.50**	85.62
	Fusion w/CC	**83.90**	77.10	96.00	**93.20**	84.40	**86.92**
$w = 3$ $\sigma = 1.3, \lambda = 1$	Feng et al. [4]	69.80	73.20	76.60	73.10	52.70	69.08
	Cao et al. [7]	42.60	42.30	74.70	50.40	74.50	56.90
	Pevný et al. [27]	71.30	70.30	**98.80**	89.50	**93.90**	84.76
	SVM-based	63.90	69.30	96.80	85.80	88.00	80.76
	Fusion w/out CC	79.70	75.30	96.90	**97.30**	92.10	88.26
	Fusion w/CC	**84.50**	**78.70**	95.60	97.20	92.30	**89.66**

Table 4
Comparison of the operations identification accuracies (%) of the proposed method and other forensics methods when the falsified images are JPEG compressed. "w/out CC" means that the credibility calculation is not used. "w/CC" is to utilize the credibility calculation. "AVG" calculates average accuracy.

Parameter	Method	H_0	H_1	H_2	H_3	H_4	AVG
$w = 3$ $\sigma = 0.8, \lambda = 1.5$ $QF1 = 80, QF2 = 95$	Cao et al. [7]	13.40	65.80	77.30	31.50	56.90	48.98
	Pevný et al. [27]	64.00	65.40	81.80	**89.70**	58.90	71.96
	SVM-based	**69.00**	**69.90**	75.30	85.10	67.50	73.36
	Fusion w/out CC	62.70	65.70	93.50	88.50	65.70	75.22
	Fusion w/CC	66.90	61.80	**94.80**	89.40	**69.10**	**76.40**
$s = 1.5$ $\sigma = 0.8, \lambda = 1.5$ $QF1 = 80, QF2 = 95$	Popescu et al. [3]	69.50	56.20	71.10	52.20	55.60	60.92
	Cao et al. [7]	35.10	58.50	25.30	42.40	41.80	40.62
	Pevný et al. [27]	65.10	65.70	81.70	65.40	70.70	69.72
	SVM-based	58.00	62.30	78.50	34.40	69.30	60.50
	Fusion w/out CC	78.50	73.70	93.30	**71.20**	83.50	80.04
	Fusion w/CC	**83.80**	**76.70**	**95.20**	70.00	**85.80**	**82.30**

operator chains are used as examples. For an investigated image, there are five hypotheses for possible processing history of the image.

H_0 : It is double compressed with quality factors QF1 then QF2,
H_1 : It is double compressed with quality factors QF1 then QF2 interleaved by A,
H_2 : It is double compressed with quality factors QF1 then QF2 interleaved by B,
H_3 : It is double compressed with quality factors QF1 then QF2 interleaved by A then B,
H_4 : It is double compressed with quality factors QF1 then QF2 interleaved by B then A,

(11)

where A denotes the upsampling operation and median filtering operation, respectively. B represents the sharpening operation.

To create training and testing images, we first randomly select 2000 original images from the BOSSbase dataset and 1000 unaltered images from the UCID dataset, respectively. Then, these images are converted into gray-scale images and forged as Eq. (11). According to the combination rule, some forensic classifiers for detecting possible manipulations that images have undergone are applied and the final identification result will be obtained by integrating the forensics results from these classifiers. Table 4 shows the accuracy of manipulations identification in different operator chains. It is worth noting that our proposed method based on decision fusion is better than the single operation forensic methods in terms of image operations identification when the images are JPEG compressed.

For each image operator chain, we carry out four comparative experiments with the methods of Peng et al. [18], Chu et al. [19], Gao et al. [21] and Chetty et al. [17] to judge the detection performance. Fig. 7 demonstrates the comparison results. We can find that our method has an advantage over the four methods mentioned in the comparative experiments in image manipulations identification even the falsified images are JPEG compressed.

Compared with the methods mentioned in [18,19,21], the principal advantage of our method is that we can integrate multiple forensic information and identify tampering operations experienced by images from different aspects, instead of relying on a single perspective for image forensics. Compared with Chetty et al. [17], the principal advantage of our method is that when a new forensic algorithm needs to be added, it is necessary for the method [18] to re-fuse new features and re-train a new classifier. While our method only needs to obtain the forensic result of the new algorithm and directly integrate forensic results. Moreover, from Figs. 4–7, we can clearly see that compared with the methods mentioned in [17–19,21], our proposed method can achieve higher accuracy in the image operations identification in different operator chains.

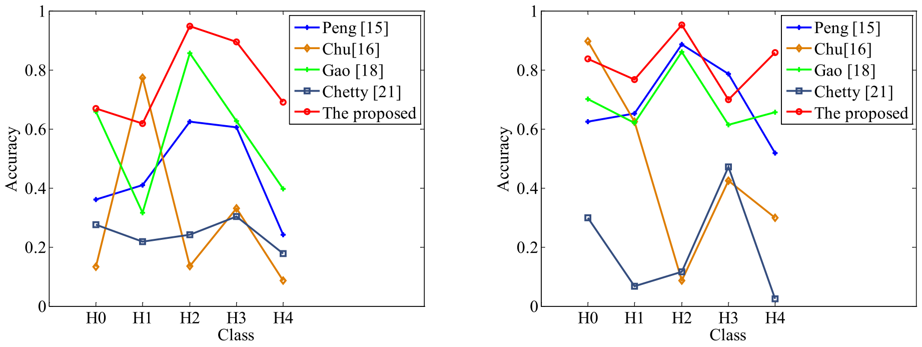
5.5. *Time complexity analysis*

Suppose there are N falsified images. We select n image forensic algorithms, which are based on the assumption that the image has only been altered by one tampering operation, for detecting the operations in operator chains. Then, we calculate the credibility of the forensic results obtained from these algorithms and use the combination rule to fuse these forensic results. All of the forensic algorithms are implemented with MATLAB R2014a. The processor of the computer is Intel core i7-7700 CPU with 3.60 GHz, the RAM capacity is 16 GB, and the operating system is Windows 10. The time complexity analysis of the proposed decision fusion is as follows.

- The main point of forensic algorithms for operations identification is to extract a useful feature. Let d_i represents the dimension of extracted feature based on the forensic algorithm c_i. Assuming that these algorithms obtain forensic results through a support vector machine (SVM) classifier, the computational complexity of these algorithms is related to the dimension of features and the number of sample images, namely, the time complexity is $O(N \times d_{\max})$.
- The main point of credibility calculation is to obtain the similarity matrix of n evidence. Thus, the time complexity is $O(n^2)$.
- The main point of fusion is to sequentially calculate the basic mass assignments of n forensic evidence. Therefore, the time complexity is $O(n)$.

Then, we calculate the average time for training classifiers and testing an image by utilizing the proposed method. Table 5 shows the computational time comparison among different image operator chains. Note that "MF-RS", "RS-SP" and "MF-SP" denote "the chain consists of median filtering and upsampling", "the chain consists of upsampling and sharpening" and "the chain consists of median filtering and sharpening", respectively. "RS-SP JPEG" and "MF-SP JPEG" represent the images altered by different chains are stored in JPEG format. It is observed that the average time cost of our method for training classifiers and receiving the identification results is less than 0.1 s, which is a tiny cost. Furthermore, because the time complexity is related to the dimension of extracted features, the computational time required for operations identification in different operator chains is different.

Finally, we verify the identification performance of tampering operations among three operator chains in the real-time situation. That is, the chain consisting of median filtering and upsampling, the chain consisting of upsampling and sharpening, and the chain consisting of median filtering and sharpening. According to Eqs. (1), (11), each operator chain contains 5 possible processing histories of a given image. We use 1000 images selected from the UCID dataset, hence, 1000



(a) The operator chain consists of median filtering and sharpening

(b) The operator chain consists of upsampling and sharpening

Fig. 7. Comparison of the identification performance of four state-of-the-art forensic methods and the proposed method when the falsified images are JPEG compressed.

Table 5
Computational time used for operations identification in different operator chains applying the proposed method.

Operator chain	Average training time (s)	Average testing time (s)				
		H_0	H_1	H_2	H_3	H_4
MF-RS	0.085	0.023	0.022	0.021	0.023	0.023
RS-SP	0.053	0.016	0.014	0.016	0.013	0.016
MF-SP	0.097	0.009	0.009	0.009	0.009	0.009
RS-SP JPEG	0.051	0.009	0.010	0.009	0.010	0.008
MF-SP JPEG	0.048	0.009	0.008	0.008	0.008	0.007

Table 6
The overall performance of operations identification in operator chains using the proposed method in the real-time situation.

Time (s)/Accuracy	H_0	H_1	H_2	H_3	H_4	AVG
$w = 3$ $s = 1.5$	22.17/ 99.40%	22.29/ 91.30%	21.04/ 97.60%	22.66/ 95.80%	22.91/ 86.60%	22.21/ 94.14%
$s = 1.5$ $\sigma = 1.3, \lambda = 1$	16.36/ 89.60%	14.90/ 89.90%	16.18/ 97.90%	13.66/ 97.90%	16.73/ 95.90%	15.57/ 94.24%
$w = 3$ $\sigma = 1.3, \lambda = 1$	9.21/ 84.50%	9.09/ 78.70%	9.63/ 95.60%	9.14/ 97.20%	9.33/ 92.30%	9.28/ 89.66%
$s = 1.5$ $\sigma = 0.8, \lambda = 1.5$ $QF1 = 80, QF2 = 95$	9.59/ 83.80%	10.53/ 76.70%	9.54/ 95.20%	10.04/ 70.00%	8.50/ 85.80%	9.64/ 82.30%
$w = 3$ $\sigma = 0.8, \lambda = 1.5$ $QF1 = 80, QF2 = 95$	9.01/ 66.90%	8.04/ 61.80%	8.12/ 94.80%	8.04/ 89.40%	7.01/ 69.10%	8.04/ 76.40%

testing images will be obtained for each tamper class. Table 6 provides the total test time and identification accuracy of each tamper class under different chains and operating parameters. For uncompressed images, the proposed method achieves an average identification accuracy of 92.68% when the average time cost is less than 0.016 s. For JPEG compressed images, the average identification accuracy is 79.35% when the average time cost is less than 0.009 s. The results show that our method can achieve better performance with a tiny time cost in real-time. The reason for the decrease in the recognition accuracy of JPEG compressed images is that compression leads to the loss of high-frequency information, which makes the existing forensic algorithm less effective in detecting JPEG compressed images. If the algorithm that detects a single operation can resist the impact of JPEG compression, then combined with our decision fusion method, the accuracy of operations identification in operator chains will be improved.

6. Discussions

Compared with existing forensic algorithms, the main advantage of our method is that we can merge multiple forensic information and identify tampering operations from varied aspects instead of relying on a single perspective for image forensics. Experimental results demonstrate that the proposed method can achieve better detection performance than other forensic algorithms. The limitation is mainly reflected in the degradation of operations identification performance of compressed images, which is due to the loss of high-frequency information caused by JPEG compression. Therefore, the improvement of identification performance for compressed images is one of our future work.

Based on the above discussion, we need to obtain several forensic algorithms based on single tampering operation detection under the same hypothesis frame. It needs to be pointed out that we assume that the forger is tampering with the whole image, thus, the cited methods are designed for identifying the global tampering operations, such as median filtering and sharpening. Local tampering operations (like copy-move, splicing, and removing) classification and tampered regions detection are very important works in the future. For the frame $H = \{H_0, H_1, \ldots, H_{16}\}$ corresponding to the operation set $O = \{copy - move,\ splicing, removing\}$, we will try to extend decision fusion idea to design a new method for detecting local processing history. Currently, most of the released datasets are images processed by local tampering operations. Thus, we can utilize these datasets for experimental analysis in the future.

Unlike fusion at the feature level, which may incur problems such as dimensionality curses, redundant features and high training complexity, our decision fusion method consider the output of the forensic algorithms as they are and fuse them. On the one hand, our method allows us to retain as much information as possible from the analysis of a single forensic algorithm. On the other hand, suppose we want to introduce a new forensic method in a certain hypothesis frame (e.g., the frame $H = \{H_0, H_1, \ldots, H_5\}$ corresponding to the operation set $O = \{sharpening,\ upsampling\}$), and this new method searches for a trace that is already considered in the operation set (e.g., the trace of sharpening). We only need to calculate the credibility of the forensic result obtained by the method with the results obtained from other forensic classifiers and use the combination rule to fuse the forensic results after reallocating the weights. Then, we will get the recognition results we need. The calculation process of this decision fusion is very simple. In addition, it avoids retraining a whole classifier, which will appear in the fusion at the feature level.

If the new method is to detect a new kind of manipulation (e.g., median filtering), this method can still be used to classify the five types of images in the frame H and get the classification results. Similarly, applying our decision fusion method to merge the information of the new method to get the identification result. Note that the new method may provide conflicting evidence, thereby weakening the information of other evidence. At this point, we should study a new fusion strategy, for instance, we can determine the similarity between the new evidence and the pieces of previous evidence through the credibility calculation. If the similarity with all previous evidence is less than 0.5, discard this piece of evidence. That is an important part of our future work.

7. Conclusions

In this paper, we study the more practical image forensics, that is, identifying image processing operations when the suspected images undergo multiple tampering manipulations. The image operations detection method based on decision fusion is proposed. We introduce the concept of similarity coefficient and calculate the credibility of each detection results coming from forensic algorithms (these algorithms assume that the suspected images are altered by a single tampering operation). Utilizing the combination rule based on local conflict management to merge these reallocated results, so as to obtain the identification result of tampering operations in the image operator chain. Experimental results demonstrate that the proposed method can effectively identify the processing history of the images. Moreover, compared with the previous works, the proposed method achieves better identification accuracy.

In the future, we are going to develop a robust detection method against JPEG compression. And then use our decision fusion method to integrate the forensic results of this method with the single operation forensic results to improve the operations recognition performance of compressed images.

CRediT authorship contribution statement

Jiaxin Chen: Conceptualization, Methodology, Formal analysis, Experimental design and data collection, Writing - original draft. **Xin Liao:** Conceptualization, Data interpretation; Writing - review & editing, Supervision, Funding acquisition. **Zheng Qin:** Resources, Writing - review & editing, Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work is supported by National Natural Science Foundation of China (Grant Nos. 61972142, 61772191), Hunan Provincial Natural Science Foundation of China (Grant No. 2020JJ4212), Key Lab of Forensic Science, Ministry of Justice, China (Academy of Forensic Science) (Grant No. KF202118), Science and Technology Program of Changsha, China (Grant No. kq2004021).

References

[1] M.C. Stamm, M. Wu, K.J.R. Liu, Information forensics: An overview of the first decade, IEEE Access 1 (2013) 167–200.

[2] J.A. Redi, W. Taktak, J.-L. Dugelay, Digital image forensics: A booklet for beginners, Multimedia Tools Appl. 51 (1) (2011) 133–162.

[3] A.C. Popescu, H. Farid, Exposing digital forgeries by detecting traces of resampling, IEEE Trans. Signal Process. 53 (2) (2005) 758–767.

[4] X. Feng, I.J. Cox, G. Doërr, Normalized energy density-based forensic detection of resampled images, IEEE Trans. Multimedia 14 (3) (2012) 536–545.

[5] L. Peng, X. Liao, M. Chen, Resampling parameter estimation via dual-filtering based convolutional neural network, Multimedia Syst. (2020) http://dx.doi.org/10.1007/s00530-020-00697-y.

[6] G. Cao, Y. Zhao, R. Ni, Detection of image sharpening based on histogram aberration and ringing artifacts, in: 2009 IEEE International Conference on Multimedia and Expo, Hilton Cancun, Cancun, Mexico, Jun. 28 - Jul. 3, 2009.

[7] G. Cao, Y. Zhao, R. Ni, A.C. Kot, Unsharp masking sharpening detection via overshoot artifacts analysis, IEEE Signal Process. Lett. 18 (10) (2011) 603–606.

[8] F. Ding, G. Zhu, W. Dong, Y.-Q. Shi, An efficient weak sharpening detection method for image forensics, J. Vis. Commun. Image Represent. 50 (2018) 93–99.

[9] J.-Y. Sun, S.-W. Kim, S.-W. Lee, S.-J. Ko, A novel contrast enhancement forensics based on convolutional neural networks, Signal Process., Image Commun. 63 (2018) 149–160.

[10] D. Bhardwaj, V. Pankajakshan, A JPEG blocking artifact detector for image forensics, Signal Process., Image Commun. 68 (2018) 155–161.

[11] C. Kumawat, V. Pankajakshan, A robust JPEG compression detector for image forensics, Signal Process., Image Commun. 89 (2020) 116008.

[12] X. Qiu, H. Li, W. Luo, J. Huang, A universal image forensic strategy based on steganalytic model, in: Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security, Salzburg, Austria, Jun. 11-13, 2014.

[13] H. Li, W. Luo, X. Qiu, J. Huang, Identification of various image operations using residual-based features, IEEE Trans. Circuits Syst. Video Technol. 28 (1) (2018) 31–45.

[14] K. Cai, X. Lu, J. Song, X. Wang, Blind image tampering identification based on histogram features, in: 2011 International Conference on Multimedia Information Networking and Security, Shanghai, China, Nov. 4-6, 2011.

[15] Y.-F. Hsu, S.-F. Chang, Statistical fusion of multiple cues for image tampering detection, in: 2008 42nd Asilomar Conference Signals, Systems and Computers, Pacific Grove, CA, USA, Oct. 26-29, 2008.

[16] S. Kumar, M. Hebert, Discriminative random fields, J. Comput. Vis. 68 (2) (2006) 179–201.

[17] G. Chetty, M. Singh, Nonintrusive image tamper detection based on fuzzy fusion, J. Comput. Sci. Netw. Secur. 10 (9) (2010) 86–90.

[18] A. Peng, S. Luo, H. Zeng, Y. Wu, Median filtering forensics using multiple models in residual domain, IEEE Access 7 (2019) 28525–28538.

[19] X. Chu, Y. Chen, K.J.R. Liu, An information theoretic framework for order of operations forensics, in: 2016 International Conference on Acoustics, Speech and Signal Processing, Shanghai, China, Mar. 2049-2053, 2016.

[20] X. Chu, Y. Chen, K.J.R. Liu, Detectability of the order of operations: An information theoretic approach, IEEE Trans. Inf. Forens. Secur. 11 (4) (2016) 823–836.

[21] S. Gao, X. Liao, X. Liu, Real-time detecting one specific tampering operation in multiple operator chains, J. Real-Time Image Process. 16 (2019) 741–750.

[22] M. Fontani, T. Bianchi, A.D. Rosa, A. Piva, M. Barni, A Dempster-Shafer framework for decision fusion in image forensics, in: 2011 IEEE International Workshop on Information Forensics and Security, Iguacu Falls, Brazil, Nov. 29-Dec. 2, 2011.

[23] M. Fontani, T. Bianchi, A.D. Rosa, A. Piva, M. Barni, A framework for decision fusion in image forensics based on Dempster-Shafer theory of evidence, IEEE Trans. Inf. Forens. Secur. 8 (4) (2013) 593–607.

[24] G. Shafer, A Mathematical Theory of Evidence, Princeton University Press, Princeton, NJ, USA, 1976.

[25] G. Wu, Belief function combination and local conflict management, Comput. Eng. Appl. 40 (34) (2004) 81–84.

[26] A.P. Dempster, Upper and lower probabilities induced by a multivalued mapping, Ann. Math. Statist 38 (1967) 325–339.

[27] T. Pevný, P. Bas, J. Fridrich, Steganalysis by subtractive pixel adjacency matrix, IEEE Trans. Inf. Forens. Secur. 5 (2) (2010) 215–224.

[28] P. Bas, T. Filler, T. Pevný, Break our steganographic system: The ins and outs of organizing BOSS, in: 2011 International Workshop on Information Hiding, Berkeley, CA, USA, May. 15-18, 2011.

[29] G. Schaefer, M. Stich, UCID: An uncompressed color image database, in: Proceedings SPIE, Storage and Retrieval Methods and Applications for Multimedia, San Jose, California, USA, Jan. 18, 2004.