Information Sciences 637 (2023) 118961

Contents lists available at ScienceDirect

Information Sciences

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

Identification of image global processing operator chain based on feature decoupling

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

[a] Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
[b] National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China

ARTICLE INFO

Keywords:
Image forensics
Global processing operator chain
Operator chain identification
Feature decoupling

ABSTRACT

Image authenticity verification is an important issue to be studied, which has attracted growing attention recently. Most of the existing forensic methods are aimed at detecting a specific manipulation. However, due to the superimposed processing artifacts caused by using different operations to forge images, the image global processing operator chain identification, which is composed of multiple global manipulations in a certain order, remains a challenge. In this paper, we focus on detecting multiple manipulations and identifying the order of these manipulations. By analyzing the relationship between blind signal separation and operator chain identification, we find that the independent source features of different operations will be coupled when the image is processed by multiple operations, which is similar to what in blind signal separation. Therefore, it is reasonable to formulate the problem of operator chain identification with blind signal separation. Then, a feature decoupling method is proposed to estimate the source feature from the coupled features by optimizing a decoupling matrix. These estimated decoupled features are valid evidence for operator chain identification. For the realistic scenario where images are saved in JPEG format, the comparison with some state-of-the-art methods demonstrates that the proposed method could identify operator chains with better performance.

1. Introduction

Digital images are widely used as important evidence in news reports and forensic testimony due to their intuitive and easy-to-understand [1,2]. However, with the help of image processing techniques [3,4], image editing without leaving any perceptible artifacts has become easy. It is vital to know whether the digital image is authentic and trustworthy. Image forensics is a challenging topic in multimedia security, drawing much attention [5]. It is developed to determine the authenticity, processing history, and origin of digital image content, which can provide evidence for reconstructing who, when, how, and what has been done to the digital image.

Forensic researchers have designed several state-of-the-art techniques to detect a specific global tampering operation, such as resizing [6], blur [7], median filtering [8,9], and JPEG compression [10]. In [7], the authors proposed a Bi-directional Residual Refining network for defocus blur detection, which encoded the spatial details and semantic information to suppress background clutter and enhance the detected blurred region details. In [10], a candidate step function with a similar shape to the DCT coefficients distribution of compressed images is designed for JPEG quantization step estimation. To develop general-purpose image forensic

* Corresponding author.
E-mail address: xinliao@hnu.edu.cn (X. Liao).

https://doi.org/10.1016/j.ins.2023.118961
Received 21 June 2022; Received in revised form 16 November 2022; Accepted 16 April 2023

Available online 20 April 2023

methods that can identify various manipulations simultaneously, authors in [11] and [12] analyzed the properties of local pixels in the residual domain and extracted an effective universal feature set to detect many typical operations. Singh et al. [13] proposed a GIMD network that exploited local dense connections and global residual learning for general-purpose forensics. In [14], the authors proposed a constrained convolutional neural network (CNN) model to detect five different manipulations.

However, the above forensic methods are based on the assumption that the image only undergoes one manipulation. In a realistic scenario, multiple global tampering operations are usually inevitably required to complete an image forgery. There have been some image forensic techniques reported to detect the existence of a single operation in a certain global processing chain composed of JPEG compression and a specific tampering operation (e.g., contrast enhancement [15,16], resampling [17,18]). In [5], a parameters estimation of image operator chain was proposed. In [19], the authors proposed an information theoretical framework to quantify the detectability of tampering operation in operator chains. Considering the order of an image operator chain, a mutual information-based criterion was introduced in [20] to determine when we can or cannot detect the order of operations. Boroumand et al. [21] designed a CNN model to detect the processing history of images. Further, our recent work [22] achieved manipulations detection in an image operator chain by using a decision fusion method to integrate multiple forensic information.

Since the use of multiple operations to falsify an image will cause superimposed processing artifacts, that is, the traces of previous manipulations would be affected by the later manipulations [23]. What is more, applying different manipulations and processing orders will lead to diverse tampering artifacts, making forensics difficult. Thus, the identification of image global processing operator chains is still a challenging issue. In this paper, considering the order of tampering operations, we try to study the superimposed processing artifacts and realize tampering history detection (the existence of manipulations and the order of the involved manipulations detection) in an operator chain.

Due to the superimposed processing artifacts, the artifacts left by different processing operations will be coupled. Image features extracted from fake images are utilized as the mapping of these coupled artifacts. It is worth noting that the extracted features are coupled in an unknown manner. If these features can be decoupled, it means that the artifacts of different operations are decoupled, making the operator chain identification easier. The initial idea of decoupling the tampering artifacts between multiple operations based on our method was proposed in [24], and this paper explores and investigates the global processing operator chain identification method more thoroughly and systematically. The main contributions of this work can be summarized as follows:

1) We analyze the relationship between image processing operator chain identification and blind signal separation. To the best of our knowledge, this is the first attempt to utilize the blind signal separation technique in the image forensics of image operator chains.
2) We design a novel feature decoupling method that decouples the coupled operation features due to the superimposed processing artifacts. Moreover, a processing history detection strategy is introduced, which utilizes these decoupled features as evidence to identify image manipulations and their order in different operator chains.
3) The case study of identifying processing history in an image operator chain composed of two different global tampering manipulations is examined. Experimental results show the effectiveness of our proposed method. Furthermore, our method performs well in general-purpose processing history detection.

The rest of this paper is organized as follows. Section 2 formulates the image operator chain identification issue with blind signal separation. Section 3 describes the proposed feature decoupling method. The strategy of image processing history detection in the operator chain is presented in Section 4. Several experimental analyses are provided in Section 5, the results demonstrate the effectiveness of our method. Section 6 shows the corresponding discussions. Finally, the concluding remarks are given in Section 7.

2. Analysis of image operator chain identification and blind signal separation

In this section, the concept of the image global processing operator chain and the influence of different operator chains on tampering artifacts are described in detail. Further, the operator chain identification is presented from the view of blind signal separation.

2.1. Change of tampering artifacts under different chains

The actual image tampering process is usually more complicated and may include a variety of global tampering operations (e.g., resizing and median filtering), which collectively constitute a complete image processing operator chain in a specific order. Each operation will leave a unique tampering trace in the image. When multiple different operations are used to alter the image continuously, these traces may be superimposed and coupled, resulting in the tampering artifacts of earlier applied operations being destroyed. Moreover, the coupling between traces is related to the order of operations. If the order of operations changes, the final remaining tampering artifacts may also be different.

Fig. 1 provides two different operator chains consisting of the same tampering operations. Inverting the order of median filtering and sharpening in operator chain 1, we get another different operator chain 2. From this figure, it is difficult to find obvious differences between the two images processed by the two operator chains in terms of visual effects. Nevertheless, taking the example of observing the facial pixel values of the two fake images, it can be found that their pixel values are completely different, which also indicates that the artifacts of the tampering manipulations are coupled in a nonlinear way if images are altered by multiple manipulations.

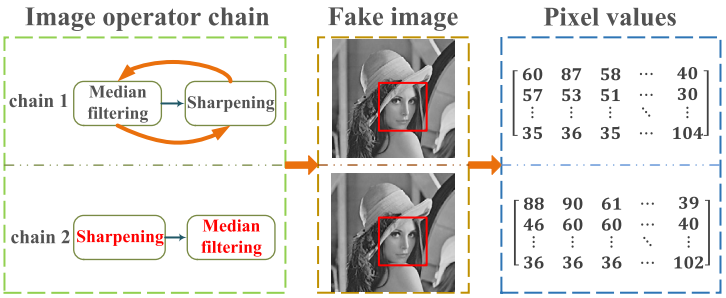


Fig. 1. Illustration of two image global processing operator chains consisting of the same two global manipulations with different orders.

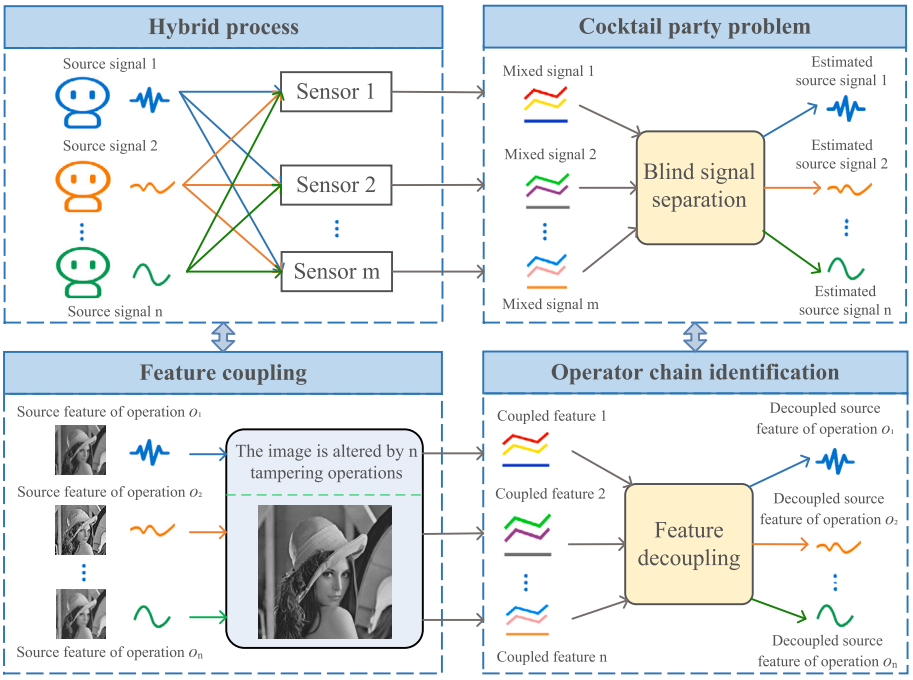


Fig. 2. The relationship between operator chain identification and blind signal separation.

2.2. Relationship between image operator chain identification and blind signal separation

In the case where the source signals are independent, the blind signal separation technique can recover the unknown source signals from the observed mixed signals [25]. The cocktail party problem [26] is one of the most widely applied examples of blind signal separation, which aims at obtaining the distinctive voice signal of each person speaking at the same time at the cocktail party. Supposing there are n guests participating in the cocktail party, and m microphones are scattered around the room to record the voice signals of the guests, where $m \geq n$. The voice signal of each guest can be viewed as a source signal. When n guests communicate with each other, their voice signals are superimposed on each other, and m microphones simultaneously record the voice signals of each guest. In addition, due to the different distances between the guests and the microphones, the voice signals of n guests recorded by the m microphones are different. Consequently, the microphones will receive several diverse mixed voice signals. For achieving the purpose of deriving each guest's unique voice signal from these mixed signals, the blind signal separation technique is utilized.

Analogously, when applying a tampering operation to alter an image, comparing the operation to a guest attending a cocktail party, the independent feature extracted from the image is the same as the voice signal of a guest. If the image experiences multiple operations, the traces left by various single tampering operations may have a superimposed and coupling effect. Then, we will derive coupled features from the fake image, which are similar to the mixed voice signals recorded by microphones. Thus, a reasonable thought is to apply blind signal separation technology to perform image processing history detection in an operator chain.

Specifically, as demonstrated in Fig. 2, we have n possible operations $\{o_1, o_2, \cdots, o_n\}$ may be applied to complete an image falsification. Since each tampering operation used to modify an image would destroy the statistical properties of the image, we should choose a valid feature to achieve the identification of the image operator chain. For the processing operation o_i, there exists an independent source feature. However, when images are altered by n tampering operations $\{o_1, o_2, \cdots, o_n\}$, the trace of the previous operation o_i

might be affected by the later operation o_j, where $1 \le i < j \le n$ in an unknown way. Therefore, the image features we extracted from the given image are coupled features processed by multiple tampering operations. While in the cocktail party problem, m sensors in the hybrid process are used for recording source signals and the outputs from these sensors are mixed signals. If the hybrid process in the cocktail party problem is regarded as the process of continuously using n specific tampering operations to falsify images, then the coupled features extracted from the image can be viewed as the mixed signals obtained by m sensors.

The tasks of image operator chain identification and the cocktail party problem would become similar. That is, just as the blind signal separation technique is used to estimate the source signals from the observed mixed ones in the cocktail party problem, in the image operator chain identification issue, we can derive the decoupled source features of processing operations by exploiting a feature decoupling method based on blind signal separation. It can simplify the processing history identification in the image operator chain composed of tampering operations $\{o_1, o_2, \cdots, o_n\}$.

Inspired by the idea of blind signal separation, an image global processing operator chain detection method is proposed, which utilizes feature decoupling to identify the manipulations and their order in an image operator chain.

3. The proposed feature decoupling method

In this section, we first illustrate the detailed idea of the proposed feature decoupling method. Then, a metric property for the feature decoupling performance is introduced. Finally, the time complexity of our method is analyzed.

3.1. Blind signal separation based feature decoupling method

It is well known that the inherent statistical characteristics of an image will inevitably be distorted if the image is falsified by a tampering operation. While applying multiple tampering operations on an image will result in superimposed processing artifacts, making the image processing history difficult to identify. According to this analysis, we study how to obtain the decoupled source feature of each operation through feature decoupling based on blind signal separation.

Supposing that n possible tampering operations may be utilized to forge m digital images, where $m \ge n$. Let $I = \{I_1, I_2, \cdots, I_m\}$ and $O = \{o_1, o_2, \cdots, o_n\}$ represent the set of fake images and tampering operations. Because n operations are linearly applied to the image, the artifacts left by operations $\{o_1, o_2, \cdots, o_n\}$ are linearly superimposed on the image. Besides, if these operations are applied to images in a different order, the artifacts of the final image might be disparate, which shows that the latter operations have a nonlinear coupling effect on the artifacts left by the previous operations. As a result, the tampering artifacts of operations $\{o_1, o_2, \cdots, o_n\}$ are coupled in an unknown nonlinear way, image features as the mapping of tampering artifacts are also coupled in this way.

Definition 1. Let $\boldsymbol{s}_i$ denote the intrinsic operation feature of operation o_i. The nonlinear coupling function g and coupling matrix $\boldsymbol{A}$ represent the coupling way, where $\boldsymbol{A} \in \mathbb{R}^{m \times n}$. Then, the feature coupling process in an operator chain can be formulated as

$$\begin{bmatrix} \boldsymbol{f}_1 \\ \boldsymbol{f}_2 \\ \vdots \\ \boldsymbol{f}_m \end{bmatrix} = g\left(\begin{bmatrix} \boldsymbol{A}_{1,:} \\ \boldsymbol{A}_{2,:} \\ \vdots \\ \boldsymbol{A}_{m,:} \end{bmatrix} \begin{bmatrix} \boldsymbol{s}_1 \\ \boldsymbol{s}_2 \\ \vdots \\ \boldsymbol{s}_n \end{bmatrix} \right), \tag{1}$$

where $\boldsymbol{f}_i$ denotes the coupled feature extracted from I_i directly. The dimension of $\boldsymbol{f}_i$ and $\boldsymbol{s}_i$ are d. $\boldsymbol{A}_{i,:}$ represents the i^{th} row in the coupling matrix $\boldsymbol{A}$.

Definition 2. Let p and $\boldsymbol{W}$ ($\boldsymbol{W} \in \mathbb{R}^{n \times m}$) denote a nonlinear decoupling function and a decoupling matrix. By multiplying the matrix and function, the decoupled operation features $\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_n]^T$ can be transformed.

$$\begin{bmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \\ \vdots \\ \boldsymbol{y}_n \end{bmatrix} = \begin{bmatrix} \boldsymbol{W}_{1,:} \\ \boldsymbol{W}_{2,:} \\ \vdots \\ \boldsymbol{W}_{n,:} \end{bmatrix} p\left(\begin{bmatrix} \boldsymbol{f}_1 \\ \boldsymbol{f}_2 \\ \vdots \\ \boldsymbol{f}_m \end{bmatrix} \right), \tag{2}$$

where $\boldsymbol{y}_i$ denotes an estimate of the source operation feature $\boldsymbol{s}_i$ and $\boldsymbol{W}_{i,:}$ is the i^{th} row in the decoupling matrix $\boldsymbol{W}$.

Proof. If $p = g^{-1}$ represents the inverse function of the nonlinear coupling function g, then

$$\begin{aligned} p([\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_m]^T) &= p(g(\boldsymbol{A}[\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_n]^T)) \\ &= g^{-1}(g(\boldsymbol{A}[\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_n]^T)) \\ &= \boldsymbol{A}[\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_n]^T. \end{aligned} \tag{3}$$

What is more, if $\boldsymbol{W} = \boldsymbol{A}^{+}$ represents the pseudo inverse matrix of $\boldsymbol{A}$, the following formula exists,

$$\boldsymbol{W}\boldsymbol{A} = \begin{bmatrix} \boldsymbol{W}_{1,:}\boldsymbol{A}_{:,1} & 0 & \cdots & 0 \\ 0 & \boldsymbol{W}_{2,:}\boldsymbol{A}_{:,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{W}_{n,:}\boldsymbol{A}_{:,n} \end{bmatrix}, \tag{4}$$

where $\boldsymbol{A}_{:,i}$ is the i^{th} column in the coupling matrix $\boldsymbol{A}$. Because $\boldsymbol{W}$ is the pseudo inverse matrix of $\boldsymbol{A}$, the following constraint is satisfied,

$$\boldsymbol{W}_{i,:}\boldsymbol{A}_{:,i} = 1, 1 \le i \le n. \tag{5}$$

Thus, feature decoupling can be formulated by decoupling matrix $\boldsymbol{W}$, decoupling function p and observed coupled features $\boldsymbol{F} = [\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_m]^T$. The decoupled feature $\boldsymbol{y}_i$ corresponding to operation o_i can be transformed as

$$\begin{aligned} \begin{bmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \\ \vdots \\ \boldsymbol{y}_n \end{bmatrix} &= \begin{bmatrix} \boldsymbol{W}_{1,:} \\ \boldsymbol{W}_{2,:} \\ \vdots \\ \boldsymbol{W}_{n,:} \end{bmatrix} \begin{bmatrix} \boldsymbol{A}_{1,:} \\ \boldsymbol{A}_{2,:} \\ \vdots \\ \boldsymbol{A}_{m,:} \end{bmatrix} \begin{bmatrix} \boldsymbol{s}_1 \\ \boldsymbol{s}_2 \\ \vdots \\ \boldsymbol{s}_n \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{W}_{1,:}\boldsymbol{A}_{:,1} & 0 & \cdots & 0 \\ 0 & \boldsymbol{W}_{2,:}\boldsymbol{A}_{:,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \boldsymbol{W}_{n,:}\boldsymbol{A}_{:,n} \end{bmatrix} \begin{bmatrix} \boldsymbol{s}_1 \\ \boldsymbol{s}_2 \\ \vdots \\ \boldsymbol{s}_n \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} \boldsymbol{s}_1 \\ \boldsymbol{s}_2 \\ \vdots \\ \boldsymbol{s}_n \end{bmatrix} = \begin{bmatrix} \boldsymbol{s}_1 \\ \boldsymbol{s}_2 \\ \vdots \\ \boldsymbol{s}_n \end{bmatrix}. \end{aligned} \tag{6}$$

Since the nonlinear coupling function g and coupling matrix $\boldsymbol{A}$ are unknown, it is difficult to directly calculate the inverse function p and pseudo inverse matrix $\boldsymbol{W}$. Our goal is to find the decoupling function p and matrix $\boldsymbol{W}$. Thus, it is possible to obtain the decoupled feature $\boldsymbol{y}_i$ that represents the source operation feature $\boldsymbol{s}_i$. Then, the decoupled operation features $\boldsymbol{Y}$ can be effective resources to detect the image processing history in an operator chain.

In order to decouple the coupled features $\boldsymbol{F}$ extracted from m fake images, feature whitening emerges as a feature decoupling preprocessing technique that attempts to estimate independent source features of tampering operations from the coupled features $\boldsymbol{F}$ by transforming $\boldsymbol{F}$ into uncorrelated features and then rescaling features to be with unit variance. Through the whitening process, the correlation of coupled features is weakened and redundant information is reduced, thereby helping feature decoupling.

We use the classical Sphering method [27] based on the eigenvalue decomposition of the covariance matrix to whiten $\boldsymbol{F}$. The whitening process can be formulated by whiten matrix $\boldsymbol{V}$ and coupled features $\boldsymbol{F}$,

$$\boldsymbol{Z} = \boldsymbol{V}\boldsymbol{F}, \tag{7}$$

where $\boldsymbol{Z} = [\boldsymbol{z}_1, \boldsymbol{z}_2, \cdots, \boldsymbol{z}_m]^T$ represents the whitened features matrix. It should be noted that the matrix $\boldsymbol{V}$ is formulated as follows,

$$\boldsymbol{V} = \boldsymbol{\Lambda}^{-\frac{1}{2}}\boldsymbol{U}^T, \tag{8}$$

where $\boldsymbol{\Lambda}$ and $\boldsymbol{U}$ denote the diagonal matrix with the eigenvalues of the covariance matrix of $\boldsymbol{F}$ as diagonal elements and the matrix with the eigenvector corresponding to each eigenvalue as a column, respectively.

In the following analysis, we use the whitened features $\boldsymbol{Z} = [\boldsymbol{z}_1, \boldsymbol{z}_2, \cdots, \boldsymbol{z}_m]^T$ as input data and the decoupled features $\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_n]^T$ can be calculated based on Eq. (2),

$$\begin{bmatrix} \boldsymbol{y}_1 \\ \boldsymbol{y}_2 \\ \vdots \\ \boldsymbol{y}_n \end{bmatrix} = \begin{bmatrix} \boldsymbol{W'}_{1,:} \\ \boldsymbol{W'}_{2,:} \\ \vdots \\ \boldsymbol{W'}_{n,:} \end{bmatrix} p'\left(\begin{bmatrix} \boldsymbol{z}_1 \\ \boldsymbol{z}_2 \\ \vdots \\ \boldsymbol{z}_m \end{bmatrix} \right). \tag{9}$$

Because we will decouple the whitened feature $\boldsymbol{z}_i$ instead of directly decouple the coupled feature $\boldsymbol{f}_i$ extracted from the image, let $\boldsymbol{W'}$ and p' represent the decoupling matrix and function corresponding to the whitened features matrix $\boldsymbol{Z}$. $\boldsymbol{W'}_{i,:}$ denotes the i^{th} row in the matrix $\boldsymbol{W'}$.

In our work, we test three commonly used nonlinear functions to simulate the inverse function of the coupling function. Through experiments, the hyperbolic tangent function is determined as the optimal inverse function p' in the feature decoupling process to decouple the whitened features $\boldsymbol{Z}$,

$$p'(\boldsymbol{z}_i) = \frac{e^{\boldsymbol{z}_i} - e^{-\boldsymbol{z}_i}}{e^{\boldsymbol{z}_i} + e^{-\boldsymbol{z}_i}}. \tag{10}$$

Algorithm 1 The feature decoupling algorithm.

Require: $\boldsymbol{F} = [\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_m]^T$: the observed coupled features
Ensure: $\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_n]^T$: the decoupled operation features
1: Estimate the whiten matrix $\boldsymbol{V}$ and compute the whitened features matrix $\boldsymbol{Z} = \boldsymbol{V}\boldsymbol{F}$
2: The inverse function $p'(\boldsymbol{z}_i) = \frac{e^{z_i} - e^{-z_i}}{e^{z_i} + e^{-z_i}}$
3: Randomly initialize matrix $\boldsymbol{W}'$
4: Initialize iteration times $t = 1$, $max_{iter} = 1000$
5: **repeat**
6: Compute $\boldsymbol{W}'_{i,:}(t+1) = E[p'(\boldsymbol{Z})(\boldsymbol{W}'^T_{i,:}(t)p'(\boldsymbol{Z}))^3] - 3\boldsymbol{W}'_{i,:}(t)$
7: Compute $\boldsymbol{W}'_{i,:}(t+1) = \frac{\boldsymbol{W}'_{i,:}(t+1)}{\|\boldsymbol{W}'_{i,:}(t+1)\|}$
8: **if** $||\boldsymbol{W}'(t+1)\boldsymbol{W}'^T(t) - 1||$ converges **then**
9: exit
10: **else**
11: return to step 6
12: **end if**
13: **until** $(t = max_{iter})$
14: Compute the decoupled features $\boldsymbol{Y} = \boldsymbol{W}'p'\boldsymbol{Z}$

Furthermore, to calculate the optimal decoupling matrix $\boldsymbol{W}'$, we utilize the fixed-point algorithm [28] based on the fourth-order cumulant. The calculation formula can be expressed as,

$$\begin{cases} \boldsymbol{W}'_{i,:}(t+1) = E[p'(\boldsymbol{Z})(\boldsymbol{W}'^T_{i,:}(t)p'(\boldsymbol{Z}))^3] - 3\boldsymbol{W}'_{i,:}(t), \\ \boldsymbol{W}'_{i,:}(t+1) = \frac{\boldsymbol{W}'_{i,:}(t+1)}{\|\boldsymbol{W}'_{i,:}(t+1)\|}, \end{cases} \tag{11}$$

where t represents iteration times, $E[\cdot]$ denotes the mean value of the sampled values of $\boldsymbol{Z}$, and $\|\cdot\|$ is matrix norm.

The decoupled features $\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_n]^T$ could be calculated as described in Algorithm 1, where $\boldsymbol{y}_i$ can be regarded as an estimated feature of the corresponding tampering operation o_i and provide a direct evidence for the forensics of the image operator chain composed of operations $\{o_1, o_2, \cdots, o_n\}$.

3.2. Metric property

Given that there exist different tampering artifacts and coupled features in the image operator chain with different tampering operations $\{o_1, o_2, \cdots, o_n\}$, the deviations between the decoupled features $\{\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_n\}$ obtained by the proposed feature decoupling method and the intrinsic operation features $\{\boldsymbol{s}_1, \boldsymbol{s}_2, \cdots, \boldsymbol{s}_n\}$ in diverse operator chains are different. Nevertheless, the more similar the decoupled feature $\boldsymbol{y}_i$ is to the corresponding intrinsic operation feature $\boldsymbol{s}_i$, the more accurate the processing history detection in operator chains.

Because the magnitude of the decoupled features is different from that of the intrinsic operation features, we first normalize the two kinds of features. For detecting whether the feature decoupling can effectively estimate the feature of each operation in an operator chain, the formula used for calculating the cosine distance between the decoupled operation feature $\boldsymbol{y}_i$ and the source operation feature $\boldsymbol{s}_i$ is as follows,

$$\begin{cases} sim_i = \frac{\sum_{j=1}^{d}(\boldsymbol{y}_{ij}\boldsymbol{s}_{ij})}{\sqrt{\sum_{j=1}^{d}\boldsymbol{y}_{ij}^2} \times \sqrt{\sum_{j=1}^{d}\boldsymbol{s}_{ij}^2}}, \\ dis = 1 - \frac{1}{n}\sum_{i=1}^{n} sim_i, \end{cases} \tag{12}$$

where n and d are the number and dimension of operation features, respectively. The range of sim_i is $[-1, 1]$. Thus, the range of cosine distance dis is $[0, 2]$.

The purpose of feature decoupling is to recover the source operation features from the coupled features as much as possible. Thus, the smaller the value of dis, the smaller the distance between the decoupled features and the source features, which indicates that the decoupled features are similar to the source features and the decoupling performance of the proposed method is better.

As long as the feature decoupling performance is great, the decoupled features $\boldsymbol{Y} = [\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_n]^T$ could be applied to identify the existence of manipulations and distinguish the order of these manipulations in an operator chain.

3.3. Time complexity analysis

For the proposed feature decoupling method used to detect processing history in different image operator chains, we could analyze the time complexity.

Suppose there are n possible tampering operations $\{o_1, o_2, \cdots, o_n\}$ are applied to forge m images, then we will obtain m coupled features $\boldsymbol{F} = [\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_m]^T$ extracted from the m fake images, where the dimension of coupled feature $\boldsymbol{f}_i$ is d. Analyzing the computational complexity of the process of whitening the coupled features, because each value of feature $\boldsymbol{f}_i$ is calculated, so the

whitening process is related to the number and dimension of the coupled features $\boldsymbol{F}$. Besides, the dimension d is a constant, that is, the complexity is $O(m \times d) = O(m)$.

According to Eq. (9), our feature decoupling method is formulated by decoupling matrix $\boldsymbol{W}'$ ($\boldsymbol{W}' \in \mathbb{R}^{n \times m}$), decoupling function p' and whitened coupled features $\boldsymbol{Z}$ ($\boldsymbol{Z} \in \mathbb{R}^{m \times d}$). We find that the use of decoupling function p' for nonlinear transformation is mainly concerned with the whitened coupled features $\boldsymbol{Z}$, as a result, the time complexity is also $O(m \times d) = O(m)$.

When computing a decoupling matrix $\boldsymbol{W}'$ and converting features processed by nonlinear transformation into n decoupled source features of operations corresponding to operations $\{o_1, o_2, \cdots, o_n\}$, as described in Eq. (11), it is observed that the iteration variable is the decoupling matrix $\boldsymbol{W}'$ and the process of finding the matrix is a linear iterative process. We specify the iteration times is t, then the multiplication computation is $n \times m \times t$. Since the involved n and m are variables and they have to satisfy $m \geq n$, the time complexity of this process is $O(m \times n) = O(m^2)$.

In summary, the time complexity of the feature decoupling method is $O(m + m + m^2) = O(m^2)$. That is, the image tampering history detection in an operator chain via feature decoupling could be achieved in polynomial time.

4. Image processing history detection strategy in an operator chain

In this section, to meet the requirements of blind signal separation, we first introduce some image expansion methods to increase image quantity. Then, the strategy of image processing history detection is presented.

4.1. The image expansion methods

The fixed-point algorithm requires the number of mixed signals observed in each sensor no less than the number of source signals [28]. However, for each given image, it can only be viewed as one observation channel. We can only extract one feature from each given image when the features of n possible operations have been determined. Therefore, for the forensics of processing history in the image operator chain, appropriate image expansion is required for each investigated image to obtain m ($m \geq n$) observation channels. In our work, we can derive images from various angles through image expansion, and the features extracted from these expanded images in different respects are the observation channels we need. The commonly used image expansion methods have been diversified in the following manner.

- Rotating. Specifically, rotating a suspected image 30 degree by a bilinear interpolation algorithm and then cropping the rotated image to the same size as the investigated image. The bilinear interpolation can be formulated as

$$I'(x,y) = \begin{bmatrix} 1-x & x \end{bmatrix} \begin{bmatrix} I(x_1,y_1) & I(x_1,y_2) \\ I(x_2,y_1) & I(x_2,y_2) \end{bmatrix} \begin{bmatrix} 1-y \\ y \end{bmatrix}, \tag{13}$$

  where $I(x_1, y_1)$, $I(x_1, y_2)$, $I(x_2, y_1)$ and $I(x_2, y_2)$ are the known values of four pixels in the image I. Besides, $I'(x, y)$ denotes the value of the newly inserted pixel at coordinate (x, y). To generate m images, the image rotation will be performed on the rotated image.
- Cropping. Namely, cropping a given image to m new images with the same size.
- Adding Gaussian noise. Precisely, adding Gaussian noise with zero mean to a given image, which is calculated as

$$I'(x,y) = \frac{1}{\sqrt{2\pi}\delta} e^{-\frac{I(x,y)}{2\delta^2}}, \tag{14}$$

  where $\delta = 0.1$, $I(x, y)$ and $I'(x, y)$ represent the initial value of the pixel point with coordinate (x, y) and the value after adding noise, respectively. Then, by performing image expansion on a new image with Gaussian noise, one image can be expanded into m images.

Note that we focus on the identification of tampering history in this paper, while the expansion of an image is actually equivalent to applying an operation to forge it. Such kind of operation is not included in the tampering process we consider. Thus, the impact of expansion operation on the image should be minimized. Meanwhile, the purpose of using image expansion is to provide multiple observation features in various respects and exploit them to restore the source operation features. To a certain extent, the expanded images should be different from the original image, so that we can obtain coupled features from multiple aspects. Through experimental results, we find that rotation is a suitable approach to expanding the image. Please see Section 5.3 for details.

4.2. The implementation of image processing history detection

In practical scenarios, a forger usually modifies an image using different tampering operations, which can be combined in any order or topology to generate multiple operator chains [5,19,20]. For example, we use two global manipulations, such as median filtering and resizing, to fake an image. The manipulations are used in different orders, which will generate different processing operator chains. That is the image is forged by median filtering followed by resizing, which constitutes an operator chain. If the order is swapped, i.e. the image is processed first with resizing and then with median filtering, a new operator chain would be formed. Applying different operator chains to fake an image, the resulting images are also different.

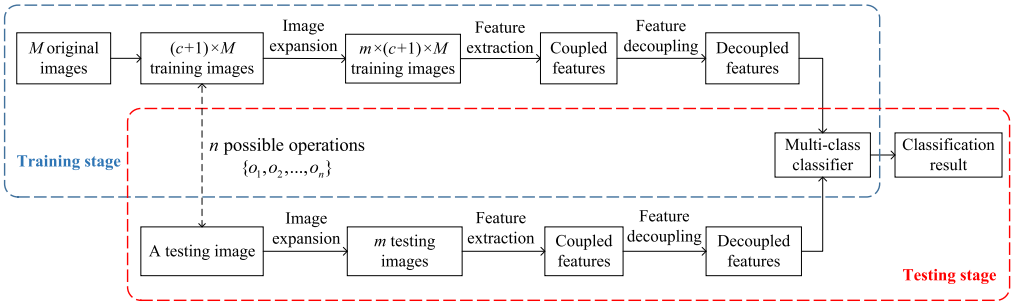


Fig. 3. Implementation strategy of image processing history detection in an operator chain.

The image processing history detection in an operator chain with supervised learning can be performed as illustrated in Fig. 3. Our goal includes not only identifying the type of operations, but also detecting the order of those operations. Assuming that there are n possible global operations $\{o_1, o_2, \cdots, o_n\}$ utilized to falsify a testing image, where $n \geq 1$. The image processing history detection strategy consists of training and testing stages.

In the training stage, we first collect M original images. When utilizing n possible operations to forge an original training image, $c + 1 = \sum_{i=1}^{n} A_n^i + 1$ kinds of training images can be generated. Notice that the $c + 1$ images include the classes of the original image itself and images forged by A_n^k kinds of tampering operations, where $1 \leq k \leq n$. For each training image, as the number of images should be no less than the number of operations, we expand it into m $(m \geq n)$ training images by employing a reasonable image expansion method. Hence, we will obtain $m \times (c + 1) \times M$ images.

To improve the forensics performance, determining a valid feature to map the trace of tampering operation is of significance. Then, we extract features from $m \times (c + 1) \times M$ training images. Considering that multiple operations may cause superimposed processing artifacts and couple the feature of each operation, it is necessary to distinguish the different features left by utilizing tampering operations to alter images. For addressing this problem, we adopt our method to recover n decoupled operation features from the coupled features extracted from training images. Meanwhile, when an image has experienced multiple processing operations, there will exist decoupled features of different operations after using feature decoupling. If a single decoupled feature is employed for processing history detection in the operator chain, it may not be able to fully recognize the processing history of the image that has undergone multiple manipulations. By cascading the n decoupled features into a new feature vector, it can effectively detect whether the image has tampered with multiple operations. Finally, the new feature is used to train a multi-class classifier.

In the testing stage, the same as the training stage, assuming that the testing image is modified by n tampering operations $\{o_1, o_2, \cdots, o_n\}$. In order to meet the requirement of feature decoupling that the number of observed images needs to be greater than or equal to the number of operations, we should expand the testing image to m testing images based on an applicable image expansion method. Then, we could extract m features from these m testing images. Due to the superimposed processing artifacts, the m features are coupled features, making it difficult to detect image tampering history. By exploiting our feature decoupling method, we could derive n decoupled operation features from m coupled features. Furthermore, the n decoupled features are expressed as a new feature vector, which is fed to the obtained multi-class classifier in the training stage to get the forensics results of the image operator chain.

Based on the strategy presented in Fig. 3 with supervised learning, we can complete the detection of image processing history in different image global processing operator chains.

5. Experimental results

In this section, following the experimental setup, we first determine the feature sets which are utilized for forensics of image processing history in different image operator chains. Secondly, the correlation of the features between the suspected image and the expanded image is analyzed. Thirdly, we simulate the process of feature coupling and decoupling. Then, we study the feature decoupling performance. Furthermore, considering a scenario where the image is forged by two different tampering operations and the processed image is stored in the JPEG format, several experiments are conducted as examples to demonstrate the effectiveness of our proposed method. We also provide the performance comparisons of the proposed method with state-of-the-art methods. Finally, we show the performance of our method when dealing with general-purpose processing history identification.

5.1. Experimental setup

In practice, images are usually JPEG compressed during the process of digital camera imaging to save storage space. When completing an image forgery, a forger may use some global tampering operations to change the content of the image, and then save the tampered image again in JPEG format [18]. Therefore, we investigate the scenario where tampered images are double JPEG compressed. In the image operator chain identification problem, assuming an image operator chain might contain two processing manipulations A and B. For a given image, we consider the following five hypotheses for possible processing history.

$$\begin{aligned}
&H_0: \text{It is double compressed with quality factors } QF_1 \text{ then } QF_2,\\
&H_1: \text{It is double compressed with quality factors } QF_1 \text{ then } QF_2 \text{ interleaved by } A,\\
&H_2: \text{It is double compressed with quality factors } QF_1 \text{ then } QF_2 \text{ interleaved by } B,\\
&H_3: \text{It is double compressed with quality factors } QF_1 \text{ then } QF_2 \text{ interleaved by } A \text{ then } B,\\
&H_4: \text{It is double compressed with quality factors } QF_1 \text{ then } QF_2 \text{ interleaved by } B \text{ then } A.
\end{aligned} \tag{15}$$

Given that JPEG compression will lead to distortion in image adjacent blocks, different JPEG compression parameters will produce a different effect on the traces of processing manipulations. Specifically, the smaller the compression quality factor (QF), the more image details are lost, making the image more distorted. In order to prove that our method can effectively detect the operator chain in any JPEG compression scenario, the parameter settings of double JPEG compression are divided into three types, namely $QF_1 > QF_2$, $QF_1 < QF_2$, and $QF_1 = QF_2$.

In this study, 2,000 images from the BOSSbase database [29] and 1,000 images from the UCID database [30] are utilized to create a training database and a testing database, respectively. We first convert these images into gray-scale images. According to Eq. (15), we perform corresponding operations on the training images and the testing images to generate a set of forged images. Therefore, a total of 10,000 training images and 5,000 testing images are obtained.

To verify the proposed detection method, some typical image manipulations, i.e., median filtering (MF), sharpening with a Gaussian kernel (SP), and resizing (RS), are applied to forge images. Every two different operations are used to collectively constitute an image operator chain,

- The chain consists of median filtering and resizing (MF & RS).
- The chain consists of resizing and sharpening (RS & SP).
- The chain consists of median filtering and sharpening (MF & SP).

All the experiments are performed using a support vector machine (SVM) classifier. We employ the polynomial kernel as the kernel function. The degree and gamma parameters of the function are 2 and 2.8, respectively.

5.2. Feature sets

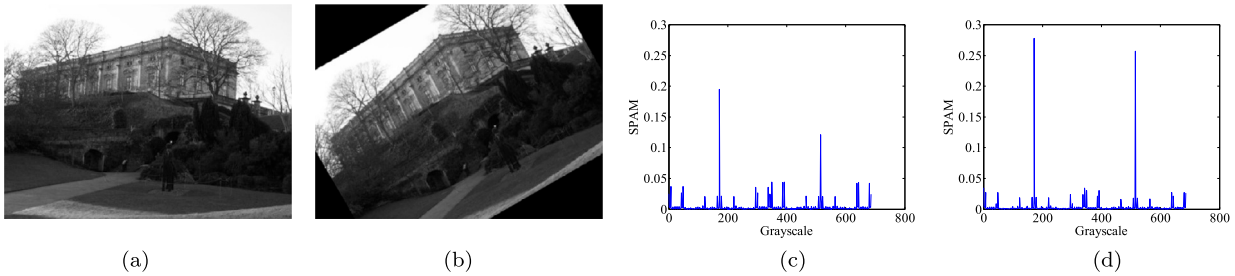
The consistency between adjacent pixels of the original image will be destroyed when applying global tampering operations to falsify an image. For example, median filtering will affect the distribution of differences between adjacent pixels, the image sharpening is an image enhancement operation that will enhance image contrast and sharpen the edges, while the image resizing operation will lead to the image's periodic artifact which may alter spatial correlations among adjacent pixels.

For detecting the image processing history, it is necessary to find a feature that is based on the artifacts of operations experienced by the image. It should be pointed out that our method is universal for the image manipulation history detection in an operator chain composed of n ($n \geq 1$) tampering operations. Using forensic features designed for a specific tampering operation to identify operator chains, detection performance degrades as different operations leave unique forgery traces in the image. In order to detect different operations, we give priority to universal forensic features. As demonstrated in [11], tampering operations will modify image pixels without considering the inherent properties within the original image, which is similar to steganography. It is reasonable to model various operations as steganography and it is useful to detect them with some universal steganalysis features. In addition, the dimensionality of most modern steganalysis features is relatively large, for example, the dimensionality of the spatial rich model (SRM) is 34,671. This makes both feature extraction and classifier training time-consuming. Therefore, we evaluate the performances of a typical steganalysis feature, i.e. subtractive pixel adjacency matrix (SPAM) [31] (the dimensionality is 686), for image processing history detection.

Since multiple manipulations will cause superimposed processing artifacts, the SPAM feature extracted from the image that has experienced multiple tampering operations is coupled. If the coupled features are utilized directly for detecting the processing history in an image operator chain, the results might not be very well because the universal feature SPAM is designed based on the assumption that the image has only undergone one tampering operation. However, if the coupled features have been decoupled by utilizing our proposed method, then we believe that the decoupled features are reasonable resources to detect the processing history.

5.3. Feature correlation analysis

As demonstrated in Fig. 3, each suspected image should be performed with an appropriate image expansion method to obtain two different angles of observation channels. We have introduced three kinds of image expansion manners, i.e., rotating, cropping, and adding Gaussian noise. Because the image generated by image expansion will be slightly different from the original image, the features extracted from the two images will also be different. However, the expansion operation is not included in the scope of the tampering operations that we consider, consequently, we choose the image expansion method that has the least impact on image



(a) (b) (c) (d)

Fig. 4. The illustration of the correlation between a gray image I (a) and its expanded image I' (b). Plotted are the SPAM features extracted from image I (c) and the SPAM feature extracted from expanded image I' (d).

features to reduce the effect of the image expansion operation on the processing history forensics, while ensuring that the observed features are obtained from diverse aspects.

We evaluate the impact on image features by analyzing the correlation between the feature $\boldsymbol{f}_I$ extracted from investigated image I and the feature $\boldsymbol{f}_{I'}$ extracted from expanded image I'. We calculate the correlation coefficient between these two features and the formula is presented below,

$$\rho = \frac{cov(\boldsymbol{f}_I, \boldsymbol{f}_{I'})}{\sqrt{D(\boldsymbol{f}_I)} \times \sqrt{D(\boldsymbol{f}_{I'})}}, \tag{16}$$

where $cov(\boldsymbol{f}_I, \boldsymbol{f}_{I'})$ represents the covariance of the features $\boldsymbol{f}_I$ and $\boldsymbol{f}_{I'}$. Besides, $D(\boldsymbol{f}_I)$ and $D(\boldsymbol{f}_{I'})$ denote the variances of the features $\boldsymbol{f}_I$ and $\boldsymbol{f}_{I'}$, and the range of ρ is $[-1, 1]$. Note that the larger the absolute value of ρ, the greater the correlation between $\boldsymbol{f}_I$ and $\boldsymbol{f}_{I'}$. Namely, the less the influence of the image expansion operation on the features of tampering operations.

We use 1,000 images to test the correlation between the original images and the expanded images. For each image, we apply three kinds of image expansion methods to expand it into two images respectively. As we have determined to use the SPAM feature to evaluate our proposed method, therefore, we need to verify the effect of image expansion on the SPAM feature. The correlation coefficient between the feature of each given image and the corresponding expanded image is calculated based on Eq. (16). The average correlation coefficients via rotating, cropping, and adding Gaussian noise are 0.799, 0.697, and 0.419, respectively. The results indicate that the coupling effect of rotation on the features of image tampering operations is less than that of the other two expansion manners. That is, the image expansion by rotating the given image is better than the other two expansion methods.

What is more, we even observe the feature change of the given image and the expanded image when applying a rotation to achieve image expansion. As shown in Fig. 4, a gray testing image I is used as the object of analysis. We then create a new image I' via rotating the testing image I 30 degree and then cropping it to the same size as the image I. From Figs. 4(a) and 4(b), we can see that the difference between the gray image and the expanded image mainly lies in the details of the image edges. Furthermore, we calculate the correlation coefficient between the two features shown in Figs. 4(c) and 4(d) based on Eq. (16). The similarity between them is 0.722, which indicates that the feature distribution of the image I and I' is similar. In addition, it can be observed that the amplitude of the feature values exists differently. These different results provide various pieces of information to decouple the observed features. At the same time, the influence of the image expansion method on the processing operations features is minimized.

5.4. Simulation of feature coupling and decoupling

When processing history identification in different operator chains is solved by using blind signal separation, it needs to be pointed out that the independent source signal refers to the feature extracted from the tampered image with only one processing operation, and the mixed signal refers to the feature extracted from the tampered image with multiple manipulations. Taking the history detection in the operator chain composed of median filtering and resizing as an example, the process of feature coupling and decoupling is simulated.

In Fig. 5(a), the SPAM features $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ are extracted from a median filtered image and a resized image, respectively. We can find that each operation has its unique source feature. Let $\boldsymbol{S} = [\boldsymbol{s}_1, \boldsymbol{s}_2]^T$ denote the source features matrix, where $\boldsymbol{S} \in \mathbb{R}^{2\times 686}$. We calculate the rank of matrix $\boldsymbol{S}$ and find that $rank(\boldsymbol{S}) = 2$. The result reports that the matrix $\boldsymbol{S}$ is row full rank. That is the two SPAM features of median filtering and resizing are linearly independent and meet the requirements of source signal independence for blind signal separation.

We use the inverse hyperbolic tangent function g and randomly generate a coupling matrix $\boldsymbol{A}$ to simulate the coupling process of two source operation features based on Eq. (1). The function g is as follows,

$$g(\boldsymbol{AS}) = \frac{1}{2} \ln \frac{1 + \boldsymbol{AS}}{1 - \boldsymbol{AS}}. \tag{17}$$

The coupled features are shown in Fig. 5(b). It can be observed that the distribution of features $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ becomes similar after nonlinear coupling, and the two features disguise each other, which is consistent with the superimposed processing artifacts caused by multiple falsifications. Then, we employ the proposed method to decouple the obtained coupled features, and the estimated decoupled features of tampering operations are provided in Fig. 5(c). We can see that although the magnitude of the decoupled

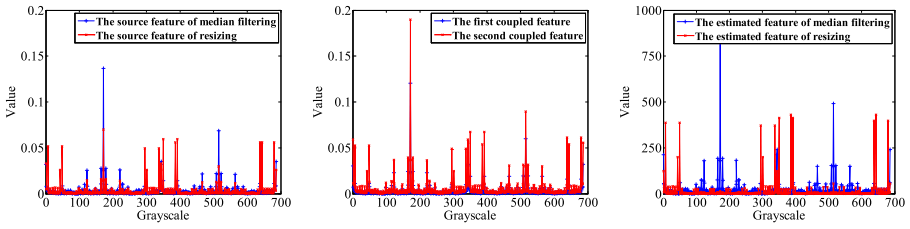


Fig. 5. The illustration of SPAM feature coupling and decoupling. Plotted are the source features extracted from images that have only experienced one tampering operation (a), the features obtained by coupling the source features (b), and the decoupled features recovered from the coupled features using feature decoupling (c).

Table 1
The cosine distance between the decoupled features and source features when applying different nonlinear decoupling functions.

Decoupling functions	MF & RS	RS & SP	MF & SP
$p_1'(z_i) = 10 + 2\log(1 + z_i)$	0.9506	1.2814	1.2455
$p_2'(z_i) = \frac{1}{1+e^{-z_i}}$	1.0766	1.4640	1.2905
$p_3'(z_i) = \frac{e^{z_i} - e^{-z_i}}{e^{z_i} + e^{-z_i}}$	0.1862	0.2472	0.2246

features changes, the distribution of the decoupled features is consistent with the source features. We calculate the Pearson correlation coefficient between the source feature of median filtering shown in Fig. 5(a) and the estimated feature of median filtering shown in Fig. 5(c), and the value of the correlation coefficient is 0.928. Besides, the Pearson correlation coefficient between the source feature of resizing shown in Fig. 5(a) and the estimated feature of resizing shown in Fig. 5(c) is calculated, and the value is 0.955, which numerically indicates that the distribution of the decoupled features and the source features are similar. Based on the different decoupled features that can characterize the tampering operations applied to the images, we can detect the tampering history in an operator chain.

5.5. Feature decoupling performance analysis

We use 1,000 images to analyze the feature decoupling performance under different decoupling functions. The operations are applied to these images according to Eq. (15). Thus, based on the three image operator chains considered in our experiments, the database contains unaltered images, median filtered images, resized images, sharpened images, median filtered and resized images, sharpened and resized images, and median filtered and sharpened images.

Because of the superimposed processing artifacts, we extract coupled SPAM features from median filtered and resized images, sharpened and resized images, and median filtered and sharpened images, respectively. The decoupled features that denote the possible operations will be derived by using the proposed feature decoupling method with three decoupling functions p'. The functions are presented in Table 1. At the same time, the source SPAM features which can represent the operations should be extracted from median filtered images, sharpened images, and resized images, respectively. To evaluate the feature decoupling performance in different processing chains, we calculate the cosine distance between decoupled features and source features according to Eq. (12).

Table 1 provides decoupling performance in various image operator chains. Comparing the results of the three decoupling functions, we found that the cosine distance between the decoupled feature and the source operation feature is the smallest when employing p_3'. That is, compared to the other two functions, this function has the best decoupling performance. Thus, p_3' is determined as the function that needs to be utilized in our proposed feature decoupling method.

5.6. Image processing history detection performance

In this subsection, we evaluate the effectiveness and feasibility of the proposed method in practical scenarios where the image has undergone multiple tampering operations and the falsified image is double JPEG compressed. Specifically, we start with detecting processing history in the operator chain consisting of median filtering and resizing. In this case, five possible processing histories needed to be distinguished as in Eq. (15) with A and B denoting median filtering and resizing. Tampered images are generated with different parameters by combining the factors of median filtering and resizing,

- The window sizes of median filtering are $w = \{3, 5\}$.
- The scaling factors of resizing are $s = \{0.7, 0.8, 1.4\}$.

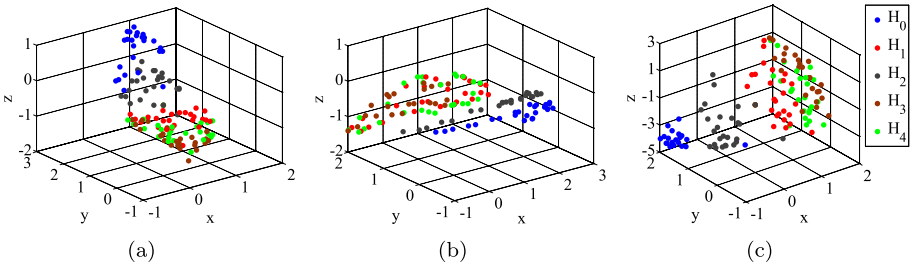


Fig. 6. Plotted are the SPAM features extracted from testing images without feature decoupling (a), the cascaded SPAM features without feature decoupling (b), and the new decoupled features obtained by using feature decoupling (c), where x, y and z are the three-dimensional coordinates of SPAM features mapped in 3D space after t-SNE dimensionality reduction, respectively. H_0-H_4 are five hypotheses for possible processing history. (A: median filtering, B: resizing).

- The quality factors of double JPEG compression are $(QF_1 = 80, QF_2 = 80)$, $(QF_1 = 70, QF_2 = 85)$, $(QF_1 = 80, QF_2 = 95)$ and $(QF_1 = 85, QF_2 = 80)$.

Now that we have determined to use the SPAM feature to detect the processing history, we then perform classification as demonstrated in Fig. 3. It is noted that the images in our experiment have experienced two operations at most, that is to say, to satisfy the requirement that the number of observation channels m is greater than or equal to the number of operations n, we create a new image I' via image rotation for any image I in the image database.

In the training stage, the coupled features $\boldsymbol{f}$ and $\boldsymbol{f}'$ are extracted from the training image I and its expanded image I'. By combining Eqs. (9)-(11), we will derive two decoupled features $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ that represent the two tampering operations. Let $\vec{\boldsymbol{y}} = [\boldsymbol{y}_1, \boldsymbol{y}_2]$ denote the new feature which will be used to train a multi-class classifier. In the testing stage, for each testing image I_{test}, the rotation is employed to generate a new testing image. We extract the coupled features from these testing images and two decoupled features $\boldsymbol{y}_{test_1}$ and $\boldsymbol{y}_{test_2}$ can be derived via feature decoupling. Let $\vec{\boldsymbol{y}'} = [\boldsymbol{y}_{test_1}, \boldsymbol{y}_{test_2}]$ denote the new feature which is fed to the classifier to obtain the classification results.

In order to verify that our proposed method is effective rather than the extracted image features are valid, a comparison experiment that does not use feature decoupling is conducted. Furthermore, to demonstrate that our method is effective in decoupling rather than increasing the feature dimension, we add a comparison experiment to realize image processing history detection by cascading coupled features (C-SPAM) extracted from the original image and its expanded image without using feature decoupling.

Fig. 6 provides an example of SPAM features obtained by using different detection methods. We utilize t-SNE, a technique that visualizes high-dimensional data by giving each data point a location in a two or three-dimensional map [32], to reduce the high-dimensional SPAM features obtained from multi-class forged images to three dimensions. From Fig. 6(a), it can be found that the distribution of SPAM features for H_3 and H_4 almost coincides, because when images undergo multiple tampering operations, the tampering traces of different operations are coupled with each other, making it difficult for SPAM features to distinguish the image processing history. Fig. 6(b) displays the cascaded SPAM features, for H_1, H_3 and H_4, the distribution of cascaded SPAM features is similar. The reason is that the increase of the feature dimension cannot effectively deal with the superimposed processing artifacts caused by multiple manipulations. Fig. 6(c) presents the decoupled features of images with five image processing histories, and the separation within the feature distribution can be observed, which demonstrates the effectiveness of feature decoupling. Then, the decoupled features can be used to identify the operator chain.

Table 2 reports the forensics accuracies in the chain composed of median filtering and resizing by employing our proposed method and two comparative methods respectively. It should be noted that "w/ fd" represents the proposed detection method via feature decoupling, while "w/out fd" denotes the comparison method which does not utilize feature decoupling. Obviously, our proposed method is superior to the other two comparison methods in detecting the existence of processing operations and distinguishing the order of these operations, and the proposed method can achieve great accuracy. We can also observe that there are some cases of individual optimal accuracy when using the method without feature decoupling. The reason is that different tampering operations will leave various traces in images, and the traces may be coupled when an image is forged by multiple operations. Besides, the parameters of the operation also affect the trace. Therefore, if the method without feature decoupling is used to classify the five types of processing history in the operator chain, the classification results will be different. It is possible that the tampering trace of a certain processing history is stronger, and the classification result of this class is better. While other classes will also be misjudged to this class, making it impossible to correctly identify the possible processing history of the image.

The next case study we examine is the operator chain consisting of resizing and sharpening. In this forensics problem, five hypotheses are considered and needed to be classified as in Eq. (15) with A and B denoting resizing and sharpening. Falsified images are generated with different parameters by combining the factors of resizing and sharpening,

- The scaling factors of resizing are $s = \{0.7, 0.8, 1.4, 1.5\}$.
- The radius and strength values of sharpening are $(\sigma = 0.8, \lambda = 1.5)$ and $(\sigma = 1.3, \lambda = 1)$.
- The factors of double JPEG compression are $(QF_1 = 80, QF_2 = 80)$, $(QF_1 = 70, QF_2 = 85)$, $(QF_1 = 85, QF_2 = 80)$ and $(QF_1 = 90, QF_2 = 85)$.

Table 2
The accuracies (%) of processing history detection using the proposed feature decoupling method and comparison experiments that do not use the feature decoupling method when applying different median filtering window sizes, resizing factors, and JPEG quality factors. "Avg" calculates average accuracy. (A: median filtering, B: resizing).

Parameters	Methods	H_0	H_1	H_2	H_3	H_4	Avg
$w=3, s=0.8$	SPAM w/out fd	22.50	64.10	54.30	43.40	19.40	40.74
$QF_1=80, QF_2=80$	C-SPAM w/out fd	44.30	48.90	52.30	53.90	39.40	47.76
	SPAM w/ fd	**69.80**	**83.90**	**91.10**	**89.10**	**91.80**	**85.14**
$w=3, s=1.4$	SPAM w/out fd	70.60	82.30	54.60	39.50	12.90	51.98
$QF_1=80, QF_2=95$	C-SPAM w/out fd	86.20	74.90	82.10	79.50	52.80	75.10
	SPAM w/ fd	**99.20**	**97.20**	**99.40**	**97.70**	**98.10**	**98.32**
$w=5, s=0.7$	SPAM w/out fd	27.60	22.00	80.00	65.50	58.20	50.66
$QF_1=70, QF_2=85$	C-SPAM w/out fd	31.40	0.00	**99.50**	63.50	**99.40**	58.76
	SPAM w/ fd	**97.90**	**92.10**	97.60	**94.30**	98.00	**95.98**
$w=5, s=0.7$	SPAM w/out fd	69.20	31.20	59.80	59.20	49.80	53.84
$QF_1=85, QF_2=80$	C-SPAM w/out fd	35.10	0.00	**95.60**	66.70	**99.00**	59.28
	SPAM w/ fd	**97.20**	**86.10**	93.00	**91.20**	96.00	**92.70**

Table 3
The accuracies (%) of processing history detection using the feature decoupling method and comparison experiments that do not use the feature decoupling method when applying different resizing factors, sharpening radius and strength values, and JPEG quality factors. "Avg" calculates average accuracy. (A: resizing, B: sharpening).

Parameters	Methods	H_0	H_1	H_2	H_3	H_4	Avg
$s=0.7, \sigma=0.8, \lambda=1.5$	SPAM w/out fd	28.50	65.10	33.20	45.20	28.00	40.00
$QF_1=80, QF_2=80$	C-SPAM w/out fd	36.40	71.10	52.40	43.40	53.40	51.34
	SPAM w/ fd	**77.50**	**78.80**	**96.00**	**73.60**	**76.90**	**80.56**
$s=1.4, \sigma=1.3, \lambda=1$	SPAM w/out fd	46.80	65.80	72.90	48.10	37.20	54.16
$QF_1=70, QF_2=85$	C-SPAM w/out fd	80.70	68.90	81.20	62.70	39.20	66.54
	SPAM w/ fd	**98.70**	**95.60**	**97.20**	**90.10**	**79.30**	**92.18**
$s=0.8, \sigma=0.8, \lambda=1.5$	SPAM w/out fd	44.90	71.30	33.20	38.70	7.20	39.06
$QF_1=85, QF_2=80$	C-SPAM w/out fd	55.10	**80.80**	43.30	38.50	26.60	48.86
	SPAM w/ fd	**88.90**	80.50	**91.60**	**72.50**	**75.90**	**81.88**
$s=1.5, \sigma=1.3, \lambda=1$	SPAM w/out fd	77.80	67.00	56.80	56.40	36.00	58.80
$QF_1=90, QF_2=85$	C-SPAM w/out fd	88.80	67.10	78.30	56.70	51.00	68.38
	SPAM w/ fd	**97.60**	**93.70**	**95.90**	**89.80**	**72.60**	**89.92**

Table 3 provides the forensics accuracies in the image operator chain composed of resizing and sharpening by applying the proposed method and two comparative methods respectively. From this table, it is indicated that compared with the two comparison methods without using the feature decoupling idea, our proposed method has a great advantage in detecting tampering history in the image operator chain with resizing and sharpening.

By applying our proposed method to the forensics of median filtering and resizing and the forensics of resizing and sharpening, the results show that our proposed method is useful in the identification of different global processing operator chains. We also examine the forensics in the operator chain composed of median filtering and sharpening. Tampered images are generated with different parameters by combining the factors of median filtering and sharpening,

- The window sizes of median filtering are $w=\{3,5\}$.
- The radius and strength values of sharpening are $(\sigma=0.8, \lambda=1.5)$ and $(\sigma=1.3, \lambda=1)$.
- The quality factors of double JPEG compression are $(QF_1=80, QF_2=80)$, $(QF_1=70, QF_2=85)$ and $(QF_1=85, QF_2=80)$.

Table 4 shows the forensics accuracies in the processing chain consisting of median filtering and sharpening by applying the proposed method and two comparative methods respectively. A noteworthy observation is that our method outperforms these comparison methods in manipulations identification and order classification.

The reason for the above results is that multiple manipulations used to falsify an image will weaken the tampering artifacts of earlier applied tampering operations on the image by later applied operations. The feature extracted from the image is a coupled feature, which makes it difficult to correctly identify the tampering process experienced by the image. While the proposed feature decoupling method can estimate the source operation feature corresponding to each tampering operation from the coupled features, which eliminates the negative impact of superimposed processing artifacts on image operator chain forensics and reduces the difficulty of processing history identification in operator chains.

Table 4
The accuracies (%) of processing history detection using the feature decoupling method and comparison experiments that do not use the feature decoupling method when applying different median filtering window sizes, sharpening radius and strength values, and JPEG factors. "Avg" calculates average accuracy. (A: median filtering, B: sharpening).

Parameters	Methods	H_0	H_1	H_2	H_3	H_4	Avg
$w=3,\sigma=1.3,\lambda=1$	SPAM w/out fd	18.60	81.80	73.20	74.60	6.50	50.94
$QF_1=70,QF_2=85$	C-SPAM w/out fd	70.90	84.50	81.60	75.90	35.60	69.70
	SPAM w/ fd	**97.30**	**94.80**	**97.20**	**91.00**	**91.80**	**94.42**
$w=5,\sigma=0.8,\lambda=1.5$	SPAM w/out fd	38.70	58.60	73.40	82.60	57.90	62.24
$QF_1=80,QF_2=80$	C-SPAM w/out fd	67.90	83.60	74.70	87.60	65.20	75.80
	SPAM w/ fd	**96.00**	**84.40**	**97.70**	**98.10**	**84.60**	**92.16**
$w=3,\sigma=0.8,\lambda=1.5$	SPAM w/out fd	14.90	85.60	65.90	74.90	41.40	56.54
$QF_1=85,QF_2=80$	C-SPAM w/out fd	71.10	**90.00**	71.60	75.10	57.90	73.14
	SPAM w/ fd	**96.50**	88.00	**96.90**	**91.80**	**81.90**	**91.02**
$w=5,\sigma=1.3,\lambda=1$	SPAM w/out fd	54.80	61.80	70.30	77.80	30.30	59.00
$QF_1=85,QF_2=80$	C-SPAM w/out fd	77.20	81.80	81.20	81.10	56.30	75.52
	SPAM w/ fd	**97.20**	**85.60**	**96.40**	**95.20**	**82.30**	**91.34**

Table 5
Comparison of the identification accuracies (%) with three state-of-the-art image forensic methods [14], [19], [21] under different median filtering and resizing parameters. "Avg" calculates average accuracy. (A: median filtering, B: resizing).

Parameters	Methods	H_0	H_1	H_2	H_3	H_4	Avg
$w=3,s=0.8$	Method [14]	37.00	39.70	44.20	72.90	59.10	50.58
$QF_1=80,QF_2=80$	Method [19]	11.00	61.20	9.80	10.00	9.10	20.22
	Method [21]	37.70	41.70	62.70	**89.90**	72.80	60.96
	Ours	**69.80**	**83.90**	**91.10**	89.10	**91.80**	**85.14**
$w=3,s=1.4$	Method [14]	75.10	22.20	54.10	82.20	93.50	65.42
$QF_1=80,QF_2=95$	Method [19]	12.00	8.40	11.60	10.50	60.40	20.58
	Method [21]	**99.90**	85.90	99.20	96.70	**99.70**	96.28
	Ours	99.20	**97.20**	**99.40**	**97.70**	98.10	**98.32**
$w=5,s=0.7$	Method [14]	44.50	51.80	37.00	91.90	51.10	55.26
$QF_1=70,QF_2=85$	Method [19]	69.10	8.80	9.90	10.60	9.10	21.50
	Method [21]	96.80	47.00	90.60	**97.50**	72.80	80.94
	Ours	**97.90**	**92.10**	**97.60**	94.30	**98.00**	**95.98**
$w=5,s=0.7$	Method [14]	57.70	51.20	73.00	91.80	50.20	64.78
$QF_1=85,QF_2=80$	Method [19]	12.20	9.70	10.30	60.30	8.90	20.28
	Method [21]	72.80	47.80	90.50	**96.10**	62.90	74.02
	Ours	**97.20**	**86.10**	**93.00**	91.20	**96.00**	**92.70**

5.7. Comparisons with state-of-the-art methods

In this subsection, we compare the proposed method with three state-of-the-art forensic methods, i.e., Bayar et al.'s method [14], Gao et al.'s method [19] and Boroumand et al.'s method [21]. Notice that Bayar et al.'s method was designed for general-purpose manipulation detection, Gao et al.'s method was aimed to quantify the detectability of tampering operations in different operator chains, and Boroumand et al.'s method was proposed to identify the image tampering history.

Tables 5-7 report the identification performance comparisons among Bayar et al.'s method, Gao et al.'s method, Boroumand et al.'s method, and our proposed method. We can see that all the identification accuracies obtained by the proposed method are higher than using Gao et al.'s method. It is because Gao et al.'s method was designed for uncompressed images. When detecting the tampering history of a double JPEG compressed image, Gao et al.'s method cannot achieve a great detection effect since JPEG compression will cause the loss of high-frequency information of images.

By comparing our method with the two CNN methods [14], [21] in detecting processing history in the image operator chain composed of median filtering and resizing, it is found that the average classification accuracies obtained by our method are better than the two CNN methods. Fig. 7 provides the comparisons of confusion matrices for detecting processing history with different methods. The results also show that the detection accuracy of our proposed method is superior to the other three forensic methods and there is only a slight misclassification in other classes.

For the detection in the chain consisting of resizing and sharpening, compared with Bayar et al.'s method and Boroumand et al.'s method, the results in Table 6 show that the average detection accuracies are improved with our method, especially for H_3 and H_4 classes, the average accuracies are increased by 43.26% and 33.91%, respectively.

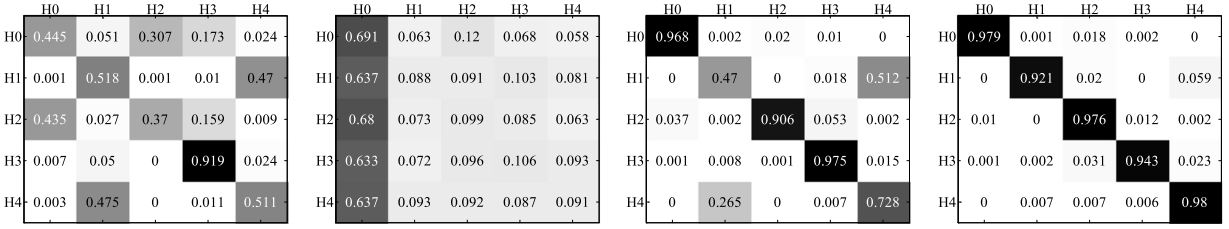
For forensics of the operator chain consisting of median filtering and sharpening, from Table 7, it can be observed that the average detection accuracies of our feature decoupling approach are better than that of Bayar et al.'s method and Boroumand et al.'s method.

Table 6
Comparison of the identification accuracies (%) with three state-of-the-art image forensic methods [14], [19], [21] under different resizing and sharpening parameters. "Avg" calculates average accuracy. (A: resizing, B: sharpening).

Parameters	Methods	H_0	H_1	H_2	H_3	H_4	Avg
$s=0.7, \sigma=0.8, \lambda=1.5$	Method [14]	40.90	47.60	68.90	21.30	43.30	44.40
$QF_1=80, QF_2=80$	Method [19]	58.20	9.20	15.70	10.50	14.30	21.58
	Method [21]	25.60	75.30	34.70	19.70	24.10	35.88
	Ours	**77.50**	**78.80**	**96.00**	**73.60**	**76.90**	**80.56**
$s=1.4, \sigma=1.3, \lambda=1$	Method [14]	76.30	98.00	68.60	2.80	63.40	61.82
$QF_1=70, QF_2=85$	Method [19]	61.80	7.50	11.00	9.80	12.50	20.52
	Method [21]	80.30	**99.00**	75.60	5.00	55.80	63.14
	Ours	**98.70**	95.60	**97.20**	**90.10**	**79.30**	**92.18**
$s=0.8, \sigma=0.8, \lambda=1.5$	Method [14]	44.80	85.30	72.90	27.30	23.80	50.82
$QF_1=85, QF_2=80$	Method [19]	53.40	10.50	12.40	14.50	13.30	20.82
	Method [21]	88.10	**89.70**	90.80	65.10	33.00	73.34
	Ours	**88.90**	80.50	**91.60**	**72.50**	**75.90**	**81.88**
$s=1.5, \sigma=1.3, \lambda=1$	Method [14]	95.30	96.60	79.60	40.40	68.20	76.02
$QF_1=90, QF_2=85$	Method [19]	11.40	55.70	14.00	14.10	15.20	22.08
	Method [21]	86.10	**98.10**	76.60	28.60	**74.70**	72.82
	Ours	**97.60**	93.70	**95.90**	**89.80**	72.60	**89.92**

Table 7
Comparison of the identification performance with three state-of-the-art image forensic methods [14], [19], [21] under different median filtering and sharpening parameters. "Avg" calculates average accuracy. (A: median filtering, B: sharpening).

Parameters	Methods	H_0	H_1	H_2	H_3	H_4	Avg
$w=3, \sigma=1.3, \lambda=1$	Method [14]	58.80	95.20	74.60	12.00	73.40	62.80
$QF_1=70, QF_2=85$	Method [19]	61.40	9.10	10.90	11.40	9.90	20.54
	Method [21]	80.90	**98.10**	76.80	47.20	66.30	73.86
	Ours	**97.30**	94.80	**97.20**	**91.00**	**91.80**	**94.42**
$w=5, \sigma=0.8, \lambda=1.5$	Method [14]	64.80	93.30	91.00	58.80	27.40	67.06
$QF_1=80, QF_2=80$	Method [19]	11.00	63.90	17.30	10.90	10.30	22.68
	Method [21]	91.40	**96.20**	87.10	94.10	53.30	84.42
	Ours	**96.00**	84.40	**97.70**	**98.10**	**84.60**	**92.16**
$w=3, \sigma=0.8, \lambda=1.5$	Method [14]	65.70	98.00	66.80	47.30	56.20	66.80
$QF_1=85, QF_2=80$	Method [19]	10.10	54.60	12.90	11.30	12.60	20.30
	Method [21]	66.20	**99.40**	54.10	57.50	44.10	64.26
	Ours	**96.50**	88.00	**96.90**	**91.80**	**81.90**	**91.02**
$w=5, \sigma=1.3, \lambda=1$	Method [14]	83.90	88.70	96.00	84.40	67.50	84.10
$QF_1=85, QF_2=80$	Method [19]	13.90	29.80	74.20	39.40	24.00	36.26
	Method [21]	**98.90**	**98.30**	90.40	93.30	66.60	89.50
	Ours	97.20	85.60	**96.40**	**95.20**	**82.30**	**91.34**



(a) Method [14] (b) Method [19] (c) Method [21] (d) Ours

Fig. 7. The comparisons of confusion matrices for processing history detection with the proposed method and three state-of-the-art image forensic methods. Median filtering window size $w=5$, resizing factor $s=0.7$, $QF_1=70$, $QF_2=85$. (A: median filtering, B: resizing).

Furthermore, when the images have experienced two operations, the identification performance of our method is superior to the two CNN methods.

Moreover, the advantage of using our method is that the experimental efficiency is much higher than that of the two CNN methods. Because a deep learning approach relies on big data, big models and big calculations, the time cost of the CNN approach is much higher than that of our proposed method on the same experimental equipment. The computation (Mult-Adds) comparisons between the proposed method and the two CNN methods are given in Table 8.

Table 8
The computation (Mult-Adds) of the proposed method and convolutional layers in two CNN methods [14,21].

Methods	Ours	Method [14]	Method [21]
Mult-Adds	4.000×10^4	3.193×10^{10}	3.739×10^9

Table 9
Comparison of general-purpose processing history identification accuracies (%) in different image operator chains using the proposed method and three state-of-the-art image forensic methods.

Parameters	Methods	ORG	MF	RS	SP	MFRS	RSMF	MFSP	SPMF	RSSP	SPRS
$w = 3, s = 1.4$	Method [14]	70.20	69.90	27.60	80.70	98.90	54.90	74.00	51.40	74.60	66.70
$\sigma = 0.8, \lambda = 1.5$	Method [19]	9.10	7.10	8.60	13.20	9.30	35.00	9.10	9.90	13.30	14.60
$QF_1 = 80, QF_2 = 95$	Method [21]	95.00	65.00	47.40	67.90	**99.90**	45.80	93.60	41.70	**99.90**	**99.10**
	Ours	**97.50**	**91.30**	**95.00**	**97.30**	97.50	**97.60**	**98.80**	**95.30**	97.40	96.20
$w = 5, s = 0.7$	Method [14]	40.90	87.60	24.30	50.20	86.40	26.90	49.80	41.20	28.40	20.10
$\sigma = 1.3, \lambda = 1$	Method [19]	9.50	7.90	7.50	10.00	8.50	6.70	6.90	36.70	12.60	10.80
$QF_1 = 85, QF_2 = 80$	Method [21]	58.70	**97.00**	36.10	54.80	**93.20**	42.80	83.10	42.60	38.70	33.10
	Ours	**94.80**	76.40	**78.80**	**90.60**	91.00	**92.80**	**94.60**	**79.00**	**73.30**	**76.00**

In summary, these results demonstrate that our proposed method has a great forensics performance than Bayar et al.'s method and Boroumand et al.'s method when forging an image with downscaling and another operation at the same time. The reason is that Bayar et al.'s method did not consider the case of forging images by the downscaling operation, and Boroumand et al.'s method was designed for the situation when an image is processed, downscaled and again JPEG compressed, where the order of operations was not taken into account. In a practical scenario, resizing is a commonly used tampering operation of image falsification. What is more, if uploading an image to social media, such as Facebook, Snapchat and WeChat, the image may need to be downscaled to meet the social media's limits on image size. The experimental results depict the feasibility of our method for processing history detection in different operator chains under the above circumstance.

5.8. General-purpose history detection performance

Given that various tampering operations could be available to complete a forgery, it is significant to study forensic approaches that can detect different tampering operations simultaneously. In this work, we verify the general-purpose forensics performance of the proposed method.

2,000 original images from the Bossbase database and 1,000 original images from the UCID database are utilized to generate tampered images set using three classes of operations, i.e., median filtering, resizing and sharpening. Each tampered image is double compressed with quality factors QF_1 then QF_2 interleaved by one or two operations. The database contains unaltered images (ORG), median filtered images (MF), resized images (RS), sharpened images (SP), median filtered then resized images (MFRS), resized then median filtered images (RSMF), median filtered then sharpened images (MFSP), sharpened then median filtered images (SPMF), resized then sharpened images (RSSP), and sharpened then resized images (SPRS).

Table 9 provides the comparison results of general-purpose processing history detection in the image operator chain. The average identification accuracy achieved by using the proposed feature decoupling method is 90.56%, which is 34.32% better than Bayar et al.'s method [14], 78.32% better than Gao et al.'s method [19], and 23.79% better than Boroumand et al.'s method [21]. From these results, it can be observed that our proposed method is significantly better than other methods in operator chain detection when only the possible tampering operation range is known. The reason is that our feature decoupling method separates the features of each operation from the superimposed processing artifacts, and the presence of an operation feature indicates that the operation is included in the image operator chain. While other methods learn operation detection features directly from the superimposed processing artifacts. In different complex forgery scenarios, the superimposed processing artifacts will change, making the learned detection features invalid. For example, Boroumand et al.'s method [21] may learn enough forensic information from the superimposed processing artifacts of certain classes, such as MFRS, so that the detection performance of these classes is better. However, Boroumand et al.'s method [21] may not be robust enough for other superimposed processing artifacts to learn more information, thus, the detection accuracy decreases.

6. Discussions

Using a single tampering operation to falsify an image, the artifacts left in the image by different operations are independent, and the features we extract from the image are also independent. However, when the forger sequentially applies diverse operations to alter the image, the artifacts left by the latter operations are linearly superimposed on the artifacts of the previous operations. Moreover, applying different orders of operations may cause disparate tampering artifacts, namely, the independent trace of each tampering operation on the image is not only a linear superposition but also a coupling in a nonlinear manner. Therefore, exploiting image features mapping to the tampering artifacts, our feature decoupling method is designed based on the source operation features being superimposed linearly and then coupled in a nonlinear way.

Since blind signal separation requires the number of observed signals to be greater than or equal to the number of source signals, corresponding to the identification in an operator chain, a given image can only provide one observed coupled feature. It is necessary to increase the observation images on different aspects via image expansion so that we can extract multi-angle features from these observation images to estimate the source features of tampering operations. In this work, we use $n = 2$ as an example, where n denotes the number of possible tampering operations. For each suspected image, a new observation image is created by rotating the image 30 degree. When the number of operations $n > 2$, we can generate multiple new images by rotating a given image at different degrees.

In this paper, we are committed to studying how to detect processing history in operator chains. It should be pointed out that we only consider global operations. When completing an image forgery, global tampering operations such as resizing, median filtering, and sharpening are usually used to change the image quality, thereby hiding some information about the image. Thus, the forensic of global tampering operations is of great significance. There are also some semantic-focused operations, such as splicing and copy-move. As part of our future effort, we intend to build a detector based on blind signal separation for identifying semantic-focused operations and localizing tampered regions.

Generally, there is no prior knowledge of manipulations when detecting image processing history. We have to admit that our work assumes that the kind of operation or the scope of the operation in an operator chain is known to the forensics detector. In the scenario where the tampering operations are unknown, the forgery detection using feature decoupling can distinguish the tampered image from the original image, and the unique features of different operations can be separated from the superimposed processing artifacts. However, since the operations do not belong to the known scope of operations in an operator chain, misjudgment may occur when judging the type of operation. The achieved results can be a valuable starting point for the proposed research in future works. In the case of unknown operations, we would analyze the different traces left by using various single operations to falsify images and make attempt to find features that can distinguish different operations by threshold determination. That is a significant part of our future work.

7. Conclusion

The identification of different global processing operator chains is an important and difficult task in image forensics. In this paper, we focus on identifying image processing history when an image has undergone multiple tampering operations. Specifically, through analogy analysis, we find that the operator chain identification process is quite analogous to blind signal separation which is utilized to recover the unknown source signals from the observed mixed signals. Then, we propose a feature decoupling method based on blind signal separation, which can eliminate superimposed processing artifacts and derive a set of decoupled operation features that represent tampering operations in the operator chain. Moreover, we design a supervised learning strategy that exploits the decoupled features as evidence to achieve processing history identification. To evaluate our proposed method, some typical global tampering operations are applied to collectively constitute image operator chains. Experimental results illustrate that the proposed method detects the processing history in different operator chains with high accuracy. Furthermore, our proposed method is effective in realistic scenarios where the falsified images are JPEG compressed.

Since multiple post-processing operations could weaken the traces of semantic-focused tampering operations, image forgery localization is also a challenge in image forensics. In the future, we would try to design a new feature decoupling based forgery detector for forgery localization, which is robust to post-processing attacks.

CRediT authorship contribution statement

Jiaxin Chen: Conceptualization; Methodology; Formal Analysis; Experimental Design and Data Collection; Writing Manuscript. **Xin Liao**: Conceptualization; Data Interpretation; Writing-Review and Editing; Supervision; Funding Acquisition. **Wei Wang:** Resources; Writing-Review and Editing; Supervision. **Zheng Qin:** Resources; Writing-Review and 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.

Data availability

Data will be made available on request.

Acknowledgement

This work is partially supported by the National Natural Science Foundation of China (Grant Nos. U22A2030, U20A20174, 61972142, 61972395, and 62002112), Natural Science Foundation of Hunan Province (Grant No. 2020JJ4212, and 2021JJ40117).

References

[1] P. Meel, D.K. Vishwakarma, Han, image captioning, and forensics ensemble multimodal fake news detection, Inf. Sci. 567 (2021) 23–41.
[2] Z. Dias, A. Rocha, S. Goldenstein, Image phylogeny by minimal spanning trees, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 774–788.
[3] H. Tsai, B. Chang, X. Lin, Using decision tree, particle swarm optimization, and support vector regression to design a median-type filter with a 2-level impulse detector for image enhancement, Inf. Sci. 195 (2012) 103–123.
[4] W. Sun, J. Zhou, L. Dong, J. Tian, J. Liu, Optimal pre-filtering for improving Facebook shared images, IEEE Trans. Image Process. 30 (2021) 6292–6306.
[5] X. Liao, Z. Huang, L. Peng, T. Qiao, First step towards parameters estimation of image operator chain, Inf. Sci. 575 (2021) 231–247.
[6] A.C. Popescu, H. Farid, Exposing digital forgeries by detecting traces of resampling, IEEE Trans. Signal Process. 53 (2) (2005) 758–767.
[7] C. Tang, X. Liu, S. An, P. Wang, BR^2Net: defocus blur detection via a bidirectional channel attention residual refining network, IEEE Trans. Multimed. 23 (2021) 624–635.
[8] X. Kang, M.C. Stamm, A. Peng, K.J.R. Liu, Robust median filtering forensics using an autoregressive model, IEEE Trans. Inf. Forensics Secur. 8 (9) (2013) 1456–1468.
[9] C. Chen, J. Ni, J. Huang, Blind detection of median filtering in digital images: a difference domain based approach, IEEE Trans. Image Process. 22 (12) (2013) 4699–4710.
[10] W. Li, X. Li, R. Ni, Y. Zhao, Quantization step estimation for jpeg image forensics, IEEE Trans. Circuits Syst. Video Technol. 32 (7) (2022) 4816–4827.
[11] X. Qiu, H. Li, W. Luo, J. Huang, A universal image forensic strategy based on steganalytic model, in: Proceedings of ACM Workshop on Information Hiding and Multimedia Security, 2014, pp. 165–170.
[12] 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.
[13] G. Singh, P. Goyal Gimd-net, An effective general-purpose image manipulation detection network, even under anti-forensic attacks, in: Proceedings of International Joint Conference on Neural Networks, 2021, pp. 1–8.
[14] B. Bayar, M.C. Stamm, Constrained convolutional neural networks: a new approach towards general purpose image manipulation detection, IEEE Trans. Inf. Forensics Secur. 13 (11) (2018) 2691–2706.
[15] G. Cao, Y. Zhao, R. Ni, X. Li, Contrast enhancement-based forensics in digital images, IEEE Trans. Inf. Forensics Secur. 9 (3) (2014) 515–525.
[16] J. Yang, G. Zhu, Y. Luo, S. Kwong, X. Zhang, Y. Zhou, Forensic analysis of jpeg-domain enhanced images via coefficient likelihood modeling, IEEE Trans. Circuits Syst. Video Technol. 32 (3) (2022) 1006–1019.
[17] X. Liu, W. Lu, Q. Zhang, J. Huang, Y.Q. Shi, Downscaling factor estimation on pre-jpeg compressed images, IEEE Trans. Circuits Syst. Video Technol. 30 (3) (2020) 618–631.
[18] W. Lu, Q. Zhang, S. Luo, Y. Zhou, J. Huang, Y.Q. Shi, Robust estimation of upscaling factor on double jpeg compressed images, IEEE Trans. Cybern. (2021) 1–13.
[19] S. Gao, X. Liao, X. Liu, Real-time detecting one specific tampering operation in multiple operator chains, J. Real-Time Image Process. 16 (3) (2019) 741–750.
[20] X. Chu, Y. Chen, K.J.R. Liu, Detectability of the order of operations: an information theoretic approach, IEEE Trans. Inf. Forensics Secur. 11 (4) (2016) 823–836.
[21] M. Boroumand, J. Fridrich, Deep learning for detecting processing history of images, J. Electron. Imaging 7 (2018) 2131–2139.
[22] J. Chen, X. Liao, Z. Qin, Identifying tampering operations in image operator chains based on decision fusion, Signal Process. Image Commun. 95 (2021) 116287.
[23] M.C. Stamm, X. Chu, K.J.R. Liu, Forensically determining the order of signal processing operations, in: Proceedings of IEEE International Workshop on Information Forensics and Security, 2013, pp. 162–167.
[24] J. Chen, X. Liao, W. Wang, Z. Qin, A features decoupling method for multiple manipulations identification in image operation chains, in: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, 2021, pp. 2505–2509.
[25] C. Jutten, J. Herault, Space or time adaptive signal processing by neural network models, in: Proceedings of International Conference on Neural Network for Computing, 1986, pp. 206–211.
[26] S. Haykin, Z. Chen, The cocktail party problem, Neural Comput. 17 (2005) 1875–1902.
[27] J.V. Stone, Independent component analysis: A tutorial introduction, MIT Press, Cambridge, MA, 2004.
[28] A. Hyvärinen, A family of fixed-point algorithms for independent component analysis, in: Proceedings of International Conference on Acoustics, Speech and Signal Processing, 1997, pp. 3917–3920.
[29] T.F.P. Bas, T. Pevný, 'Break our steganographic system': the ins and outs of organizing boss, in: Proceedings of International Conference on Information Hiding, 2011, pp. 59–70.
[30] G. Schaefer, M. Stich, UCID: an uncompressed color image database, in: Proceedings of SPIE, Storage and Retrieval Methods and Applications for Multimedia, 2004, pp. 472–480.
[31] P.B.T. Pevný, J. Fridrich, Steganalysis by subtractive pixel adjacency matrix, IEEE Trans. Inf. Forensics Secur. 5 (2) (2010) 215–224.
[32] L.V.D. Maaten, G. Hinton, Visualizing data using t-SNE, J. Mach. Learn. Res. 9 (2) (2008) 2579–2605.