Multimedia Tools and Applications
https://doi.org/10.1007/s11042-019-7288-y

Multi-scale segmentation strategies in PRNU-based image tampering localization

Weiwei Zhang[1] · Xinhua Tang[2] · Zhenghong Yang[1] · Shaozhang Niu[3]

Received: 31 May 2018 / Revised: 13 December 2018 / Accepted: 27 January 2019
Published online: 26 February 2019

Abstract
With the rapid development of advanced media technology, especially the popularization of digital cameras and image editing software, digital images can be easily forged without leaving visible clues. Therefore, image forensics technology for identifying the accuracy, integrity, and originality of digital images has become increasingly important. Photo-response non-uniformity (PRNU) noise, a unique fingerprint of imaging sensors, is a valuable forgery detection tool because of its consistently good detection performance. All kinds of forgeries, including copy-move and splicing, can be dealt with in a uniform manner. This paper addresses the problem of forgery localization based on PRNU estimation and aims to improve the resolution of PRNU-based algorithms. Different from traditional overlapping and sliding window-based methods, in which PRNU correlations are estimated on overlapped patches, the proposed scheme is analyzed based on nonoverlapping and irregular patches. First, the test image is segmented into nonoverlapped patches with multiple scales. Second, correlations of PRNU are estimated on nonoverlapped patches to obtain the real-valued candidate tampering probability map for each individual scale. Then, all of the candidate maps are fused into a single and more reliable probability map through an adaptive window strategy. In the final step, the final decision map is obtained by adopting a conditional random field (CRF) to model neighborhood interactions. The contributions of this work include the following: a novel PRNU-based forgery localization scheme using multi-scale nonoverlapping segmentation is proposed for the first time. Furthermore, the adaptive fusion strategy involves selecting the best candidate tampering probability individually for each location in the image. Additionally, the experimental results prove that the proposed scheme can achieve much better detection results and robustness compared with the existing state-of-the-art PRNU-based methods.

Keywords Photo-response non-uniformity · Image tampering localization · Multi-scale segmentation · Adaptive fusion strategy · Conditional random field

✉ Shaozhang Niu
szniu@bupt.edu.cn

Extended author information available on the last page of the article

1 Introduction

Today's advanced media technology, such as digital image processing, video coding [38], high-efficiency video coding (HEVC) [24, 35], Internet of Things (IoT) [36, 45], and cloud computing (CC) [39], represents a fascinating time that will considerably affect daily life. In particular, digital images are being used in many applications such as the military, medical diagnosis, art pieces, and photography. The reliability of digital images is thus becoming an important issue. However, currently, it is very easy to manipulate digital images without leaving visible traces using photo editing software. Therefore, it is important to focus on the image forensics field. One of the principal problems in image forensics is determining whether a particular image is authentic and, if manipulated, to localize which parts have been altered. Since forgery localization requires pixel-level analysis rather than image-level analysis, it faces more challenges compared to forgery detection.

1.1 Related works

Instead of using digital watermarks [3] and signatures [47], many passive methods have been proposed for image forgery detection. Copy-move and splicing forgery are the most common forms to manipulate digital images. For copy-move forgery, there are mainly two classes of detection algorithms [11]. One is based on blockwise division, such as discrete wavelet transform (DWT) [43], principal component analysis (PCA) [34], and Zernike moments [42], and the other is based on keypoint extraction, such as scale-invariant feature transform (SIFT) [4, 27, 41] and speeded-up robust features (SURF) [37]. For splicing forgery, the spliced region from another image has a significantly different intrinsic noise variance. The method in [33] exposes region splicing by revealing inconsistencies in local noise levels. However, the spliced region and the target image differ under many more aspects than just noise. In [13], a feature-based algorithm to detect image splicing was proposed. Local features were computed from the co-occurrence of image residuals and used to extract synthetic feature parameters. The authors in [14] regarded features coming from the spliced area as anomalies and iterated autoencoder-based modeling and discriminative labeling to distinguish them. Noise discrepancies in multi-scales are used for image splicing forgery detection in [40]. Similarly, Yao et al. [46] explored possible noise level inconsistency using a noise level function (NLF) to detect image splicing.

Recently, a multitask fully convolutional network (MFCN) was proposed to localize image splicing attacks [44]. Since JPEG format is widely used and image splicing usually involves the operation of double JPEG compression, Bianchi et al. [5] exploited the artifacts arising from double JPEG compression. The illumination environment in pictures also presents some consistency: directions of lights [21], shadows [30] and illumination colors [6] can be estimated and used as cues. However, the methods mentioned above are intrinsically sensitive only to specific manipulations.

In addition, some methods rely on machine learning [12, 16, 18] and have reported good performance. However, these methods essentially depend on the availability and quality of training data, which is not always guaranteed.

An interesting approach for forgery detection relies on the characteristics of the digital camera, such as the color filter array (CFA) interpolation artifacts [17], lens aberration [22] and sensor pattern noise (SPN) [32], which has drawn considerable attention due to the uniqueness of individual cameras and the stability against environmental conditions. Photo-response non-uniformity (PRNU) noise is the dominant component of SPN. PRNU is the result of imperfections caused by the manufacturing process and the inhomogeneity of silicon wafers. Lukas et al. [32]

initially developed a PRNU-based technique for image forgery detection and camera identification. The camera PRNU noise is estimated by averaging noise residues extracted from images acquired by the camera. Given an image, they obtained the pattern noise from the image using a smoothing filter and identified the camera model by comparing with candidate reference patterns. In [7], the maximum likelihood estimator (MLE) was used to estimate the camera PRNU. In view of the good performance of the PRNU-based algorithm, many studies have made improvements under several aspects. Since denoising filtering contributes significantly to the accuracy of PRNU estimation, denoising filters, such as predictors based on the eight-neighbor context-adaptive interpolation (PCAI) algorithms [23] and block matching and 3D filtering (BM3D) algorithms [15], have been discussed. Since the PRNU is a very weak signal, Lin et al. [28] believed that some components of SPN have been severely contaminated by the errors introduced by denoising filters and that the quality of PRNU can be improved by abandoning those components. To reduce undesirable nonunique noise components, Lin et al. [29] proposed the method of equalizing the magnitude spectrum of the reference SPN to decrease the false identification rate. Later, a three-stage enhancement of the PRNU was proposed in [26]. More recently, PRNU has been used to detect forgeries caused by hue modification [20]. However, these methods mainly aim to discriminate whether a given image is pristine or fake. In practice, we are more interested in determining the tampered regions, which are called tampering localization.

In this paper, we focus on tampering localization based on the PRNU algorithm. The core of PRNU-based tampering localization involves the correlation of a known noise pattern with its estimate from the investigated image. The operation is often performed in a sliding window manner. To detect small-sized manipulations, Chierchia et al. proposed segmentation-based analysis [9] and a spatially adaptive filtering technique [8]. In addition, the authors in [10] cast the problem in terms of Bayesian estimation and adopted a Markovian prior to model the strong spatial dependences of the source, which allows for the propagation of reliable decisions into ambiguous areas. More recently, a multi-scale analysis was adopted to improve the localization resolution in [25]. Although the above methods can improve the resolution dramatically, these methods are all based on overlapped sliding windows, which can lead to many false decisions when the sliding window falls near the boundary between tampered and authentic regions. Lower localization accuracy near the boundary of tampered objects is still a major problem to be solved in tampering localization. Therefore, obtaining accurate image segmentation is necessary to improve the localization resolution.

Image segmentation aims to partition an image into several parts automatically or with simple interactions. It is a key step in image analysis. Graph cut technology is one of the leading algorithms for interactive segmentation [2], which is suitable for delineating a boundary of one or multiple objects from images. A multilevel banded heuristic for computation of graph cuts is proposed in [31] for fast image segmentation. Recently, an efficient hierarchical graph cut method was proposed for interactive RGB-D image segmentation, which can generate high-quality segmentation results and real-time interactions [19]. In recent years, researchers have focused on superpixels in the field of image segmentation. A new superpixel algorithm, simple linear iterative clustering (SLIC), which adapts a k-means clustering approach to efficiently generate superpixels, was proposed [1].

1.2 Contributions

To address the abovementioned problems, in this study, we propose a novel PRNU-based forgery localization scheme using multi-scale nonoverlapping segmentation. The main

contributions of this work are as follows: 1) the test image is segmented into nonoverlapping superpixels of multiple scales by the SLIC algorithm. This is the first time that a multi-scale SLIC strategy is proposed in the framework of PRNU-based algorithms. 2) In each individual scale, unlike existing sliding window-based algorithms in which PRNU correlations are estimated on overlapped sliding windows, our algorithm directly computes correlations on nonoverlapped irregular patches, which can accurately delineate boundaries of contrasting objects with lower complexity. 3) An adaptive fusion strategy is used to combine multi-scale tampering probability maps. 4) Compared with existing state-of-the-art PRNU-based methods, the proposed algorithm retains better experimental results in diverse situations.

The rest of this paper is organized as follows. Section 2 introduces the PRNU-based localization method. Section 3 describes the proposed strategy in detail. Section 4 shows a series of experiments and comparisons with state-of-the-art methods. Finally, conclusions are drawn in section 5.

2 Background

This section mainly introduces basic analysis strategies in PRNU-based tampering localization. Let $y \in R^N$ be a digital image taken from a given camera, y_i indicates the value at site i, either the grayscale or a single color component from a color image. Let us consider a simplified model [32] in which y can be written as:

$$y = x + kx + \theta \tag{1}$$

where x is the acquired noise-free image, θ an additive noise term, and k is the camera PRNU. For the purpose of forgery detection, k is the signal of interest, while all the rest can be considered undesired disturbances. Therefore, to eliminate the original signal x, the noise residual r is estimated as follows:

$$r = y - \hat{x} = yk + (x - \hat{x}) + (x - y)k + \theta = yk + n \tag{2}$$

where $\hat{x} = D(y)$ is an estimate of the noise-free image x by applying a denoising filter D and n is the ensemble of all disturbances.

The main steps of the PRNU-based algorithm are as follows.

As the preliminary step, the camera PRNU is estimated by a large number of photos taken by the target camera. The noise residuals are extracted using Eq. (2) from a number of low-contrast images taken by the target camera; then, the camera PRNU k is obtained by maximum likelihood estimation of noise residuals [7]. That is

$$\hat{k} = \frac{\sum_{i=1}^{m} W_i I_i}{\sum_{i=1}^{m} I_i^2} \quad i = 1, \cdots, m \tag{3}$$

where m is the number of images involved in the calculation, I_i is the ith image taken by the target camera, and W_i is the corresponding noise residual extracted from I_i. Note that the multiplication operation in Eq. (3) is element wise.

Then, the image PRNU is estimated by Eq. (2) in the second step. Since there is only one image to be detected, the noise residual r is often used to approximate its image PRNU.

Third, tamper detection was based on sliding window analysis. Let w_i denote the sliding analysis window of size $w \times w$ centered around pixel i. For each analysis window w_i, the

normalized cross-correlation q_i is used to compare the image PRNU against the camera PRNU in Eq. (4).

$$q_i = corr(r_{w_i}, z_{w_i}) = \frac{\left(r_{w_i} - \bar{r}_{w_i}\right) \odot \left(z_{w_i} - \bar{z}_{w_i}\right)}{\|r_{w_i} - \bar{r}_{w_i}\| \cdot \|z_{w_i} - \bar{z}_{w_i}\|} \tag{4}$$

Note that r_{w_i} is the noise residual and $z_{w_i} = y_{w_i} \cdot k_{w_i}$ is an estimate of the camera PRNU in Eq. (4).

Given k, the detection problem can be formulated as a binary hypothesis test between hypothesis H_0 that the camera PRNU is absent and hypothesis H_1 that the PRNU is present:

$$\begin{cases} H_0: & q_i \sim N(0, \sigma_0) \\ H_1: & q_i \sim N(\hat{q}_i, \sigma_1) \end{cases} \tag{5}$$

where the expected correlation predictor $\hat{q}_i$ account for special situations such as saturated image regions where PRNU cannot be detected. σ_0, σ_1 are the variances of the detection statistics for H_0 and H_1, respectively.

Then, Korus et al. [25] converted the measured correlation q_i into tampering probability map c_i:

$$c_i = P(q_i | \sigma_0, \sigma_1, \hat{q}_i) = \left(1 + e^{-\log(\sigma_1/\sigma_0) - \frac{(q_i - \hat{q}_i)^2}{2\sigma_1^2} + \frac{q_i^2}{2\sigma_0^2}}\right)^{-1} \tag{6}$$

In the last step, the final decision map is obtained by a conditional random field (CRF) model [25].

3 The proposed PRNU-based multi-scale tampering localization algorithm

This section describes the proposed multi-scale segmentation strategies in PRNU-based image tampering localization. Figure 1 shows the framework of the proposed algorithm. First, a multi-scale segmentation method is proposed to segment the test image into successive scales. The segmentation result for each scale is composed of nonoverlapping and irregular patches. For each scale, PRNU correlations are computed on nonoverlapped patches to obtain a real-valued candidate tampering probability map. Subsequently, the candidate tampering probability maps of all scales are fused into a single, more reliable map by the adaptive fusion method. Finally, we use CRF modeling to obtain the final decision map.

The SLIC algorithm is applied to segment the input image on multiple scales. SLIC adopts a k-means clustering approach to efficiently generate superpixels and adheres to boundaries as well as better than other similar segmentation methods [1]. At the same time, it is fast, memory efficient and simple to use. In most cases, one image with a size of 1920 × 1080 can be segmented into thousands of patches in 2 s using a personal computer with a 3.60 GHz CPU with 16 GB of RAM. By default, the only parameter of the algorithm is J, the desired number of superpixels.

Assume the size of the test image is $M \times N$, in the segmentation stage, the computational complexity of overlapping segmentation is O(MN), and the nonoverlapping segmentation is O(J), which is much lower than the former. Compared with the existing sliding window-based analysis, superpixel segmentation by SLIC can significantly reduce the complexity of the

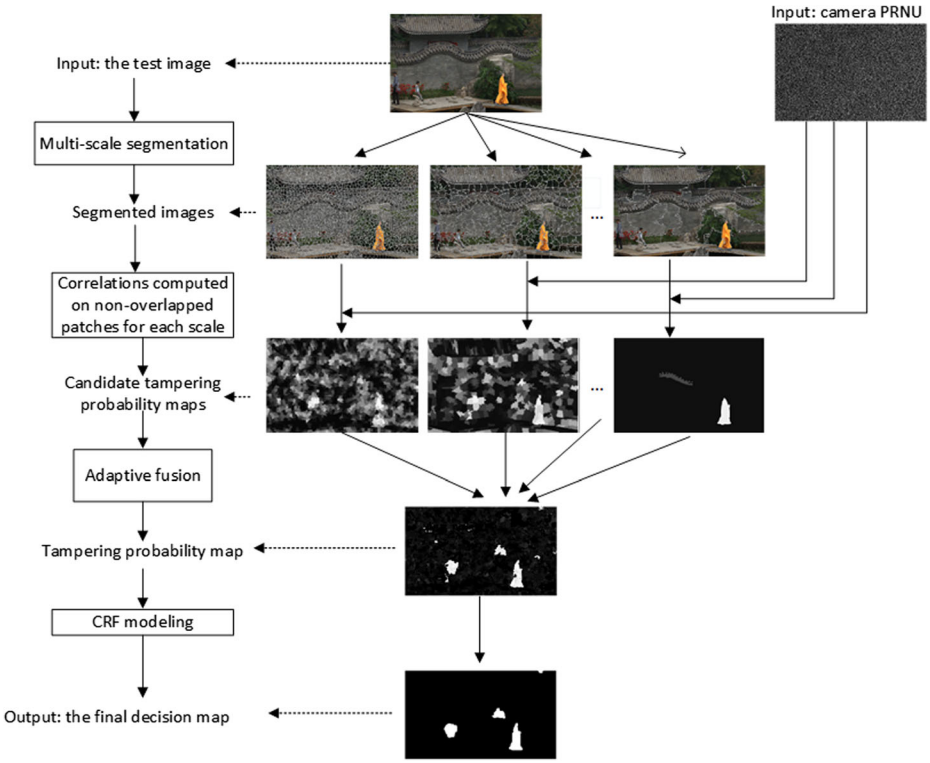


Fig. 1 Framework of the proposed multi-scale tampering localization scheme

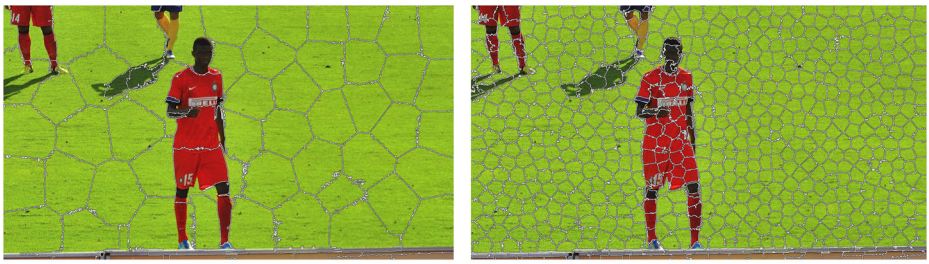
subsequent image processing. Furthermore, the irregular and meaningful regions can adhere to the boundary better than the regular blocks.

Figure 2 gives an example of image segmentation obtained by SLIC. The man dressed in red in the middle of the image is in the tampered regions. We segment the image by means of the SLIC algorithm with the initial number of superpixels $J = 100$ (left) and 1000 (right).

However, the initial number of superpixels in SLIC is difficult to determine. It is difficult to detect and locate tampered objects of various sizes with one fixed initial segmentation number. Different initial numbers of superpixels can produce different forgery detection results. When J is too small, the average size of superpixels is too large. Reliable statistics can be obtained for large superpixels. However, the small tampered regions will occupy only a small part of the superpixels, and thus it may cause false detection in the following steps. In contrast, if J is large enough to decompose all possible tampered areas, the average size of superpixels is too small. Smaller tampered regions can be accurately detected on smaller scales, while smaller superpixels yield more noise and uncertainty. Hence, to combine the benefits of small-scale and large-scale analysis, we propose to segment the test image into multiple scales. Therefore, the proposed multi-scale segmentation method plays an important role in detecting various size forgeries.

3.1 Multi-scale segmentation

In the first step of the proposed algorithm, we segment the test image I into S scales, and the segments satisfy:



(a) (b)

Fig. 2 An example of image segmentation using SLIC. The initial number of superpixels **a** $J = 100$ and **b** $J = 1000$

$$\begin{cases} \bigcup_{j=1}^{J_s} T_j^s = I \\ T_i^s \cap T_j^s = \Phi (i \neq j, i, j = 1, \cdots, J_s) \end{cases} \quad for \quad s = 1, \cdots, S \tag{7}$$

where T_j^s indicates the jth patch, and there are J_s total segments on the sth scale. S is the total number of scales.

Note that segments for each scale s ($s = 1,\ldots, S$) are nonoverlapped and segments from different scales should not be intentionally the same, that is:

$$T^p \neq T^q \quad \text{for} \quad p \neq q \tag{8}$$

3.2 Obtaining a tampering probability map based on PRNU analysis across each scale

In contrast to sliding window-based analysis [25, 32], the proposed nonoverlapped regions of irregular shape are expected to accurately delineate boundaries of contrasting objects with lower complexity. The image PRNU and the camera PRNU are estimated by Eq. (2) and Eq. (3), respectively. Then, a PRNU-based analysis is conducted across each scale s ($s = 1,\ldots, S$) to obtain a tampering probability map. In the rest of this section, unless specified, all operations are performed on the same scale s. For each patch $T_j^s (j = 1, \cdots, J_s)$, the correlation between the image PRNU and the camera PRNU is computed only for pixels that belong to the jth patch, that is:

$$q_j = corr\left(R_j^s, Z_j^s\right) = \frac{\left(R_j^s - \overline{R}_j^s\right) \odot \left(Z_j^s - \overline{Z}_j^s\right)}{\|R_j^s - \overline{R}_j^s\| \cdot \|Z_j^s - \overline{Z}_j^s\|} \quad (j = 1, \cdots, J_s) \tag{9}$$

where R_j^s and $Z_j^s = T_j^s \cdot K_j^s$ are the image PRNU and camera PRNU, respectively, of the patch T_j^s.

The problem can be cast as a binary test between hypothesis H_0 that the camera PRNU is absent and hypothesis H_1 that the camera PRNU is present. We define $\sum T_j^s$ as the number of actual pixels of the patch T_j^s. Thus, $\omega_j = \left[\sqrt{\sum T_j^s}\right]$ represents the equivalent square window size and $[\cdot]$ represents the rounding function. Since the test image is divided into nonoverlapped regions of irregular shape, the distribution models for the hypothesis in Eq. (5) are adjusted according to the number of actual pixels used in the correlation calculation:

$$\begin{cases} H_0: & q_j \sim N\left(0, \sigma_0(\omega_j)\right) \\ H_1: & q_j \sim N\left(\hat{q}_j(\omega_j), \sigma_1(\omega_j)\right) \end{cases} \tag{10}$$

where $\sigma_0(\omega_j)$, $\hat{q}_j(\omega_j)$ and $\sigma_1(\omega_j)$ are obtained by cubic spline interpolation between the original value $\sigma_0(\omega_s)$, $\hat{q}_j(\omega_s)$ and $\sigma_1(\omega_s)$ used in multi-scale square window analysis. Note that the square window $\{\omega_s\}(s \in \{1, \cdots, S\})$ used for spline interpolation is the same as [25].

To prevent excessive degradation of the correlation statistic, at least $\omega_{\min}^2$ pixels are required for the computation in the proposed scheme. If the segmentation yields a smaller region, we expand it with morphological dilation.

Then, candidate tampering probability maps c^s for each scale $s(s = 1, \cdots, S)$ are obtained by Eq. (6). The detailed steps of the proposed PRNU-based nonoverlapping segmentation algorithm are shown in Algorithm 1.

Algorithm 1 Pseudocode for the proposed PRNU-based nonoverlapping segmentation algorithm

Symbols: D - denoising filter; $\hat{q}$ - correlation predictor; P-tampering probability;

Input: I, $\hat{K}$ ▷ input image, camera PRNU estimation
Input: ω ▷ square window size
Input: s, S ▷ the scales, the number of scales in total
Input: $\hat{q}(\omega_s), \{\sigma_0(\omega_s), \sigma_1(\omega_s)\}\ (s = 1, \cdots, S)$
▷ camera model parameters, ω_s is the square window used for interpolation
Input: $\omega_{\min}$ ▷ the minimum window size
Input: J_s ▷ the desired number of superpixels
$R \leftarrow I - D(I)$ ▷ the noise residual of test image I
for $s \leftarrow$each scale s $(s = 1, \cdots, S)$
$T_j^s\ (j = 1, \cdots, J_s) \leftarrow$ segment I using SLIC superpixels ▷ T_j^s is the jth patch in scale s
while $\omega_j = [\sqrt{\sum T_j^s}] < \omega_{\min}$ **do**
$T_j^s \leftarrow$ morphological dilation of T_j^s ▷ grow region if too small
end while
for $j \leftarrow$ each patch j $(j = 1, \cdots, J_s)$
$\hat{q}_j(\omega_j), \{\sigma_0(\omega_j), \sigma_1(\omega_j)\} \leftarrow$ spline interpolation by $\hat{q}_j(\omega_s), \{\sigma_0(\omega_s), \sigma_1(\omega_s)\}$ $(s \in \{1, \cdots, S\})$
$Z_j^s \leftarrow T_j^s \cdot \hat{K}_j^s$; $q_j \leftarrow corr(R_j^s, Z_j^s)$ ▷ correlation, Eq. (9)
$c_j^s \leftarrow P(q_j | \hat{q}_j(\omega_j), \sigma_0(\omega_j), \sigma_1(\omega_j))$ ▷ tampering prob., Eq. (6)
end for
end for
return $c^s\ (s = 1, \cdots, S)$ ▷ multi-scale tampering prob.

3.3 Fusion of the multi-scale tampering probability maps

With the analyses of PRNU-based multi-scale nonoverlapping segmentation, a set of tampering probability maps $c^s(s = 1, \cdots, S)$ of the test image can be obtained. The next task is to fuse multi-scale tampering probability maps using an adaptive fusion approach to obtain a single, more reliable tampering probability map. It can combine the benefits of both small-scale and

large-scale analyses. The analysis starts by evaluating the tampering probability c_i^s according to Eq. (6) for the smallest scale (e.g., $s = 1$ in our experiment). Note that i denotes the location of the ith pixel. If the patch is too small and a confident decision cannot be reached, the patch size is increased to the next available scale $s + 1$. Such an approach uses smaller patches in more confident, bright and flat areas and larger patches are used in darker, more textured regions of the image. In our experiments, we proceed to the next patch size if $|c_i^s - 0.5| < 0.5 - \Delta c_1$. The new tampering probability estimate is accepted if it is more confident than the previous one. If the next (larger) scale reinforces a previous, reasonably confident detection ($|c_i^s - 0.5| > \Delta c_2$), we stop increasing the scale. The described algorithm is summarized as pseudocode in Algorithm 2.

Algorithm 2 Pseudocode for the adaptive fusion algorithm

Symbols: ψ - subsampling
Input: $c^s \ (s = 1, \cdots, S)$ ▷ multi-scale tampering prob.
Input: $\Delta c_1, \Delta c_2$ ▷ score thresholds (stopping criteria)
for $i \leftarrow 1$ locations
  $s \leftarrow 1$ ▷ start with the smallest patch
  $\tilde{c} \leftarrow 0.5$ ▷ buffer for last score
  while $s \le S$ **and** $|\tilde{c} - 0.5| < 0.5 - \Delta c_1$ **do**
    if $|c_i^s - 0.5| > |\tilde{c} - 0.5|$ **then**
      $c_i \leftarrow c_i^s$ ▷ use new score if more confident
      if $|\tilde{c} - 0.5| > \Delta c_2$ **and** $(c_i^s - 0.5)(\tilde{c} - 0.5) > 0$ **then**
        break; ▷ if scores agree, stop
      end if
      $\tilde{c} \leftarrow c_i^s$
    end if
    $s \leftarrow s + 1$ ▷ increase window size
  end while
end for
c $\leftarrow \psi(c)$ ▷ subsampling
return $t \leftarrow \arg\min_t E(t \mid c)$ ▷ final decision, Eq. (11)

An example of the effect of using the adaptive fusion algorithm can be seen in Fig. 3, with color bars from 1 to 7 representing 7 scales. In this case, noisier and more uncertain regions are replaced by another region taken from a different scale.

3.4 Obtaining the final decision map

Based on the obtained tampering probability map, the final decision map is adopted by a CRF model. The tampering probability map c can be formulated in terms of CRF and resolves to find the optimal labeling of authentication units (with labels $t_i = 1$ denotes tampered regions) that minimizes the following energy function [25]:

$$E(t|c) = \sum_{i=1}^{N} E_\tau(c_i, t_i) + \alpha \sum_{i=1}^{N} t_i + \sum_{i=1}^{N} \sum_{j \in \Delta_i} \beta_{ij} |t_i - t_j| \tag{11}$$

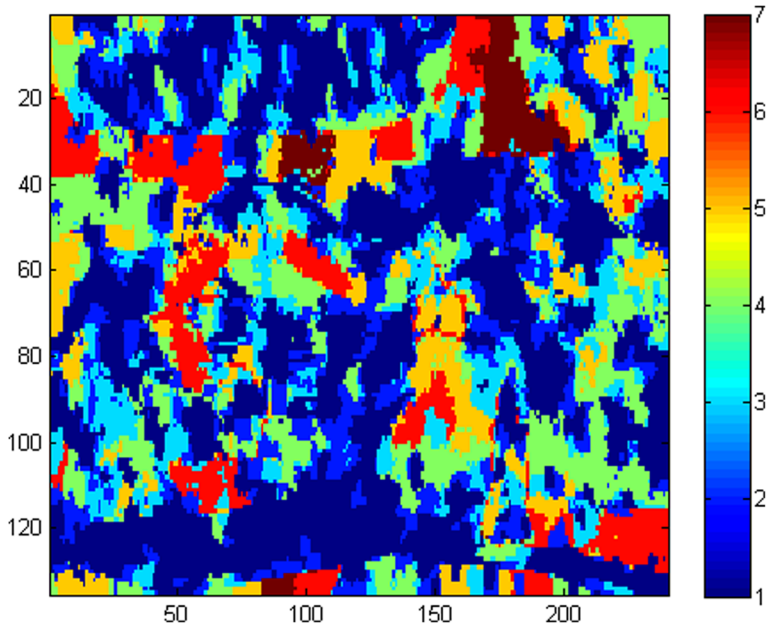


Fig. 3 An example of an adaptive fusion method. Color bars from 1 to 7 represent 7 scales

where N is the number of pixels in the test image. The decision is controlled by a decision threshold τ and parameterized by tampering penalty α and interaction parameter β. Readers can refer to [25] for more details. To speed up processing, the tamper probability map is resized to a smaller size (e.g., 240 × 135 in our experiment) before using CRF in the proposed scheme.

4 Experimental results

In this section, we discuss the performance of the proposed technique. The proposed method was implemented using MATLAB2015a on a computer with a 3.4 GHz CPU and 16 GB of RAM. In this section, the forgery localization performance is evaluated with the F_1-score as follows:

$$F_1 = \frac{2 \cdot TP}{2 \cdot TP + FN + FP} \tag{12}$$

Table 1 Parameters used in the experiments

Symbol	Parameter	Value
S	The total number of scales	7
$\omega_{\min}$	Minimum window size	64
$\omega_s(s = 1, \cdots, S)$	The square window used for interpolation	{32, 48, 64, 96, 128, 192, 256}
$J_s(s = 1, \cdots, S)$	The number of initial segment patches for S scales	{2025, 900, 506, 225, 127, 56, 32}
Δc_1	Parameters used in adaptive fusion	0.1
Δc_2		0.25

where *TP*, *FN*, *FP* denote statistics of the detected true positives, false negatives, and false positives, respectively. In addition, we also generate the corresponding receiver operation characteristics (ROC) curve by sweeping the decision threshold τ over 24 values, uniformly distributed in (0, 1).

4.1 Dataset selection

Experiments are conducted on a realistic tampering dataset proposed by Korus et al. [25], which contains a total of 136 tampered images originating from four cameras: a Sony α57, a Canon 60D, a Nikon D90, and a Nikon D7000. The cameras contain 52, 27, 31 and 26 tampered images, respectively. All images have the same size of 1920×1080 pixels RGB uint8 bitmaps stored in the TIFF format. The forgeries are of various sizes and characters and include object insertion, object removal and more subtle changes to existing content, such as subtle shadows or reflections, which are unlikely to be detected with PRNU analysis. The experiment was performed separately for each camera.

4.2 Parameter selection

Table 1 shows the parameter values used in the experiments. The square window $\omega_s (s = 1, \cdots, S)$ used for interpolation includes $\{32, 48, 64, 96, 128, 192, 256\}$. Parameter J is related to the number of segmentation patches. Note that, in our experiment, the relationship between ω_s and J_s satisfies Eq. (13):

$$\omega_s = \left[\sqrt{\frac{M \times N}{J_s}} \right] \tag{13}$$

where $M \times N$ represents the size of the test image and $[\cdot]$ indicates the rounding function. The parameters used in the camera model and CRF decision are the same as in [25].

4.3 Localization performance and comparisons

To validate the effectiveness of the proposed multi-scale SLIC (M-SLIC) algorithm, we compare the proposed scheme with the 7 single-scale ($\{2025, 900, 506, 225, 127, 56, 32\}$) SLIC methods. ROC curves and the average F_1-score are plotted in Fig. 4 when changing the decision threshold τ on each of the camera datasets separately. Figure 4a shows the ROC curves for four cameras. To improve readability, we show only a close-up of the most relevant region. Compared with all 7 single scales, the proposed M-SLIC strategy delivered superior performance for all four cameras. Similar results can be observed in Fig. 4b, where the average F_1-score plotted when changing the decision threshold τ on each of the datasets. The maximum average F_1-score of the M-SLIC method performed better than all 7 single scales for all cameras. This confirmed that the proposed fusion strategy could effectively combine the benefits of both small-scale and large-scale analyses.

To assess the performance of the proposed PRNU-based M-SLIC algorithm, we also compare it with two other PRNU-based methods. One is the sliding window-based segmentation-guided (SW-SG) strategy [25], and the other is the sliding window-based single scale (SW-SS) detectors with the standard 128×128 pixel window [32]. For these two methods, we use the source codes provided by the authors with default parameters to generate the results. In

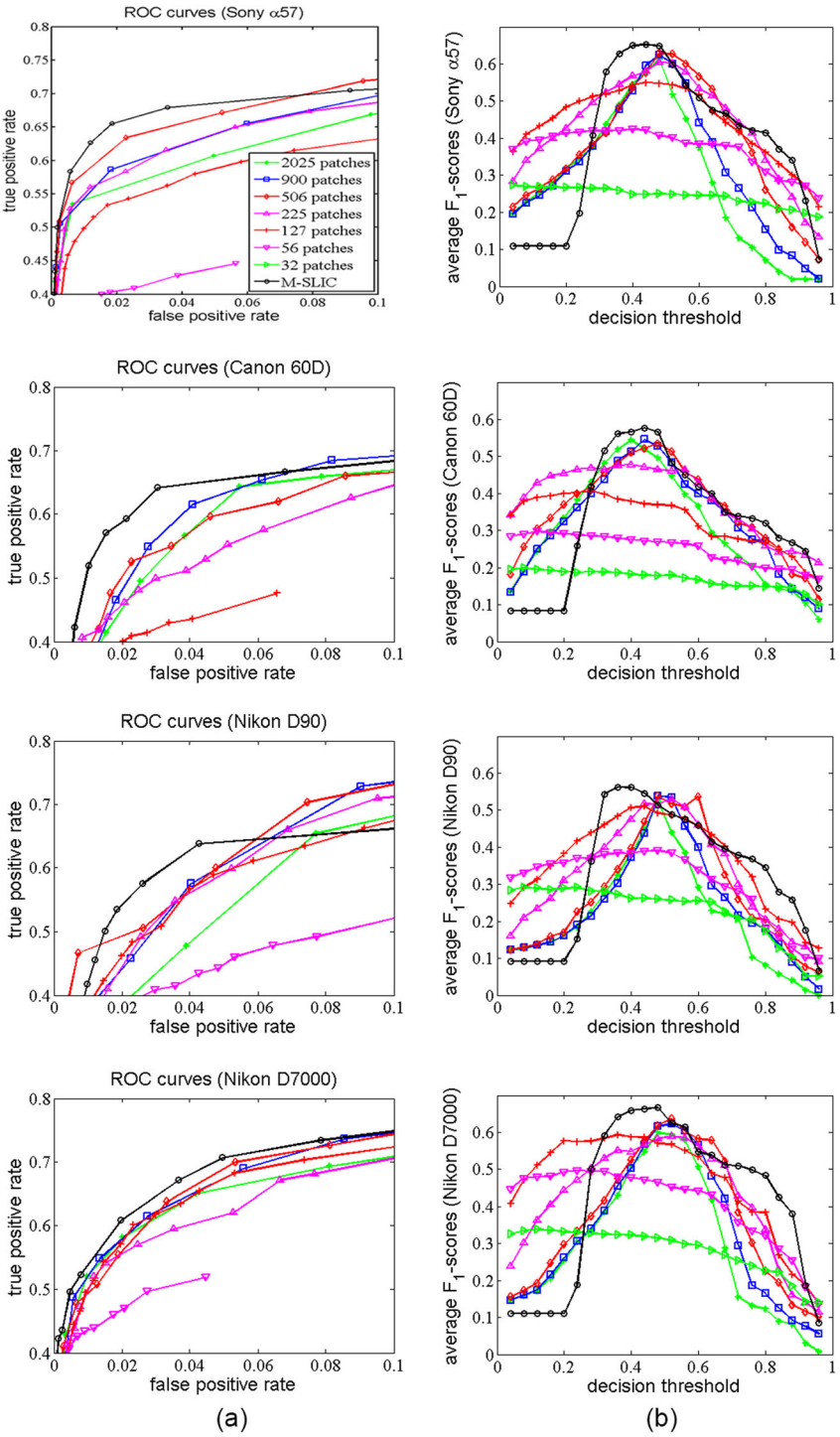


Fig. 4 Comparison of the proposed M-SLIC algorithm with individual single-scale SLIC algorithm. **a** ROC curve comparison. **b** Average F_1-score comparison

addition, we also compare the proposed M-SLIC algorithm with the single-scale SLIC (S-SLIC) algorithm proposed in our previous paper.

In our previous study, it was confirmed through experiments that the average F_1-scores all reached the maximum, with the parameter $J = 700$ for all four cameras. Therefore, in the following comparison, J is fixed to 700 in the S-SLIC algorithm. The obtained results are shown in Figs. 5 and 6. It can be seen that for the Sony α57, Canon 60D and Nikon D7000 cameras, the most stable improvement can be seen for the proposed M-SLIC strategy, which performs better than the SW-SG, SW-SS and S-SLIC methods. For the Nikon D90 dataset, M-SLIC has similar performance as the SW-SG method and is better than the other two methods. Similar tendencies can be observed from the average F_1-score plotted in Fig. 6.

To clearly show which methods perform better, the maximum average F_1-score is shown in Table 2. The maximum value of each camera is highlighted in bold. As shown in Table 2, most of the bold numbers appear in the proposed scheme (the last column), indicating the effectiveness of the proposed M-SLIC algorithm. The insignificant performance decline appears in the Nikon D90 camera. The reason is that in the dataset of the Nikon D90 camera, there are many subtle object removal forgeries.

We also present some examples of tampering localization results in Fig. 7 for the strategies mentioned above. It can be observed that the proposed algorithm can detect small size and large size forgeries. At the same time, the proposed algorithm can not only detect additive

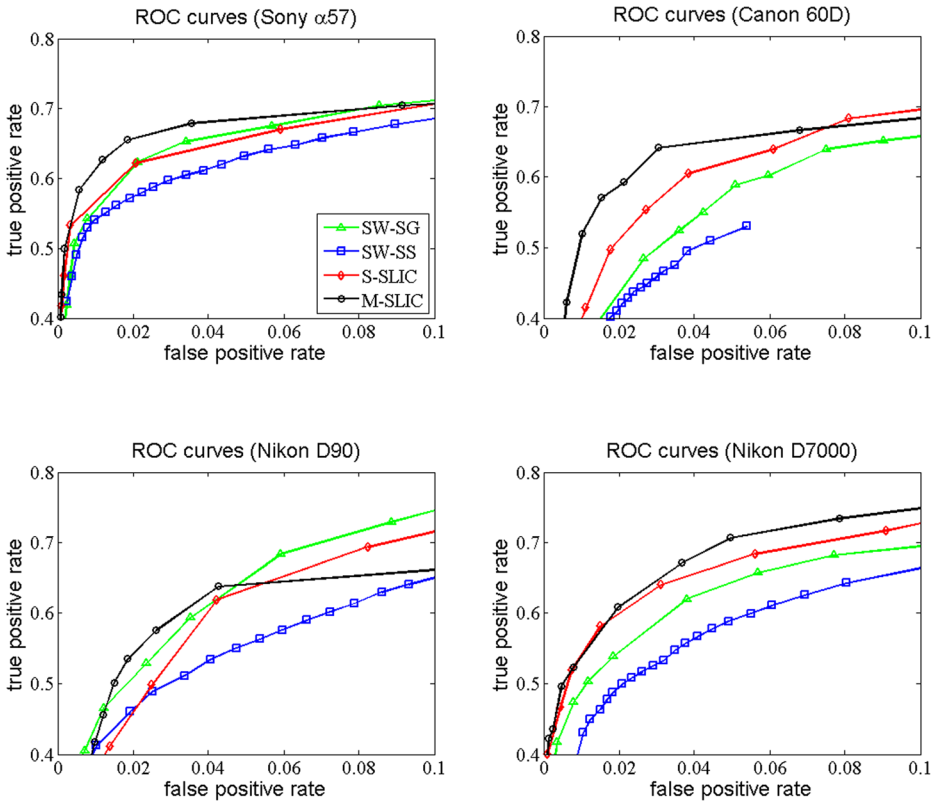


Fig. 5 Comparison of the ROC curves between the proposed M-SLIC algorithm and the SW-SG, SW-SS and S-SLIC ($J = 700$) algorithms for the four cameras

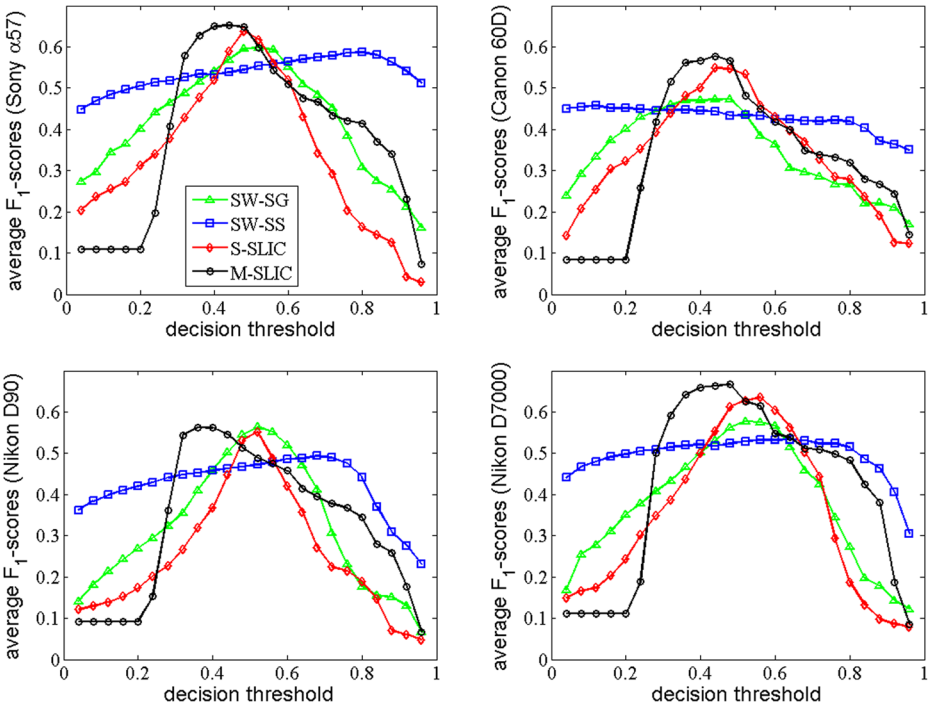


Fig. 6 Comparison of the average F_1 scores between the proposed M-SLIC algorithm and the SW-SG, SW-SS and S-SLIC ($J = 700$) algorithms for the four cameras

tampering (2th and 4th rows), but also detect object removal tampering (1th and 3th rows). Besides, compared with the SW-SG and SW-SS algorithms, the proposed scheme can achieve much better localization accuracy.

4.4 JPEG compression robustness test

The tampered image may undergo JPEG compression after manipulation. The following experimental results demonstrate the performance of the proposed method when the images are JPEG compressed. We used the Nikon D7000 dataset for this experiment. Photoshop is used to compress the TIFF images into JPEG format images with quality factors varying from 100 to 70 in steps of −10. That is, each picture in the original forgery dataset is altered to four versions. We used the same camera models and predictors as in the previous experiments.

Table 2 Maximum average F_1-scores for the four cameras

	Method			
Camera	SW-SS [32]	SW-SG [25]	S-SLIC	Proposed M-SLIC
Sony α57	0.5870	0.5983	0.6384	0.6521
Canon 60D	0.4578	0.4740	0.5500	0.5775
Nikon D90	0.4935	0.5634	0.5516	0.5622
NikonD7000	0.5331	0.5777	0.6347	0.6671

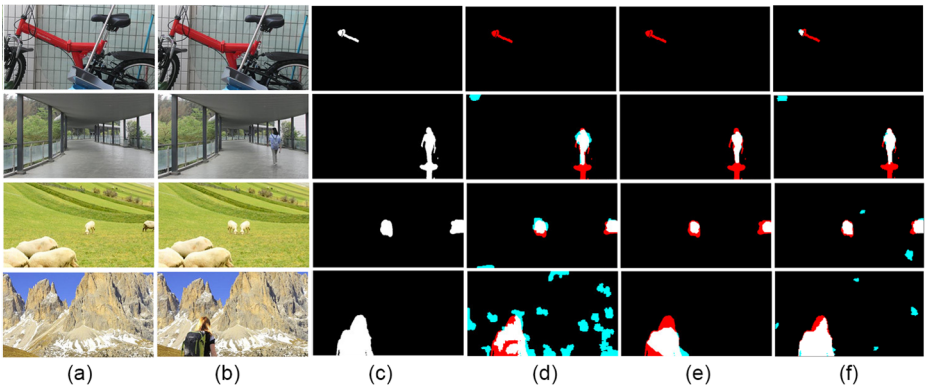


Fig. 7 Example of tampering localization results. The pixels in white, black, red, and green indicate true positive, true negative, false positive, and false negative, respectively. Here, positive means fake pixels, while negative means pristine pixels. **a** Original image. **b** Tampered image. **c** Ground truth. **d** SW-SS [32] method. **e** SW-SG [25] method. **f** Proposed M-SLIC method

The impact of JPEG compression on tampering localization performance is shown in Fig. 8. As the quality factor decreases, the detection result deteriorates. The proposed multi-scale fusion strategy delivers the best maximum average F_1-score for all JPEG quality factors.

5 Conclusion

This paper introduced a novel PRNU-based multi-scale fusion method to expose copy-move and splicing forgery in digital images. Different from existing sliding window-based algorithms, in which correlations of PRNU are estimated on overlapped patches, the proposed

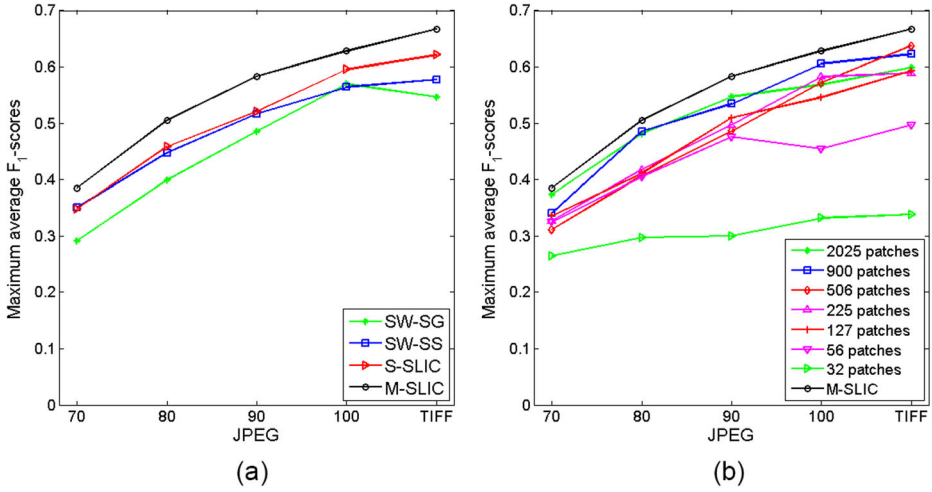


Fig. 8 JPEG compression test for the Nikon D7000 dataset. Note that 70, 80, 90 and 100 are the compression quality factors and TIFF present uncompressed TIFF format images. **a** Comparison of the average F_1-scores between the proposed algorithm with SW-SS and SW-SG algorithms. **b** Comparison of the average F_1-scores between the proposed algorithm with the 7 single scale ($J \in \{2025, 900, 506, 225, 127, 56, 32\}$) SLIC algorithms

algorithm directly segments the test image into nonoverlapping and irregular blocks of multiple scales and computes correlations on nonoverlapped segmentation patches.

The merits of the proposed approach are as follows. The proposed algorithm is particularly good at identifying the location and shape of the object insertion forgeries. It uses nonoverlapped irregular segmentation, which can accurately delineate boundaries of contrasting objects with lower computational complexity. In addition, multi-scale analysis can detect as many types of forgery as possible.

Despite the present advances, there is still considerable room for improvement. Although subtle object removal forgeries can be detected by the proposed scheme, the localization accuracy needs to be further improved in future work. Since PRNU can be contaminated mainly by image content and non-unique artefacts of JPEG compression, how to improve the estimated quality of PRNU is one of the major research orientations in the future. In addition, as a future study, we suggest that we need to design a better and more robust correlation predictor for the PRNU detector.

Acknowledgments This work was supported by National Natural Science Foundation of China (contract No. 61370195, U1536121).

References

1. Achanta R, Shaji A, Smith K, Lucchi A, Fua P, SüSstrunk S (2012) SLIC Superpixels Compared to State-of-the-Art Superpixel Methods. IEEE Transactions on Pattern Analysis & Machine Intelligence 34(11): 2274–2282
2. Al YYB (2001) Interactive Graph Cuts for Optimal Boundary & Region Segmentation of Objects in N-D Images. Iccv 1:105–112
3. Al-Haj A, Amer A (2014) Secured Telemedicine Using Region-Based Watermarking with Tamper Localization. J Digit Imaging 27(6):737–750
4. Amerini I, Ballan L, Caldelli R, Bimbo AD, Serra G (2011) A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery. IEEE Transactions on Information Forensics & Security 6(3):1099–1110
5. Bianchi T, Piva A (2012) Image Forgery Localization via Block-Grained Analysis of JPEG Artifacts. IEEE Transactions on Information Forensics & Security 7(3):1003–1017
6. Carvalho TJD, Riess C, Angelopoulou E, Pedrini H, Rocha ADR (2013) Exposing Digital Image Forgeries by Illumination Color Classification. IEEE Transactions on Information Forensics & Security 8(7):1182–1194
7. Chen M, Fridrich J, Goljan M, Lukás J (2008) Determining Image Origin and Integrity Using Sensor Noise. IEEE Transactions on Information Forensics & Security 3(1):74–90
8. Chierchia G, Cozzolino D, Poggi G, Sansone C, Verdoliva L (2014) Guided filtering for PRNU-based localization of small-size image forgeries. In: IEEE International Conference on Acoustics, Speech and Signal Processing, pp 6231–6235
9. Chierchia G, Parrilli S, Poggi G, Sansone C, Verdoliva L (2011) PRNU-based detection of small size image forgeries. In: International Conference on Digital Signal Processing, pp 1–6
10. Chierchia G, Poggi G, Sansone C, Verdoliva L (2014) A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection. IEEE Transactions on Information Forensics & Security 9(4):554–567

11. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An Evaluation of Popular Copy-Move Forgery Detection Approaches. IEEE Transactions on Information Forensics & Security 7(6):1841–1854
12. Cozzolino D, Gragnaniello D, Verdoliva L (2015) Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques. In: IEEE International Conference on Image Processing, pp 5302–5306
13. Cozzolino D, Poggi G, Verdoliva L (2016) Splicebuster: A new blind image splicing detector. In: IEEE International Workshop on Information Forensics & Security
14. Cozzolino D, Verdoliva L (2017) Single-image splicing localization through autoencoder-based anomaly detection. In: IEEE International Workshop on Information Forensics and Security, pp 1–6
15. Dabov K, Foi A, Katkovnik V, Egiazarian K (2007) Image denoising by sparse 3-D transform-domain collaborative filtering. IEEE Trans Image Process 16(8):2080–2095
16. Fan W, Wang K, Cayre F (2016) General-purpose image forensics using patch likelihood under image statistical models. In: IEEE International Workshop on Information Forensics and Security, pp 1–6
17. Ferrara P, Bianchi T, Rosa AD, Piva A (2012) Image Forgery Localization via Fine-Grained Analysis of CFA Artifacts. IEEE Transactions on Information Forensics & Security 7(5):1566–1577
18. Gaborini L, Bestagini P, Milani S, Tagliasacchi M, Tubaro S (2015) Multi-clue image tampering localization. In: IEEE International Workshop on Information Forensics and Security, pp 125–130
19. Ge L, Ju R, Ren T, Wu G (2015) Interactive RGB-D Image Segmentation Using Hierarchical Graph Cut and Geodesic Distance. In: Pacific Rim Conference on Multimedia, Gwangju. Springer, pp 114–124. https://doi.org/10.1007/978-3-319-24075-6
20. Hou JU, Lee HK (2017) Detection of Hue Modification Using Photo Response Nonuniformity. IEEE Transactions on Circuits & Systems for Video Technology 27(8):1826–1832
21. Johnson MK, Farid H (2007) Exposing Digital Forgeries in Complex Lighting Environments. IEEE Transactions on Information Forensics & Security 2(3):450–461
22. Kai SC, Lam EY, Wong KKY (2006) Source camera identification using footprints from lens aberration. Proceedings of SPIE - The International Society for Optical Engineering 6069:60690J–60690J-60698
23. Kang X, Chen J, Lin K, Peng A (2014) A context-adaptive SPN predictor for trustworthy source camera identification. Eurasip Journal on Image & Video Processing 2014(1):1–11
24. Kokkonis G, Psannis KE, Roumeliotis M, Ishibashi Y (2016) Efficient algorithm for transferring a real-time HEVC stream with haptic data through the internet. J Real-Time Image Proc 12(2):343–355
25. Korus P, Huang J (2017) Multi-Scale Analysis Strategies in PRNU-Based Tampering Localization. IEEE Transactions on Information Forensics & Security 12(4):809–824
26. Lawgely A, Khelifi F (2017) Sensor Pattern Noise Estimation Based on Improved Locally Adaptive DCT Filtering and Weighted Averaging for Source Camera Identification and Verification. IEEE Transactions on Information Forensics & Security 12(2):392–404
27. Li J, Li X, Yang B, Sun X (2015) Segmentation-Based Image Copy-Move Forgery Detection Scheme. IEEE Transactions on Information Forensics & Security 10(3):507–518
28. Lin X, Li CT (2016) Enhancing Sensor Pattern Noise via Filtering Distortion Removal. IEEE Signal Processing Letters 23(3):381–385
29. Lin X, Li CT (2017) Preprocessing Reference Sensor Pattern Noise via Spectrum Equalization. IEEE Transactions on Information Forensics & Security 11(1):126–140
30. Liu Q, Cao X, Deng C, Guo X (2011) Identifying Image Composites Through Shadow Matte Consistency. IEEE Transactions on Information Forensics & Security 6(3):1111–1122
31. Lombaert H, Sun Y, Grady L, Xu C (2005) A multilevel banded graph cuts method for fast image segmentation. Iccv 1 251:259–265
32. Lukas J, Fridrich J, Goljan M (2006) Digital camera identification from sensor pattern noise. IEEE Transactions on Information Forensics & Security 1(2):205–214
33. Lyu S, Pan X, Zhang X (2014) Exposing Region Splicing Forgeries with Blind Local Noise Estimation. Int J Comput Vis 110(2):202–221
34. Mahdian B, Saic S (2007) Detection of copy-move forgery using a method based on blur moment invariants. Forensic Sci Int 171(2):180–189
35. Memos VA, Psannis KE (2016) Encryption algorithm for efficient transmission of HEVC media. J Real-Time Image Proc 12(2):473–482
36. Memos VA, Psannis KE, Ishibashi Y, Kim BG, Gupta BB (2017) An efficient algorithm for media-based surveillance system (EAMSuS) in IoT Smart City Framework. Future Generation Computer Systems
37. Mishra P, Mishra N, Sharma S, Patel R (2013) Region duplication forgery detection technique based on SURF and HAC. Sci World J 2013(1):267691
38. Psannis KE, Ishibashi Y (2006) Impact of Video Coding on Delay and Jitter in 3G Wireless Video Multicast Services. EURASIP J Wirel Commun Netw 2006(1):1–7

39. Psannis KE, Stergiou C, Gupta BB (2018) Advanced Media-based Smart Big Data on Intelligent Cloud Systems. IEEE Transactions on Sustainable Computing. https://doi.org/10.1109/TSUSC.2018.2817043
40. Pun CM, Liu B, Yuan XC (2016) Multi-scale noise estimation for image splicing forgery detection. J Vis Commun Image Represent 38(C):195–206
41. Pun CM, Yuan XC, Bi XL (2015) Image Forgery Detection Using Adaptive Over-Segmentation and Feature Points Matching. IEEE Transactions on Information Forensics & Security 10(8):1705–1716
42. Ryu SJ, Kirchner M, Lee MJ, Lee HK (2013) Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments. IEEE Transactions on Information Forensics & Security 8(8):1355–1370
43. Saiqa K, Arun K (2011) Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform. Int J Comput Appl 6(7):31–36
44. Salloum R, Ren Y, Kuo CCJ (2017) Image Splicing Localization using a Multi-task Fully Convolutional Network (MFCN). J Vis Commun Image Represent 51:201–209
45. Stergiou C, Psannis KE, Plageras AP, Kokkonis G, Ishibashi Y (2017) Architecture for Security monitoring in IoT Environments. Paper presented at the 26th IEEE International Symposium on Industrial Electronics, Edinburgh
46. Yao H, Wang S, Zhang X, Qin C, Wang J (2017) Detecting Image Splicing Based on Noise Level Inconsistency. Multimed Tools Appl 76(10):1–23
47. Zhao Y, Wang S, Zhang X, Yao H (2013) Robust Hashing for Image Authentication Using Zernike Moments and Local Features. IEEE Transactions on Information Forensics & Security 8(1):55–63

Weiwei Zhang received her B.Sc. in Mathematics and Applied Mathematics from Shandong Normal University, Jinan, China in 2004 and the M.S. in Computational Mathematics from Wuhan University, Wuhan, China in 2006. Between 2006 and 2015 She worked as a lecturer at Xingtai University. She is currently pursuing her Ph.D. degree at School of Science, China Agricultural University, Beijing, China. Her current research interests include information security and digital image forensics.

Xinhua Tang received his B.Sc. in Mathematics and Applied Mathematics from Shandong Normal University, Jinan, China in 2004 and the M.S. in Computational Mathematics from Wuhan University, Wuhan, China in 2007. He is currently a lecturer at Shandong University of Political Science and Law, Jinan, China. His research interests include information security and digital image forensics.

Zhenghong Yang received his M.S.degree from Beijing Normal University, Beijing, China, in 1990 and the Ph. D. in 2000 from the same institution. He is currently a professor with the College of Science, China Agricultural University, Beijing, China. His research interests include Matrix Theory and Information Security.

Shaozhang Niu received the B.S. and M.S. degree from Beijing Normal University, Beijing, China, in 1985 and 1988, respectively, and the Ph. D. degree from Beijing University of Posts and Telecommunications, Beijing, China in 2004. He is currently a professor with the School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China. His research interests include Steganography, Steganalysis and digital forensics.

Affiliations

Weiwei Zhang [1] · Xinhua Tang [2] · Zhenghong Yang [1] · Shaozhang Niu [3]

[1] School of Science, China Agricultural University, Beijing 100083, China

[2] School of Information, Shandong University of Political Science and Law, Jinan 250014, China

[3] Beijing Key Lab of Intelligent Telecommunication Software and Multimedia, Beijing University of Posts and Telecommunications, Beijing 100876, China