This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

Image Tampering Localization Using Demosaicing Patterns and Singular Value Based Prediction Residue

Cheol Woo Park[1], Yong Ho Moon[2], and Il Kyu Eom[1]

[1]Department of Electronics Engineering, Pusan National University, 2 Busandaehak-Ro 63 Beon-Gil, Pusan 46241, Republic of Korea
[2]Department of Aerospace and Software Engineering/ReCAPT, Gyeongsang National University, 501 Jinju-daero, Jinju 52828, Republic of Korea

Corresponding author: Il Kyu Eom (e-mail: ikeom@ pusan.ac.kr).

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (NRF-2018R1D1A1B07046213).

ABSTRACT Almost all image sensors measure only one color per pixel through the color filter array. Missing pixels are estimated using a demosaicing process. For this reason, a demosaiced image leaves a particular trace. When an image is manipulated or tampered, the demosaicing trace can be changed. This change can serve as a basic clue for detecting or localizing image tampering. Demosaicing pattern-based tampering localization algorithms require a re-interpolation process, and the prediction residue between the given image and the re-interpolated image is commonly used to localize tampered regions. However, the prediction residue is not always valid because the demosaicing interpolation kernel cannot be known, which deteriorates the localization performance. This paper presents an effective re-interpolation process using singular value decomposition for an unknown demosaicing method. First, the green channel of the given image is decomposed into four sub-images according to the Bayer pattern. For a small block of each sub-image, the singular value decomposition is performed. The prediction residue is obtained by reconstructing the image block after removing the largest singular value. The feature to localize the forged regions is extracted by the logarithm ratio of the prediction residue variance. The proposed method does not require any statistical model for the extracted feature, because the prediction residue is more accurate than that of conventional methods. We perform intensive experiments for three test datasets and compare the proposed method with state-of-the-art tampering localization methods, the results of which indicate that the proposed scheme outperforms existing approaches.

INDEX TERMS Image tampering localization, demosaicing trace, singular value decomposition, prediction residue, re-interpolation kernel, color filter array, image splicing.

I. INTRODUCTION

Images are often used as evidence to determine the authenticity of an event. In recent decades, image manipulation has been employed for the purpose of simple entertainment or as the initial step of a photomontage. However, the use of manipulated images for malicious purposes can demonstrate a negative impact on human society. Because detecting forged images by human eye is difficult, the development of a reliable image tampering detection method is required to determine image authenticity. A wide range of research has been conducted with respect to the detection of various image forgeries [1-4].

A commonly used tampering method is image splicing. If a part of an image is spliced to a part of another image, the spliced image exhibits heterogeneous statistical properties. Choosing which characteristics appear differently by image tampering is vital. Therefore, identifying the different statistical characteristics of the parts of a tampered image is the basis for detecting or localizing image splicing. Splicing detection [5-10] can determine whether a given image is authentic or tampered. In practical forensic applications, localizing splicing regions [11-13] compared with splicing detection is more effective.

Image manipulation always leaves a trace, which can be used to detect tampered images or localize forged regions. In particular, the statistical inconsistencies of blurring [14-16], noise patterns [17-19], JPEG artifacts [20], and color filter

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

array (CFA) patterns [21-23] are widely used as clues to detect forged images or localize tampered regions. Recently, machine learning-based forgery localization networks [24-26] received serious research interest. Among the traces caused by image manipulation, we are interested in CFA pattern artifacts. Various digital forensic approaches are based on CFA pattern, such as source camera-model identification [27], CFA pattern configuration [28-30], color change detection [31, 32], and image authentication [33, 34].

CFA is a specially designed element in a single-sensor imaging pipeline to acquire low-resolution color information in the image scene. The raw data captured by the image sensor with CFA are converted into a full-resolution color image by a demosaicing process, which is a kind of interpolation. When an image is tampered, forged regions exhibit demosaicing inconsistencies within authentic image regions. Accordingly, a number of studies have been conducted [35-40] to localize forged regions using demosaicing traces. However, the interpolation kernel for demosaicing is generally unknown. Thus, almost all methods use the prediction residue between the given suspected image and the estimated image by re-interpolation.

In forgery localization based on CFA patterns, the re-interpolation process is very important and is the first step in generating a tampering localization map. The performance of tampering localization can depend on the selection of the re-interpolation kernel. In general, the re-interpolation kernel is assumed to be bilinear, bicubic, or median [35-37, 40]. These interpolation kernel types only use intra-channel information, and they are, therefore, inappropriate for demosaicing methods using inter-channel color information. To address this, least-squares-based approaches [38, 39] are used to estimate the re-interpolation kernel. However, estimating one kernel for one image is not desirable because more than two interpolation kernels can exist for one spliced image.

This paper presents a novel prediction residue estimation method based on singular value decomposition (SVD) for forgery localization. In the proposed method, the prediction residue is obtained by the reconstructed image by examining the remaining singular values after removing the largest singular value. The proposed method is more efficient in estimating prediction residue compared with conventional estimation algorithms based on the re-interpolation process. We propose a simple feature for the variance ratio of prediction residue to localize the tampered image regions. The proposed scheme does not require CFA configuration information, and it generates superior forgery localization results than conventional localization methods.

The remainder of this paper is organized as follows. Related works are briefly reviewed in Section II. Section III analyzes the variance of prediction residue and its application to forgery localization. The proposed prediction residue estimation and tampering localization algorithm are presented in Section IV. Section V presents the experimental results obtained using the proposed approach, and finally, the paper is concluded in Section VI.

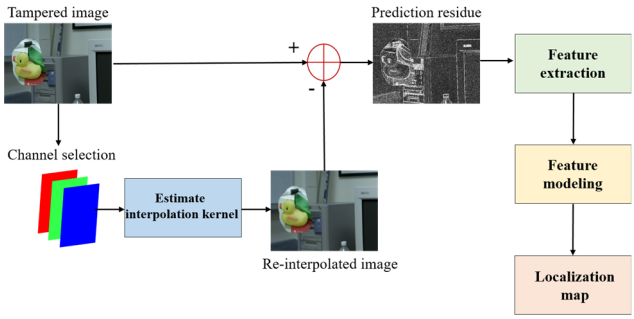


FIGURE 1. A typical process of CFA-based forgery localization.

II. RELATED WORK

Fig. 1 shows the typical process of forgery localization methods using CFA artifacts. First, the green channel [36, 37, 39] or all color channels [35, 38, 40] are selected to estimate the re-interpolation kernel. Next, prediction residue is generated using the difference between the tampered and re-interpolated images by the estimated kernel. Based on the prediction residue, various features are extracted, the most common of which is the variance ratio. Feature models to classify authentic or tampered regions can be developed based on extracted features. Finally, the localization map is obtained using the parameters of the feature model.

In 2009, Dirik et al. [35] presented image tampering detection techniques based on CFA processing. They exploited the fact that the sensor noise variance in interpolated pixels obtained by the demosaicing process is significantly lower than acquired pixels. Based on this, they recognized that a ratio of noise variances between interpolated and acquired pixels can be used to identify image tampering. This method was successfully applied to tamper detection with low error rates. However, this scheme exhibits a limited performance for small tampered regions and produces coarse localization of image forgery.

Ferrara et al. [36] assumed that image tampering removes artifacts due to the demosaicing process. They proposed a new feature measuring the presence of demosaicing artifacts, that is, the logarithm of the geometric mean ratio of the prediction error variance, and introduced a new statistical model that derives the tampering probability of each mage block. This algorithm can generate fine-grained localization of tampered regions. However, the detection performance is affected by JPEG compression, and the forgery maps exhibit high false positives.

Singh et al. [37] presented a high-order statistical approach to detect image forgery. This method uses the Markov transition probability matrix (MTPM) to identify the presence or absence of CFA artifacts in a particular image region. The MTPM was employed on the local variance of the prediction error between the observed and estimated pixels, which improved the quality of forgery map, however, high false

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

positives were recorded in the presence of uniform image regions.

Fernández et al. [38] proposed an image tampering detection technique based on CFA artifacts arising from the differences in the distribution of acquired and interpolated pixels. This approach identifies tampered areas by computing the probability of each pixel of being interpolated and then applying discrete cosine transform (DCT) on small blocks of the probability map. The value of the DCT coefficient for the highest frequency on each block was used to decide whether the analyzed region had been tampered with. However, the method failed to clearly localize tampered regions in the image.

In 2019, Le et al. [39] introduced an improved forgery localization algorithm using demosaicing artifacts. They first explained why the demosaicing-based approach is less effective with JPEG compressed images. A robust statistical feature was presented on the basis of the green-channel prediction residue, and a penalized expectation maximization (EM) algorithm was used to localize forged areas in the tampered image. This method achieved a high localization performance, however, the localization performance was still limited to uncompressed images.

Recently, an image tampering detection technique [40] was proposed by exposing the CFA artifacts in the difference domain through high-order MTPM-based statistical analysis. The suspicious image was first re-interpolated with four of the most commonly used Bayer CFA patterns, and then, the difference between the given image and the re-interpolated versions was evaluated to analyze CFA inconsistencies. The MTPM in the DCT domain was obtained for the difference image. This method produced a significant false positive rate due to the presence of uniform regions.

III. ANALYSIS OF PREDICTION RESIDUE

The prediction residue plays a vital role in localizing the tampered regions of an image. In particular, in almost all methods, the prediction residue variance is exploited to extract features for forgery localization. In this section, we examine demosaicing traces in terms of the mean and variance of the prediction residue in both authentic and interpolated pixels. The analysis is given for a one-dimensional case, the results of which can be easily extended to two-dimensional case.

A. DEMOSAICING PROCESS

Letting $p_A(x)$ be the acquired pixel, we consider demosaicing interpolation of the green pixel in a particular image row, as shown in Fig. 2. The acquired pixel is

$$p_A(x)=\begin{cases} G(x), & \text{if } x \text{ even} \\ 0, & \text{if } x \text{ odd} \end{cases}, \tag{1}$$

where $G(x)$ denotes the green pixel value at location x. Letting $p_D(x)$ denote the demosaiced green pixel at position x, it can be expressed as

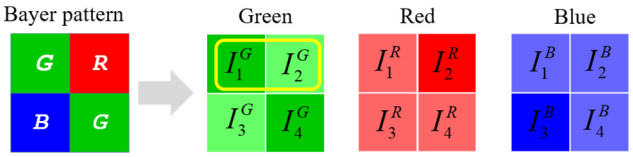


FIGURE 2. Green pixel selection in a row of image surrounded in yellow box.

$$p_D(x)=\begin{cases} G(x), & \text{if } x \text{ even} \\ \sum_u h_u p_A(x+u), & \text{if } x \text{ odd} \end{cases}, \tag{2}$$

where h_u is the interpolation kernel, and $\Sigma_u h_u=1$. When x is odd, the interpolation is achieved using the signal $G(x)$ at x in even positions. Therefore, only odd u values contribute to the convolution in (2). In this case, we assume that the inter-channel information is not used, and the acquired pixels are not modified in the interpolation process.

B. PREDICTION RESIDUE

In many studies, re-interpolation is proven to be efficient with respect to extracting features for forgery localization. However, the choice of the re-interpolation kernel is arbitrary and can affect the localization performance. Letting k_u be the re-interpolation kernel, the re-interpolated pixel $p_R(x)$ can be expressed as

$$p_R(x)=\sum_u k_u p_D(x+u)\ . \tag{3}$$

The prediction residue $e(x)$ can be defined as $e(x)=p_D(x)-p_R(x)$, which can be further expressed

$$e(x)=\begin{cases} G(x)-\sum_u k_u p_R(x+u), & \text{if } x \text{ even} \\ \sum_u h_u p_A(x+u)-\sum_u k_u p_R(x+u) & \text{if } x \text{ odd} \end{cases}. \tag{4}$$

Using (3) and (4), we can obtain

$$e(x)=\begin{cases} G(x)-\sum_u k_u \sum_v h_v G(x+u+v), & \text{if } x \text{ even} \\ \sum_u (h_u-k_u) G(x+u) & \text{if } x \text{ odd} \end{cases}, \tag{5}$$

where $\Sigma_u k_u=1$.

C. VARIANCE OF PREDICTION RESIDUE

Let us assume that $p_A(x)$ is independent and an identically distributed signal. Accordingly, we can easily verify that the mean of $e(x)$ is zero regardless of the position of x. Alternatively, the variance of the prediction residue is dependent on the position of x. If x is even (acquired pixel), the variance of $e(x)$, σ_A^2 can be expressed as

$$\sigma_A^2=\sigma_G^2\left(1+\sum_u k_u^2 \sum_v h_v^2\right), \tag{6}$$

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

where σ_G^2 is the variance of $G(x)$. The variance of the prediction residue at odd x values (interpolated pixel), σ_T^2 is

$$\sigma_T^2 = \sigma_G^2 \sum_u (h_u - k_u)^2 . \quad (7)$$

The detail derivations for these two variances are outlined by [36] and [39].

According to (6) and (7), we can assume that σ_A^2 is higher than σ_T^2 in the presence of CFA demosaicing. If we know the demosaicing kernel h_u, then σ_T^2 is obviously zero. When an image has been forged, the relation $\sigma_A^2 \geq \sigma_T^2$ can be broken. Therefore, the imbalance between the prediction residue variance for even and odd locations is an important clue in detecting/localizing image tampering.

The relation $\sigma_A^2 \geq \sigma_T^2$ is available under the assumption that the demosaicing interpolations do not use inter-channel information. However, the relation $\sigma_A^2 \geq \sigma_T^2$ can be broken when inter-channel interpolation is used. To examine this, we selected 50 images with RGGB Bayer pattern, and performed six famous demosaicing interpolations, including bilinear kernel, the adaptive homogeneity-directed (AHD) method [41], the variable number of gradients (VNG) algorithm [42], DCB demosaicing [43], IGV demosaicing [44], and the heterogeneity-projection hard-decision (HPHD) color interpolation [45]. For re-interpolation, the most popular bilinear method is used, as well as kernel estimation methods based on ordinary least squares (OLS) [38] and OLS using with smooth regions (OLSSR) [39].

Table 1 shows the probability that σ_A^2 is greater than σ_T^2 for the green color channel. For any image, a 2×2 Bayer pattern matrix has four components. Therefore, σ_A^2 is obtained by adding two variances based on i=2 and i=3. Alternatively, σ_T^2 is calculated by adding two variances based on i=1 and i=4. As shown Table 1, bilinear- and DCB-demosaiced cases are successful for all re-interpolation methods. However, three re-interpolation algorithms for the other demosaicing interpolations either slightly (AHD and VNG) or significantly (IGV and HPHD) fail to satisfy $\sigma_A^2 \geq \sigma_T^2$. On average, three kinds of re-interpolation kernels essentially have same success rates (roughly 0.78). The performance of the forgery localization is highly dependent on the variance of the prediction error between demosaiced and re-interpolated images. As observed in Table 1, the conventional re-interpolation methods demonstrate limited performances. As such, we introduce a new algorithm to obtain prediction residue using SVD.

TABLE 1. Probability of satisfying the relation $\sigma_A^2 \geq \sigma_T^2$.

Demosaicing kernel	Re-interpolation kernel		
	Bilinear	OLS	OLSSR
Bilinear	1.00	1.00	1.00
AHD [41]	0.88	0.94	0.94
VNG [42]	0.90	0.86	0.84
DCB [43]	1.00	0.98	0.98
IGV [44]	0.68	0.52	0.58
HPHD [45]	0.20	0.36	0.30
Average	0.78	0.78	0.77

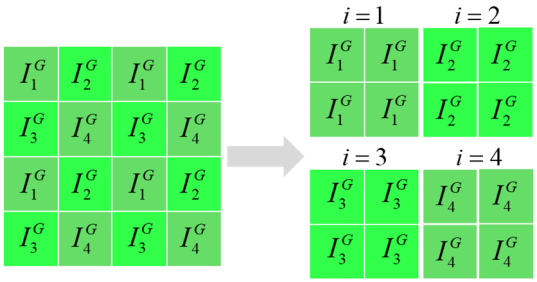


FIGURE 3. Example of green component decomposition for a Bayer pattern in an image.

IV. PROPOSED METHOD

Many demosaicing algorithms attempt to preserve or enhance the image edge component, however, this is not always successful. Accordingly distinguishing between the original and interpolated background areas can be difficult. For this reason, a bilinear kernel is a good choice for the re-interpolation kernel. However, because bilinear interpolation is performed at every position with the same kernel, it does not reflect local image variation. Because of this, the utility of the prediction residue obtained by bilinear kernelling is reduced for edge-preserving demosaicing methods.

SVD for a small image block can be used to obtain the prediction residue. The large singular values of an image block mainly contain low-frequency background information. Conversely, small singular values are associated with high-frequency block components. Therefore, an image reconstructed by small singular values can be considered as prediction residue. Because SVD is performed at a small image block, the prediction residue contains the local variation of the image.

A. IMAGE DECOMPOSION

In this paper, we only use the green channel to localize tampered regions. For the given suspicious image, we let $\mathbf{I}^G$ be the green channel (from hereon in, the superscript G is omitted). The green channel can be rearranged to four down-sampled sub-images according to pixel location in the 2×2 Bayer pattern matrix. By decomposition, $\mathbf{I}$ can be expressed as

$$\mathbf{I} = \begin{bmatrix} \mathbf{I}_1 & \mathbf{I}_2 \\ \mathbf{I}_3 & \mathbf{I}_4 \end{bmatrix}, \quad (8)$$

where $\mathbf{I}_i$ is the down-sampled green component ($i \in \{1,2,3,4\}$ is the index of the sub-image corresponding to the 2×2 Bayer pattern matrix), and $I_i(x,y)$ represents the pixel value at the (x,y) position. In this paper, we omit the variables that indicates position, that is, x and y, as long as no confusion occurs. Bold characters represent matrices and non-bold italic characters imply scalar values. Fig. 3 shows an example of color component decomposition for a GXXG Bayer pattern.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

B. PREDICTION RESIDUE BASED ON SINGULAR VALUES

Letting $\mathbf{J}_i$ be a square block with size $Q\times Q$ centered on (x,y), the SVD of $\mathbf{J}_i$ is the factorization of $\mathbf{J}_i$ into the product of three matrices as.

$$\mathbf{J}_i = \mathbf{WSZ}^T, \tag{9}$$

where $\mathbf{W}$ and $\mathbf{Z}$ are orthogonal matrices, and $\mathbf{S}$ is a diagonal matrix with singular values on the diagonal. There are Q singular values with the condition of $\lambda_1 \geq \ldots \lambda_q \geq \ldots \lambda_Q \geq 0$, where λ_q is the q-th singular value. Large singular values only contain information about the background or uniform areas, whereas small singular values contain much more detailed information. We introduce a method that can obtain the prediction residue by removing the largest singular value.

$\mathbf{J}_i$ can be alternately expressed in summation form as

$$\mathbf{J}_i = \sum_{q=1}^{Q} \lambda_q \mathbf{w}_q \mathbf{z}_q^T, \tag{10}$$

where $\mathbf{w}_q$ is the left singular vector, and $\mathbf{z}_q$ is the light singular vector. To obtain the prediction error, we reconstruct the image block after removing the largest singular value λ_1, which can be expressed as

$$\mathbf{R}_i = \sum_{q=2}^{Q} \lambda_q \mathbf{w}_q \mathbf{z}_q^T, \tag{11}$$

where $\mathbf{R}_i$ is the reconstructed block without λ_1. From (11), we can define the prediction residue $e_i(x,y)$ at (x,y) as

$$e_i(x,y) = R_i(x,y), \tag{12}$$

where $R_i(x,y)$ is the reconstructed pixel without λ_1 at (x,y). To obtain the prediction residue $e_i(x+1,y)$ at location $(x+1,y)$, the $M\times M$ block slides one pixel to the right.

Table 2 presents the probability that σ_A^2 is greater than σ_T^2 obtained by the proposed SVD-based prediction residue for the green color channel. The test conditions are the same as those in Table 1. As shown in Table 2, the average probability of satisfying the relation $\sigma_A^2 \geq \sigma_T^2$ is 0.84, which is greater than that of bilinear or OLS-based estimation methods. The prediction residue based on SVD is adaptively calculated using local pixel values without the re-interpolation kernel. Therefore, the proposed algorithm can more precisely estimate the prediction residue than existing algorithms.

TABLE 2. Probability of satisfying the relation $\sigma_A^2 \geq \sigma_T^2$ based on the proposed method.

Demosaicing kernel	Proposed SVD
Bilinear	1.00
AHD [41]	0.96
VNG [42]	0.98
DCB [43]	1.00
IGV [44]	0.66
HPHD [45]	0.42
Average	0.84

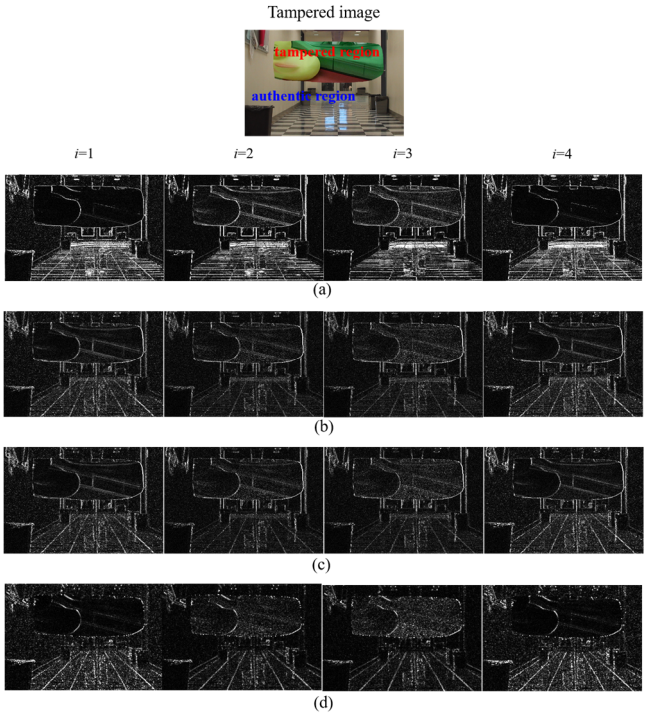


FIGURE 4. Prediction residues obtained by various re-interpolation kernels. (a) bilinear kernel, (b) OLS kernel, (c) OLSSR kernel, and (d) proposed SVD-based re-interpolation.

Fig. 4 depicts the prediction residue for a tampered image obtained by various estimation methods, including the proposed algorithm. In this example, we do not know which interpolation kernel is used in the demosaicing process. We estimate that the Bayer pattern type will be GXXG, because the variances of i=1 and i=4 seem to be greater than those of i=2 and i=3 in the authentic region. Alternatively, we can observe that the variances of i=1 and i=4 are obviously smaller than those of i=2, and i=3 in the tampered region.

As shown in Fig. 4(a), the relation $\sigma_A^2 \geq \sigma_T^2$ is broken in the tampered region when re-interpolation is performed using the bilinear kernel. However, in the authentic region, strong edges are not sufficiently removed. OLS-based re-interpolation methods provide more accurate discrimination in the acquired regions compared with bilinear re-interpolation, however, the discrimination decreases in the tampered region as shown in Fig. 4(b) and (c). In contrast, the prediction residues obtained by the proposed algorithm exhibit good discrimination in both authentic and tampered regions as shown in Fig 4(d).

C. FEATURE EXTRACTION

In most localization approaches [36-39], the weighted variance of the prediction residue and its geometric mean are both calculated. The logarithm of mean ratio is used to achieve forgery localization. In addition, Gaussian mixture modeling, which results in an EM algorithm, is exploited for the extracted logarithm-mean ratio feature.

In this paper, we propose a simple feature extraction algorithm. First, we calculate the variance of the prediction

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

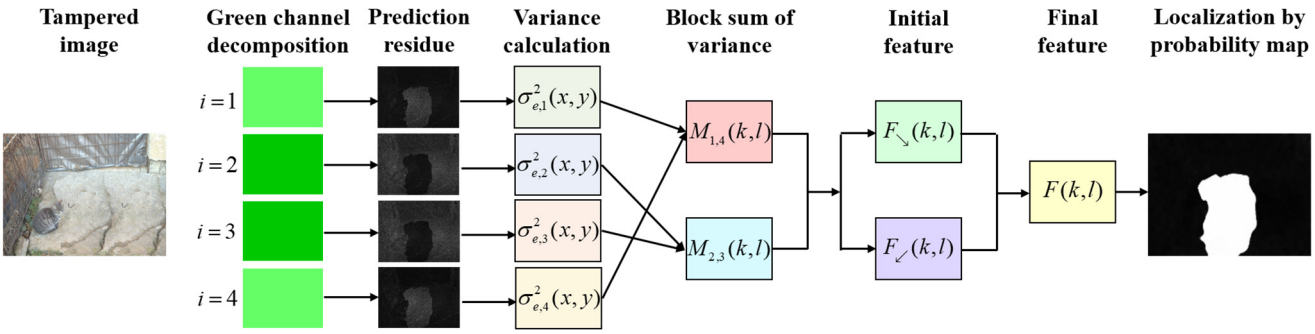


FIGURE 5. Overall system of proposed algorithm.

under the assumption that the local stationarity of prediction residue is valid in a $(2K+1)\times(2K+1)$ window. The local variance of the prediction residue is

$$\sigma^2_{e,i}(x,y)=\frac{1}{(2K+1)^2}\sum_{m,n=-K}^{K}\left[e_i^2(x+m,y+n)-\mu^2_{e,i}\right], \quad (13)$$

where $\mu_{e,i}^2$ is the local mean of the prediction residue. Next, we divide the given variance image into $B\times B$ non-overlapping blocks, where B is related to the period Bayer pattern mosaic. Letting $B_i(k,l)$ be the $B\times B$ variance block in the block index (k,l) and sub-image index i. The proposed feature, $F_{\searrow}(k,l)$ is

$$F_{\searrow}(k,l)=\log\left(\frac{M_{1,4}(k,l)}{M_{2,3}(k,l)}\right), \quad (14)$$

where

$$M_{1,4}(k,l)=\sum_{x,y\in B_1(k,l)}\sigma^2_{e,1}(x,y)+\sum_{x,y\in B_4(k,l)}\sigma^2_{e,4}(x,y), \quad (15)$$

and

$$M_{2,3}(k,l)=\sum_{x,y\in B_2(k,l)}\sigma^2_{e,2}(x,y)+\sum_{x,y\in B_3(k,l)}\sigma^2_{e,3}(x,y). \quad (16)$$

Because the Bayer pattern type is not known, swapping $M_{1,4}(k,l)$ and $M_{2,3}(k,l)$ in (14) can also be a feature. The swapped feature, of $F_{\swarrow}(k,l)$ is $-F_{\searrow}(k,l)$. The GXXG pattern corresponds to $F_{\searrow}(k,l)$, whereas the XGGX pattern corresponds to $F_{\swarrow}(k,l)$. Assuming that the tampered area is smaller than the acquired area, we define the final feature, $F(k,l)$ as follows.

$$F(k,l)=\begin{cases}F_{\searrow}(k,l), & \sum_{k,l}F_{\searrow}(k,l)<\sum_{k,l}F_{\swarrow}(k,l)\\ F_{\swarrow}(k,l), & \text{otherwise}\end{cases}. \quad (17)$$

In conclusion, the proposed algorithm can localize tampered regions even if the Bayer pattern type is unknown.

D. LOCALIZATION

The proposed feature exhibits a range of $-\infty<F(k,l)<\infty$. To localize foraged regions, we introduce a probability map using $F(k,l)$ as

$$P(k,l)=\frac{1}{1+e^{F(k,l)}}, \quad (18)$$

where $P(k,l)$ represents the probability that the block $B(k,l)$ has been tampered. Before obtaining $P(k,l)$, 5×5 median filtering is applied to $F(k,l)$.

E. OVERALL ALGORITHM

The overall proposed algorithm is presented in Fig. 5. From the given image, the green channel is decomposed into four sub-images according to the Bayer pattern. The prediction residues are obtained based on SVD by removing the largest singular value. Four variance images for four corresponding prediction residues are calculated. The feature is extracted based on (17). Finally, the probability map using (18) is calculated to localize tampered regions.

In the proposed method, there are three parameters, including Q, K, and B. Table 3 shows the parameter values used in our experiment.

TABLE 3. Three parameter values used in the experiment.

Parameter	Value
Square block size for SVD: $Q\times Q$	Q=3
Window size for variance calculation: $(2K+1)\times(2K+1)$	K=4
Square block size for feature extraction: $B\times B$	B=16

V. SIMULATION RESULTS

To verify the effectiveness of the proposed tampering localization method, we tested it on three datasets, including the Columbia uncompressed image splicing detection evaluation dataset (CUISDE) [46], image manipulation dataset (IMD) [47], and realistic tampering dataset (RTD) [48]. CUISDE presents 180 images for evaluating splicing detection performance, and it is the easiest dataset to use of the three listed. IMD is comprised of 160 images, whereas RTD presents 220 images for image forgery detection. The images of RTD are captured by four camera models, such as Canon 60D, Nikon D90, Nikon D7000, and Sony A57. RTD presents both copy-moved and spliced images. The performance of our approach is compared with those of four state-of-the-art methods, namely, Dirik's [35], Ferrara's [36], Fernández's [38], and Le's [39] algorithms. The code of the proposed algorithm is available in [49].

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

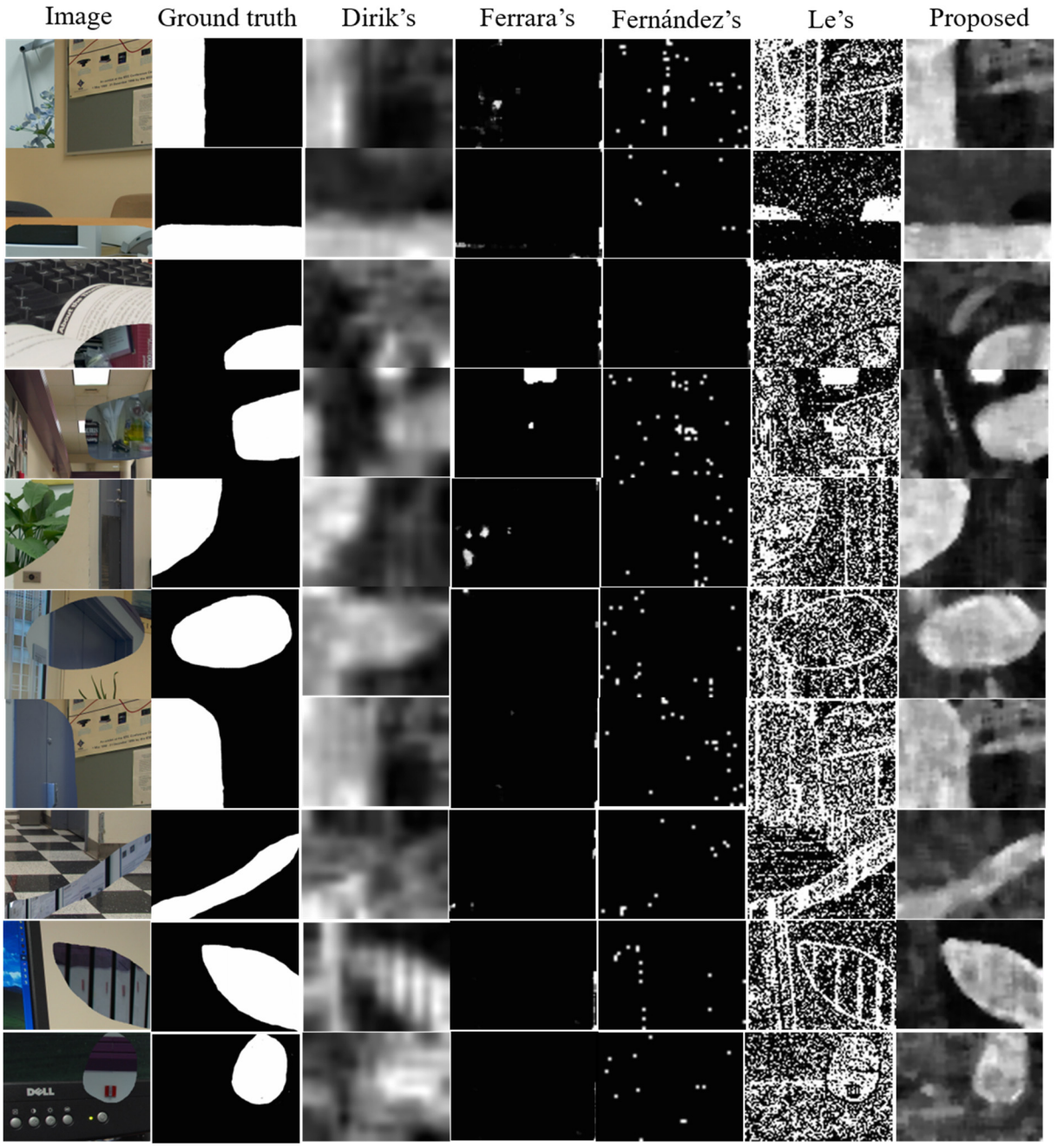


FIGURE 6. Performance comparison of various tampering localization methods for CUISDE [46].

A. QUALITATIVE COMPARISON

Fig. 6 compares the performance of the proposed algorithm for CUISDE with four image tampering localization methods. As shown in Fig. 6, Dirik's method roughly localizes the tampered region region. Ferrara's and Fernández's methods fail to localize in many cases. Le's algorithm identifies a tampered region, however, it generates a lot of false detected pixels. Overall, the proposed method has the best localization performance.

The localization results for IMD are depicted in Fig. 7. As shown in Fig. 7, Dirik's method does not efficiently localize the tampered area. Rather, it shows up the contour of the foraged areas. Ferrara's method often fails to achieve localization, however, it is successful for some images. Fernández's and Le's methods achieve reasonable localization performance, however, in some images, their algorithms produce erroneous results. The proposed scheme demonstrates the best localization performance with relatively low erroneous regions. All methods do not localize authentic

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

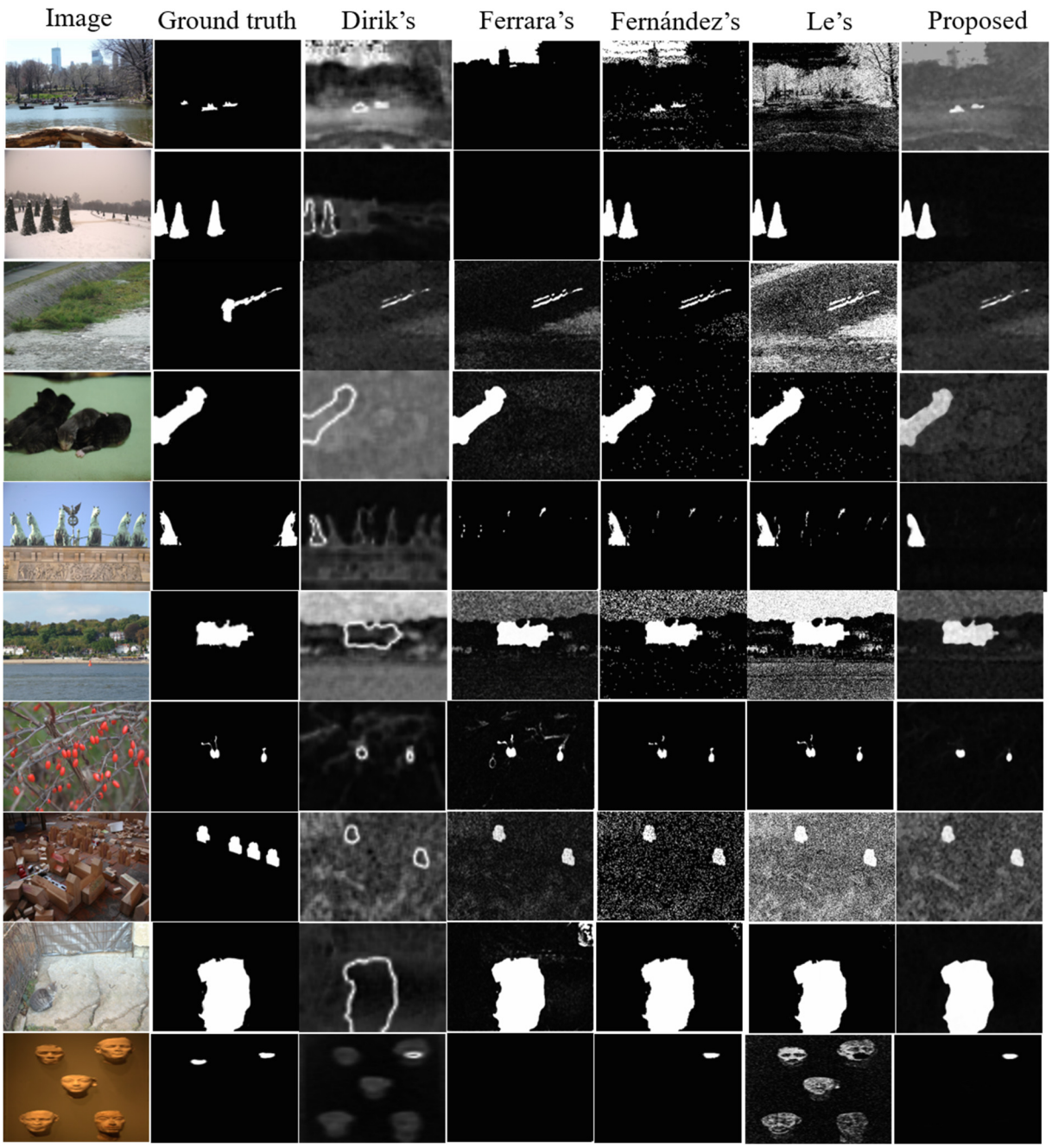


FIGURE 7. Performance comparison of various tampering localization methods for IMD [47].

regions in copy-moved images, because CFA pattern-based approaches can only localize moved areas.

Fig. 8 presents the localization performance for RTD. Dirik's method almost highlights the tampered regions, however, it exhibits large erroneous areas. Although the other three existing algorithms can identify tampered regions, they still falsely identify acquired areas as forged regions. The proposed approach achieves reasonable localization performance.

B. FAILURE CASES

If the Bayer pattern configuration and demosaicing method of the tampered region are the same as those of the acquired region, the CFA pattern-based tampering localization scheme will fail. In this case, the relation $\sigma_A^2 \geq \sigma_I^2$ does not serve as a criterion for detecting or localizing image tampering. This fact is a limitation of the forgery detection method based on demosaicing traces. Fig. 9 illustrates some failure cases of the conventional and proposed methods. As expected earlier, the localization maps exhibit a random pattern or highlight salient regions.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

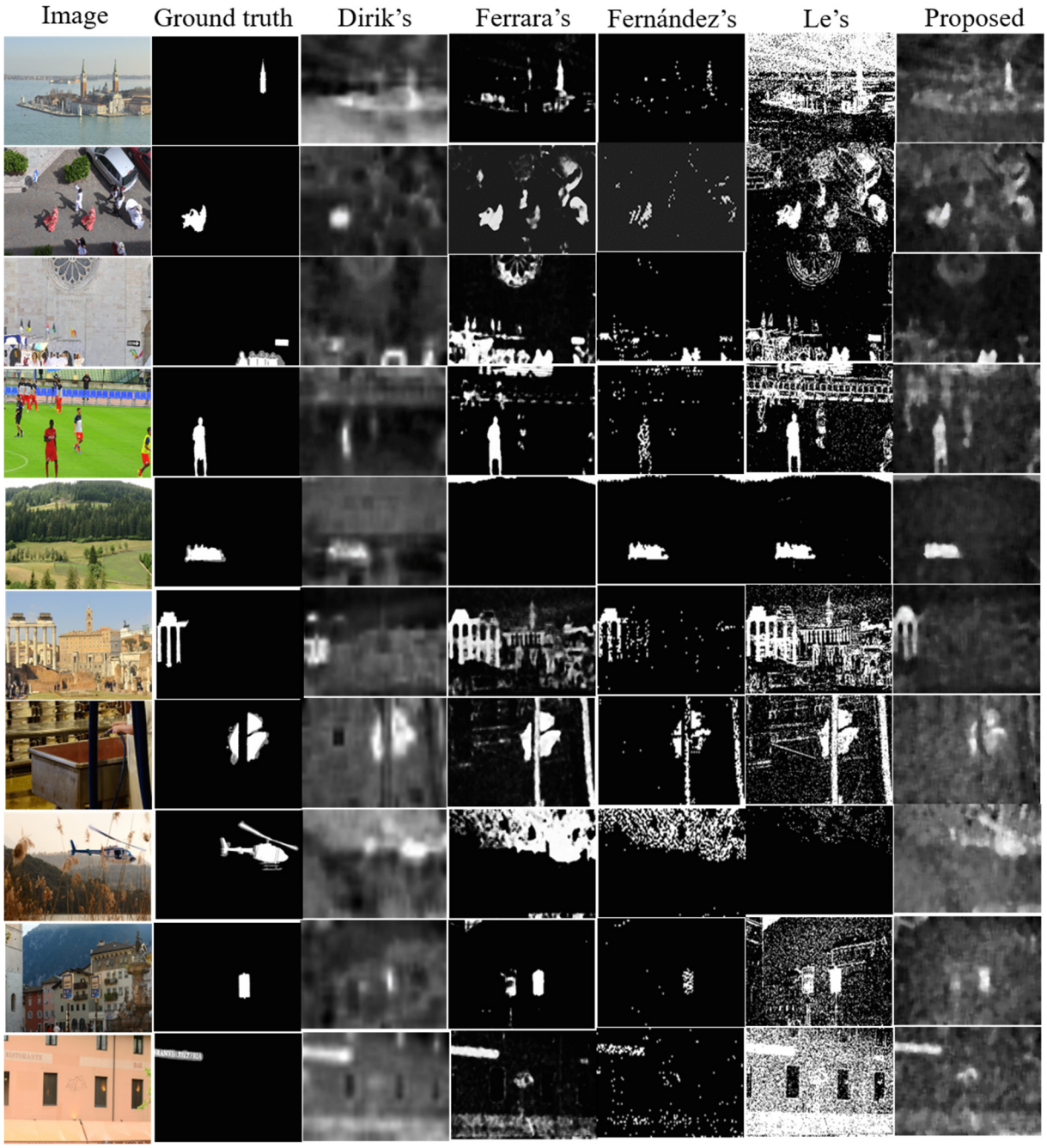


FIGURE 8. Performance comparison of various tampering localization methods for RTD [48].

C. QUANTITATIVE COMPARISON

The proposed method and four existing localization algorithms give a probability or score. Therefore, we use a receiver operator characteristic (ROC) curve [50] and a precision-recall curve for quantitative comparison. The ROC curve is a graphical plot, which shows the diagnostic ability of binary classifiers. In essence, it shows the trade-off between the true positive rate and the false positive rate. The true positive rate is the proportion of tampered pixels correctly localized, whereas the true negative rate indicates the proportion of acquired pixels wrongly localized. The ROC curve close to the top-left corner represents an optimal classification performance. The precision-recall curve shows the tradeoff between precision and recall for different threshold. A high area under this curve represents both high recall and high precision. A high precision relates to a low false positive rate, and a high recall relates to a low false negative rate. High precision-recall scores for both show that

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

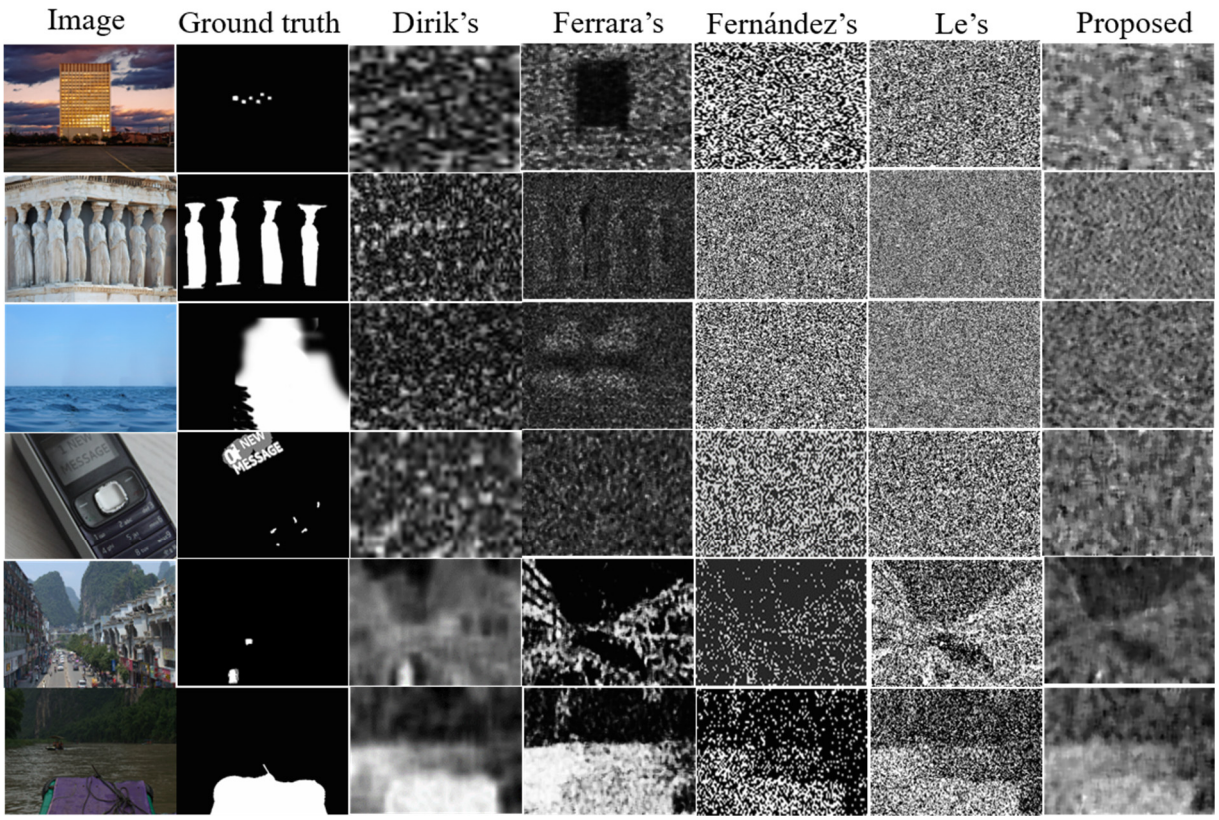


FIGURE 9. Failure cases.

the classifier is returning accurate results, as well as returning a majority of all positive results.

Fig. 10 shows the ROC curves for various tampering localization methods. In Fig. 10, we also present an area under curve (AUC) value, which is a performance indicator of each localization method into a single measure, and it is a general measure of predictive accuracy. Fig. 10(a) depicts the ROC curves for all 560 test images. As shown in Fig. 10(a), the proposed tampering localization algorithm has the best performance. The AUC value of the proposed method is 0.834, which is higher than that of other localization methods. The forgery localization performance for each dataset is also depicted in Fig. 10. Fig. 10(b) presents ROC curves and AUC values for CUISDE. The proposed algorithm has an AUC value of 0.947, which is the greatest value of the five algorithms. Le's method is ranked in second (0.865), followed by Dirik's (0.860), Ferrara's (0.805), and Fernández's (0.732) methods. The ROC curves for IMD are illustrated in Fig. 10(c). The proposed scheme demonstrates the best performance, followed by Ferrara's algorithm. For this dataset, localizing tampered regions is hard because it contains copy-move images. Finally, Fig. 10(d) shows the results for RTD. In this dataset, the localization performance is similar for the proposed method, as well as for Dirik's, and Ferrara's methods.

Fig. 11 illustrates the precision-recall curves for various forgery localization methods. Fig. 11(a) shows the precision-recall curves for all test images. As shown in Fig. 11(a), the proposed localization method has the best performance. Figs. 11(b), 11(c), and 11(d) depict curves for CUISDE, IMD, and RTD, respectively. As shown in these figures, the proposed approach has the superior localization performance for all datasets.

D. EFFECT OF PARAMETERS

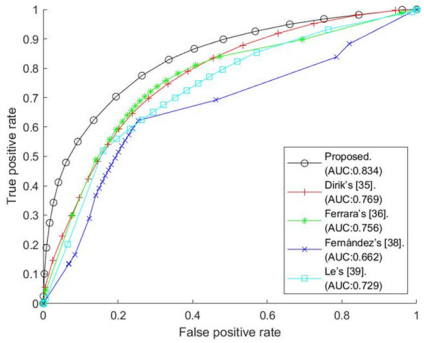
Fig. 12 shows the effect of parameters in localizing tampered regions. Fig. 12(a) presents the AUC values for various B sizes. Except for the smallest block size of B=4, all demonstrate high AUC values. Fig. 12(b) shows the ROC curves of the proposed method according to various Q size. AUC values are 0.834, 0.825, and 0.808 when Q is 3, 5, and 7, respectively. When Q=3, the largest AUC values are achieved. Even when Q=7, which exhibits the lowest ACU value, the proposed method exhibits a higher AUC value compared with the other methods. All results obtained by the proposed algorithm used the parameter values shown in Table 3.

IV. CONCLUSION

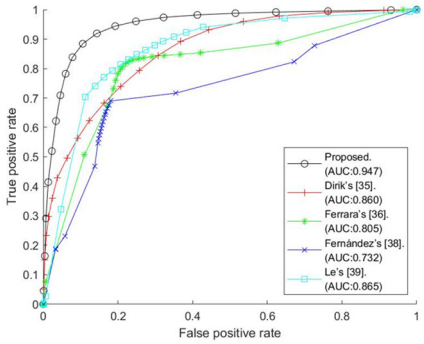
In this paper, we proposed a novel image tampering localization method based on CFA pattern artifacts without knowledge of CFA configuration. We introduced SVD to estimate the prediction residue between the acquired and re-interpolated images. The prediction residue was obtained in the reconstructed image by examining the remaining singular

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

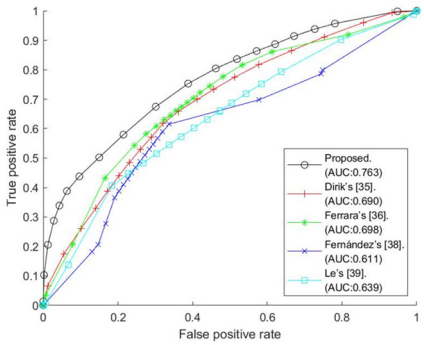
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access



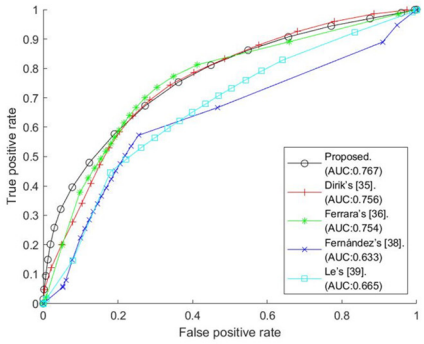
(a)



(b)

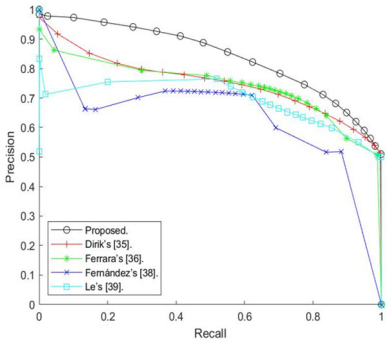


(c)

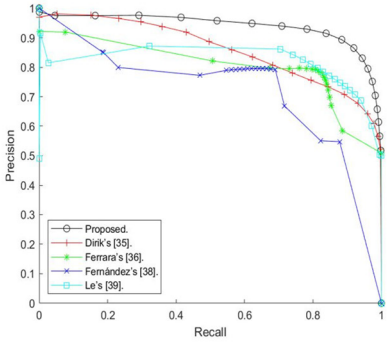


(d)

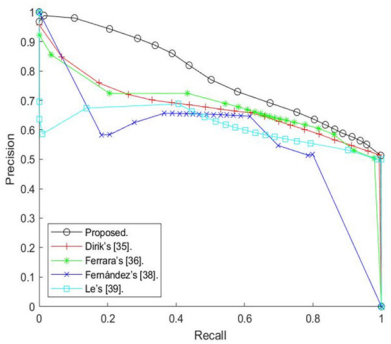
FIGURE 10. ROC curve and AUC value for various datasets. (a) all dataset, (b) CUISDE, (c) IMD, and (d) RTD.



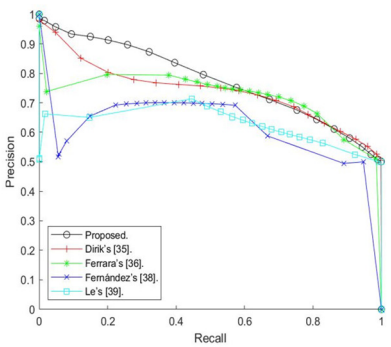
(a)



(b)



(c)



(d)

FIGURE 11. Precision-recall curve and AUC value for various datasets. (a) all dataset, (b) CUISDE, (c) IMD, and (d) RTD.

values after removing the largest singular value. We showed that the prediction residue of the proposed algorithm was more efficient for localizing forged regions. A simple feature using the logarithm of the ratio of the variance of prediction residue was extracted. Finally, we obtained the probability map to localize tampered regions using extracted features.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

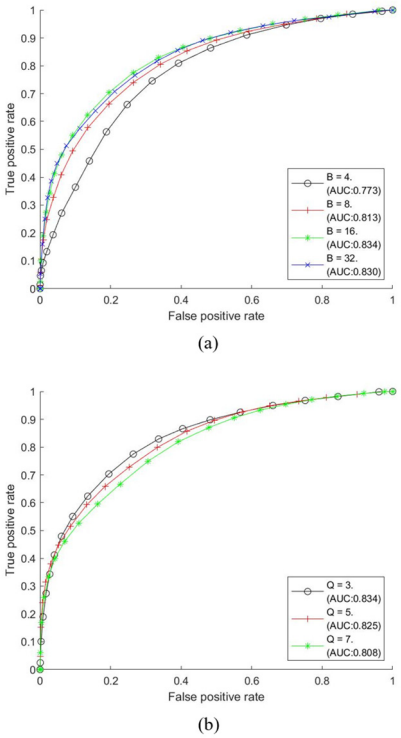


FIGURE 12. ROC curve and AUC value for various parameters obtained by proposed method. (a) various *B* values, and (b) various *Q* values.

The proposed method was compared with existing tampering localization algorithms, the results of which showed that the proposed scheme outperforms state-of-the-art approaches in terms of subjective and objective qualities.

REFERENCES

[1] W. D. Ferreira, C. B. R. Ferreira, G. Cruz Júnior, and F. Soares, "A review of digital image forensics," *Comput. Electr. Eng*., vol. 85, 106685, July, 2020.

[2] R. Thakur, R. Rohilla, "Recent advances in digital image manipulation detection techniques: A brief review," *Forensic Sci. Int*., vol. 312, 110311, July, 2020.

[3] X. Lin, J. H. Li, S. L. Wang, A. W. C. Liew, F. Cheng, and X. S. Huang, "Recent advances in passive digital image security forensics: A brief review," *Engineering*, vol. 4, pp. 29-39, Feb. 2018.

[4] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques: a review," *Aust. J. Forensic Sci*., vol. 49, no. 3, pp. 281-307, May, 2017.

[5] Z. He, W. Lu, W. Sun, and J. Huang, "Digital image splicing detection based on Markov features in DCT and DWT domain," *Pattern Recog*., vol. 45, no. 12, pp. 4292–4299, Dec. 2012.

[6] X. Zhao, S. Wang, S. Li, and J. Li, "Passive image-splicing detection by a 2-D noncausal Markov model," *IEEE Trans. Circuits Syst. Video Technol*., vol. 25, no. 2, pp. 185-199, Feb. 2015.

[7] T. H. Park, J. G. Han, Y. H. Moon and I. K. Eom, "Image splicing detection based on inter-scale 2D joint characteristic function moments in wavelet domain," *EURASIP J. Image Video Process*., vol. 2016:30, Oct. 2016.

[8] B. Chen, X. Qi, X. Sun, and Y. Q. Shi, "Quaternion pseudo-Zernike moments combining both of RGB information and depth information for color image splicing detection," *J. Vis. Commun. Image vol*., 49, pp. 283-290, Nov. 2017.

[9] J. G. Han, T. H. Park, Y. H. Moon and I. K. Eom, "Quantization based Markov feature extraction method for image splicing detection," *Mach. Vis. Appl*., vol. 29, no. 3, pp. 543-552, April, 2018.

[10] N. Kanwal, A. Girdhar, L. Kaur, and J. S. Bhullar, "Digital image splicing detection technique using optimal threshold based local ternary pattern," *Multimed. Tools Appl*., vol. 79, pp. 12829–12846, Jan. 2020.

[11] M. Zampglou, S. Papadopoulus, and Y. Kompatsiaris, "Large-scale evaluation of splicing localization algorithms for web images," *Multimed. Tools Appl*., vol. 76, pp. 4801–4834, Sep. 2016.

[12] P. Sun, Y. Lang, S. Fan, Z. Shen, L. Liu, D. Shan, and S. Peng, "Exposing splicing forgery based on color temperature estimation," *Forensic Sci. Int*., vol. 289, pp. 1-11, Aug. 2018.

[13] S. Dua, J. Singh, and H. Parthasarathy, "Detection and localization of forgery using statistics of DCT and Fourier components," *Signal Process. Image Commun*., vol. 82, 115778, March 2020.

[14] M. P. Rao, A. N. Rajagopalan and G. Seetharaman, "Harnessing motion blur to unveil splicing," *IEEE Trans. Inf. Forensics Secur*., vol. 9, no. 4, pp. 583-595, April 2014.

[15] K. Bahrami, A. C. Kot, L. Li, and H. Li, "Blurred image splicing localization by exposing blur type inconsistency," *IEEE Trans. Inf. Forensics Secur*., vol. 10, no. 5, pp. 999–1009, May 2015.

[16] D. M. Uliyan, H. A. Jalab, A. W. Wahab, P. Shivakumara, and S. Sadeghi, "A novel forged blurred region detection system for image forensic applications," *Expert Syst. Appl*., vol. 64, pp. 1–10, Dec. 2016.

[17] S. Lyu, X. Pan, and X. Zhang, "Exposing region splicing forgeries with blind local noise estimation," *Int. J. Comput. Vis*., vol. 110, no. 2, pp. 202–221, Nov. 2014.

[18] N. Zhu, and Z. Li, "Blind image splicing detection via noise level function," *Signal Process. Image Commun*., vol. 68, pp. 181-192, Oct. 2018.

[19] B. Liu, C. M. Pun, "Locating splicing forgery by adaptive-SVD noise estimation and vicinity noise descriptor," *Neurocomputing*, vol. 387, pp. 172-187, April 2020.

[20] T. Bianchi, and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Secur*., vol. 7, no. 3, pp. 1003–1017, June 2012.

[21] A. C. Popescu and H. Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Trans. Signal Process*., vol. 53, no. 10, pp. 3948-3959, Oct. 2005.

[22] S. Bayram, H. T. Sencar, and N. Memon, "Classification of digital camera-models based on demosaicing artifacts," *Digit. Invest*., vol. 5, pp. 49-59, Sep. 2008.

[23] H. Cao, and A. C. Kot, "Accurate detection of demosaicing regularity for digital image forensics," *IEEE Trans. Inf. Forensics Secur*., vol. 4, no. 4, pp. 899–910, Oct. 2009.

[24] Y. Rao, J. Ni and H. Zhao, "Deep learning local descriptor for image splicing detection and localization," *IEEE Access*, vol. 8, pp. 25611-25625, Jan. 2020.

[25] Y. Liu and X. Zhao, "Constrained image splicing detection and localization with attention-aware encoder-decoder and atrous convolution," *IEEE Access*, vol. 8, pp. 6729-6741, Jan. 2020.

[26] B. Liu, and C. M. Pun, "Exposing splicing forgery in realistic scenes using deep fusion network," *Inf. Sci*., vol.526, pp. 133-150, July 2020.

[27] S. Gao, G. Xu, and R. M. Hu, "Camera model identification based on the characteristic of CFA and interpolation," in *Proc. Int. Workshop Digit. Watermarking*, Atlantic City, NJ, USA, Oct. 2011, pp. 268-280

[28] M. Kirchner, "Efficient estimation of CFA pattern configuration in digital camera images," in *Proc. SPIE Media Forensics and Security II*, vol. 7541, San Jose, California, USA, Jan. 2010, Art. no. 754111.

[29] C. H. Choi, J. H. Choi, and H. K. Lee, "CFA pattern identification of digital cameras using intermediate value counting," in *Proc. 13th ACM Multimedia Workshop Multimedia Secur*., New York, USA, Sep. 2011, pp. 21-26.

[30] J. J. Jeon, H. J. Shin, and I. K. Eom, "Estimation of Bayer CFA pattern configuration based on singular value decomposition," *EURASIP J. Image Video Process*., vol. 2017, Art. no. 47, July 2017.

[31] C. H. Choi, H. Y. Lee, and H. K. Lee, "Estimation of color modification in digital images by CFA pattern change," *Forensic Sci. Int*., vol. 226, pp. 94-105, Mar. 2013.

[32] J. J. Jeon, and I. K. Eom, "Wavelet-based color modification detection based on variance ratio," *EURASIP J. Image Video Process*., vol. 2018, Art. no. 47, June 2018.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3091161, IEEE Access

[33] A. C. Gallagher and T. Chen, "Image authentication by detecting traces of demosaicing," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Anchorage, AK, USA, Jun. 2008, pp. 1-8.

[34] Y. Huang, and Y. Long, "Demosaicking recognition with applications in digital photo authentication based on a quadratic pixel correlation model," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit*., Anchorage, AK, USA, Jun. 2008, pp. 1-8.

[35] A. E. Dirik and N. Memon, "Image tamper detection based on demosaicing artifacts," in Proc. *16th IEEE Int. Conf. Image Process*., Cairo, Egypt, Nov. 2009, pp. 1497-1500.

[36] P. Ferrara, T. Bianchi, A. D. Rosa, and A. Piva, "Image forgery localization via fine-grained analysis of CFA artifacts," *IEEE Trans. Inf. Forensics Secur*., vol. 7, no. 5, pp. 1566-1577, Oct. 2012.

[37] A. Singh, G. Singh, and K. Singh, "A Markov based image forgery detection approach by analyzing CFA artifacts," *Multimedia Tools Appl.*, vol. 77, pp. 28949-28968, Nov. 2018.

[38] E. G. Fernández, A. L. S. Orozco, L. J. G. Villalba, and J. Hernandez-Castro, "Digital image tamper detection technique based on spectrum analysis of CFA artifacts," *Sensors*, vol. 18, no. 9, 2804, Aug. 2018.

[39] N. Le, and F. Retraint, "An improved algorithm for digital image authentication and forgery localization using demosaicing artifacts," *IEEE Access*, vol. 7, pp. 125038-125053, Sep. 2019.

[40] G. Singh, and K. Singh, "Digital image forensic approach based on the second-order statistical analysis of CFA artifacts," *Forensic Sci. Int.: Digit. Invest*., vol. 32, 200899, Mar. 2020.

[41] K. Hirakawa and T. W. Parks, "Adaptive homogeneity-directed demosaicing algorithm," *IEEE Trans. Image Process*., vol. 14, no. 3, pp. 360-369, March 2005.

[42] E. Chang, S. Cheung, and D. Y. Pan, "Color filter array recovery using a threshold-based variable number of gradients," in *Proc. SPIE, Sensors, Cameras, and Applications for Digital Photography*, San Jose, CA, USA, Mar. 1999, pp. 36–43.

[43] DCB demosaicing algorithm. Accessed: Mar. 26, 2021. [Online] Available: http://www.rawtherapee.com/.

[44] IGV demosaicing algorithm. Accessed: Mar. 26, 2021. [Online] Available: http://www.rawtherapee.com/.

[45] C. Tsai and K. Song, "Heterogeneity-projection hard-decision color interpolation using spectral-spatial correlation," *IEEE Trans. Image Process*., vol. 16, no. 1, pp. 78-91, Jan. 2007.

[46] T. T. Ng and S. F. Chang, "A dataset of authentic and spliced image blocks," *Technical Report 203–2004*, Columbia University, 2004. Accessed: Apr. 28, 2021. [Online] Available: https://www.ee.columbia.edu/ln/dvmm/downloads/authsplcuncmp/.

[47] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou "An evaluation of popular copy-move forgery detection approaches," *IEEE Trans. Inf. Forensics Secur*., vol. 7, no. 6, pp. 1841-1854, Dec. 2012. Accessed: Apr. 28, 2021. [Online] Available: https://www5.cs.fau.de/research/data/image-manipulation/.

[48] P. Korus and J. Huang, "Multi-scale analysis strategies in PRNU-based tampering localization, *IEEE Trans. Inf. Forensics Secur*., vol. 12, no. 4, pp. 809-824, Apr. 2016. Accessed: Apr. 28, 2021. [Online]. Available: https://pkorus.pl/downloads/dataset-realistic-tampering/.

[49] Source code for the proposed method: Accessed: Apr. 28, 2021. [Online] Available: https://sites.google.com/view/ispl-pnu/.

[50] A. P. Bradley, "The use of the area under the ROC curve in the evaluation of machine learning algorithms," *Pattern Recog*., vol. 30, no. 7, pp. 1145-1159, July 1997.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/