Hindawi
Security and Communication Networks
Volume 2021, Article ID 4270776, 10 pages
https://doi.org/10.1155/2021/4270776

Research Article

Image Splicing-Based Forgery Detection Using Discrete Wavelet Transform and Edge Weighted Local Binary Patterns

Muhammad Hameed Siddiqi,[1] **Khurshed Asghar**,[2] **Umar Draz**,[3,4] **Amjad Ali**,[3] **Madallah Alruwaili**,[1] **Yousef Alhwaiti**,[1] **Saad Alanazi**,[1] **and M. M. Kamruzzaman**[1]

[1]*College of Computer and Information Sciences, Jouf University, Sakaka, Al-Jouf 2014, Saudi Arabia*
[2]*Department of Computer Science, University of Okara, Okara, Pakistan*
[3]*Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Islamabad, Pakistan*
[4]*Department of Computer Science, University of Sahiwal, Sahiwal, Pakistan*

Correspondence should be addressed to Umar Draz; sheikhumar520@gmail.com

Received 25 June 2021; Accepted 8 September 2021; Published 30 September 2021

Academic Editor: Usman Habib

With the advancement of the multimedia technology, the extensive accessibility of image editing applications makes it easier to tamper the contents of digital images. Furthermore, the distribution of digital images over the open channel using information and communication technology (ICT) makes it more vulnerable to forgery. The vulnerabilities in telecommunication infrastructure open the doors for intruders to introduce deceiving changes in image data, which is hard to detect. The forged images can create severe social and legal troubles if altered with malicious purpose. Image forgery detection necessitates the development of sophisticated techniques that can efficiently detect the alterations in the digital image. Splicing forgery is commonly used to conceal the reality in images. Splicing introduces high contrast in the corners, smooth regions, and edges. We proposed a novel image forgery detection technique based on image splicing using Discrete Wavelet Transform and histograms of discriminative robust local binary patterns. First, a given color image is transformed in YCbCr color space and then Discrete Wavelet Transform (DWT) is applied on Cb and Cr components of the digital image. Texture variation in each subband of DWT is described using the dominant rotated local binary patterns (DRLBP). The DRLBP from each subband are concatenated to produce the final feature vector. Finally, a support vector machine is used to develop image forgery detection model. The performance and generalization of the proposed technique were evaluated on publicly available benchmark datasets. The proposed technique outperformed the state-of-the-art forgery detection techniques with 98.95% detection accuracy.

1. Introduction

Digital imaging is applicable in many fields such as World Wide Web (WWW), print media, insurance industry, and surveillance security [1]. All these applications leverage information and communication technology (ICT) to disseminate the digital contents including digital images [2]. The vulnerabilities in telecommunication infrastructure open the doors for intruders to access or change the transmitted data. The change in image data is hard to detect because contents of an image can be easily manipulated with the help of sophisticated image editing tools. The society is facing problems like false propaganda, fraud, counterfeiting, black mailing, etc., due to image tampering. Image authentication is required to use images as source of information or evidence in real life. In most of the cases, especially with malicious designs, image forgery is performed using copy-move and splicing procedures. During forgery process, images can be altered with the help of the same image contents or by combining contents of different images. If the tampering procedure involves the copy and paste operation of image content/s within the image, then this forgery is called copy-move; otherwise, it is referred to as splicing. Different types of postprocessing operations such as scaling, blurring, noise adding, compression, and rotation are applied on the forged regions to hide the cues of forgery [3].

Forensic analysis of images was initiated in 2000. Many techniques [4–8] were developed to detect splicing forgery and can be categorized as active and passive (or blind) on the basis of splicing detection mechanism. Active techniques work on the phenomena that given image contains the information such as watermark or signature at the time of acquisition to ensure its authenticity. Active techniques extract this watermark or signature with the original to ensure its authenticity. The use of these techniques is very limited due the nonavailability of information about the watermark or signature in most of the cases. Due to this limitation passive techniques for splicing forgery detection are being developed, which do not depend on prior information. In image splicing the contents of host images are modified by copying and pasting the contents from other images. Splicing is a fundamental and famous image forgery technique. To gain the public trust in digital image authentication, image splicing detection has become an important research area for digital image forgery detection. The image splicing operation disturbs the contents consistency, smoothness, and regularity. These factors play a very important role in detecting the forgery regions in the host image. The state-of-the-art image splicing techniques consider the variations in global statistical characteristics introduced by sudden inconsistency in spliced images [6–9]. Example of splicing image forgery is shown in Figure 1.

To detect the discontinuities that occurred in image due to splicing, first a given image is partitioned into subbands using DWT. The strong decorrelation ability of DWT represents the coefficients of four wavelet subbands at the same level. Our proposed technique measures the discontinuities that occurred in images due to splicing using the DWT subbands coefficients. The proposed scheme uses a robust technique for coding, which encodes the DWT subbands coefficients. Based on the proposed scheme which measures discontinuities and their coding, we introduce a new technique to detect splicing forgery by decomposing chroma components of a test image using DWT into subbands for measuring local discontinuities. For coding, we applied the DRLBP to determine the local discontinuities. We call the descriptor based on these methods as the DWT-DRLBP, which represents an image and is used for detecting splicing forgery as shown in Figure 2. Finally, the SVM is used to detect the image forgery in digital images.

2. Related Work

Most of the splicing forgery detection techniques are blind/passive [7]. Alahmadi et al. [9] and Min and Dong [10] used DCT coefficients and minimum and maximum filters to extract features from image blocks to detect splicing forgery. Multiresolution approaches, like DWT, are used in many algorithms [5, 11]. SIFT features are used as an alternative to block matching for detecting splicing forgery [12]. Most of the splicing forgery detection methods are evaluated on Columbia Color DVMM [13] and CASIA v1.0 and CASIA v2.0 [14] datasets. Ng et al. [15] proposed image splicing detection approach based on 3D moments of image spectrum, while features based on camera response function were passed to SVM in [16] to detect splicing forgery. Shi et al. [17] used 1D and 2D moments, Markov chain probabilities, and DCT coefficients for image splicing detection. The algorithm was evaluated on CASIA v2.0 dataset and reported accuracy is 84.86%. Xunyu et al. [5] enhanced the accuracy to 89.76% of Wang et al. method by concatenating Markov chain moments and DCT and DWT coefficients together with SVM. Markov probabilities were extracted from Cb channel in [18], for image splicing detection. The algorithm achieved 89.23% and 95.5% accuracy, respectively, when evaluated on Columbia Color DVMM and a subset of CASIA v2.0 datasets. Zaho et al. in [19] designed a chrominance channel to detect splicing forgery and improved the performance of the Wang et al. scheme proposed in [18].

With the recent development in ubiquitous computing and digital media, especially digital images, the image forgery detection has become most essential task for secure and authentic multimedia contents transmission. Alahmadi et al. [20] used DCT and LBP features for image splicing detection. Pham et al. [21] extracted Markov features to identify irregularities in images due to splicing. SVM was used for classification. Jalab et al. [22] extracted fractional entropy from DWT [23] coefficients and SVM was used for classification. Xunyu in [5] developed an efficient technique to detect the duplicate regions from forged image. The proposed technique detects the *key points* using geometric transforms to find the identical transformed regions. Similarly, Mahmoud and Hongli in [6] developed a two-level key point detection technique to highlight the image tampering effects in smooth regions. At first level the combination of scale invariant feature operator and Harris corner detector was applied to detect the key point features from smooth regions. Finally, the gradient histogram of multisupport region order descriptor was computed to efficiently detect the tampers regions in a forged image.

Min and Dong in [10] developed a novel forgery detection technique based on minimum and maximum filter. The combination of minimum filter and maximum filter highlights the pixel wise minimum and maximum variations between authentic and forged images. The investigation of interpolation and noninterpolation improved the performance of forgery detection technique in composite regions. Recently, Jinwei et al. in [11] proposed a novel deep learning technique for image splicing detection. The proposed convolutional neural network learns the weighted combination of three types of featured extraction techniques. Convolutional neural network model learns the optimal combination of parameters for feature extraction techniques. Figure 3 demonstrates that sample image is transformed to YCbCr color space, where Cb and Cr are the chroma components and Y is the luminance component. Actually, the contents of image are described by luminance channel, which is capable of hiding the content tampering traces.

In [24], authors proposed a solution to localize image splicing using Multitask Fully Convolutional Network (MFCN). The proposed scheme achieves better performance than the single task FCN scheme. In the proposed scheme, authors used FCN VGG-16 with skip connection as the base

(a) (b)

Figure 1: (a) Original image and (b) spliced image.

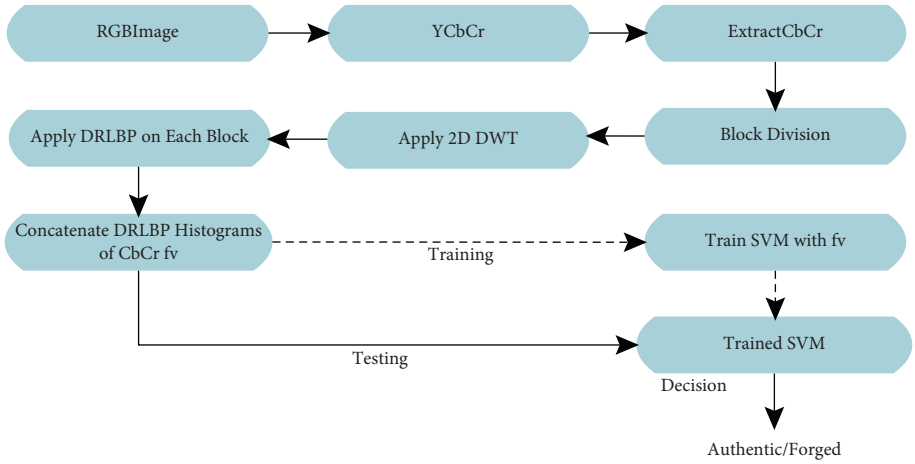

Figure 2: Proposed splicing image forgery detection approach.

Figure 3: YCbCr components of an RGB image.

network, in order to improve the learning way of CNN through recall and consolidation mechanism of human brain. Bi et al. in [25] proposed a CNN-based method called Ringed Residual U-Net (RRU-Net). The proposed scheme is end-to-end image segmentation network for image splicing detection. In this scheme, residual propagation is used to recall the input feature information to solve the degradation problem in the deeper network. The RRU-Net was tested on CASIA and Columbia datasets which were also used by Wang et al. in [26] to detect and locate image forgeries. In order to detect copy-move forgery, a two-branch DNN based architecture called BusterNet is proposed in [27]. In the proposed scheme, one layer is used for the detection of cloned regions which takes input image and uses CNN to extract features, self-correlation module to compute feature similarity, percentile pooling to collect useful statistics, mask decoder for upsampling of feature map, and binary classifier to generate binary copy-move mask, while the other layer is used for detection of tampered regions which takes input image, extracts features using CNN, upsamples feature map using mask decoder, and generates mask using binary classifier.

3. Proposed Image Forgery Detection Scheme Using the DWT-DRLBP Descriptor

In this section, we will discuss our proposed image forgery detection scheme using the DWT and the DRLBP descriptors. Splicing distorts the texture patterns that define the sharp changes such as corners, lines, and edges. Such inconsistencies in image texture can be easily detected with chroma components, because the chroma components describe the weak signals (corners, lines, and edges) [7, 18, 19]. Splicing highlights the discontinuities in the form of edges in images which change the local structure of spliced images and are well exposed using DWT coefficients, because the changes that occurred due to splicing are present in high frequency wavelet bands. To analyze these changes we propose an efficient, simple, and robust descriptor, called DWT-DRLBP descriptor, which first decomposes chroma components of a given image into subbands using Discrete Wavelet Transform (DWT) and then encodes these subbands using DRLBP [28] texture descriptor, which is a robust texture descriptor. The DWT-DRLBP descriptor of an image is passed to SVM for taking the decision whether it is authentic or spliced. We applied SVM two-class classifier to classify a sample image as forged or authentic [29]. Support vector machine is linear classifier, but the samples of image forgery dataset used in this research are not linearly separable. To overcome this issue a kernel trick is applied. The experiments were performed using LIBSVM kernel as presented in [30].

3.1. DWT-DRLBP Descriptor. Discrete wavelet transformation decomposed the sample image into four frequency bands (LL, LH, HL, and HH]. These frequency bands are called chroma components, which highlights the local inconsistencies in the forged. The proposed image splicing technique is the combination of DWT based chroma components and DRLBP features. For this purpose, first one-level DWT was applied in the image and then DRLBP descriptor was applied to highlight the splicing effects.

3.2. Wavelet Decomposition of Chroma Components. The DWT provides unique and discriminatory representation to quantify image texture efficiently with high resolution and few numbers of wavelet coefficients. The wavelet coefficients effectively highlight the structural variations in image splicing. The low frequency coefficients provide high contrast that occurs due to image splicing. The low frequency features are directly used to represent the sample image. Due to describing energy compaction in few wavelet coefficients, the procedure of image representation becomes very simple.

The low frequency components image approximations are done by highlighting the inconsistencies introduced in the forged image. The low frequency is the most suitable for localization of variations in image contents as illustrated in Figure 4. The introduction of wavelet transformation in image splicing detection allows analyzing the image at frequency domain with the help of low-pass filter and high-pass filter. The splicing forgery produces high contrast in terms of corners, edges, and lines, which are better described with high frequency. The wavelet transformation describes these transitions with the help of local sharpness and smoothness in high frequency coefficients. Based on these assumptions, each chroma channel of a given image is partitioned into four frequency bands (LL, LH, HL, and HH) using 1-level wavelet transform to characterize the changes that occurred due to splicing (see Figure 5).

3.3. DRLBP Histograms. After extracting the chroma channels from sample image, the next step is to extract the discriminate patterns and estimate their distribution. For this purpose, we adopt DRLBP descriptor, which extracts the histogram of local binary patterns such as edges, corners, spots, and lines in the form of LBP codes. Then we approximate the distribution of these patterns while considering the local gradient magnitude at subsequent locations. DRLBP descriptor highlights the changes in local regions while considering the amount of change. The overview of DRLBP descriptor is given in equations (1) to (4), whereas the detailed description of DRLBP is presented in [19]. The binary patterns of each pixel from a 3×3 window with 8 neighbors are computed from sample image; then the weighted histogram of binary patterns is computed from each region as defined in equation (3).

$$W_{\mathrm{LBP}}(i) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} G_{x,y}\,\delta\left(\mathrm{LBP}_{x,y}, i\right),$$
$$\delta(j,i) = \begin{cases} 1, & j = i, \\ 0, 0 \text{ otherwise.} \end{cases} \tag{1}$$

Here $n = 2^8$ the number of bins to represent the sample image in the form of histograms of 256 distinct patterns. $G_{x,y}$ is the gradient magnitude of central pixel (x, y) which demonstrates the contribution of the corresponding binary pattern with respect to the intensity of pixel wise local change. $M \times N$ represents resolution of each specific frequency band. To eliminate the reverse effect both in background and in foreground, we computed the weighted histogram W_{RLBP} as follows:

$$W_{\mathrm{RLBP}}(i) = W_{\mathrm{LBP}}(i) + \left(2^8 - 1 - i, 0 \le i \le 2^7\right). \tag{2}$$

After calculating the RLBP, the histogram of weighted discriminative LBP was computed to enhance the discriminative effect of binary patterns as follows:

$$W_{\mathrm{DLBP}}(i) = \left|W_{LBP} - (i)WLBP\left(2^8 - 1 - i\right)\right|, \quad 0 \le i \le 2^7. \tag{3}$$

Finally, DRLBP descriptor is computed by concatenating the histogram of weighted RLBP and weighted DLBP of each local region as follows:

$$\mathrm{DRLBP} = \left[W_{\mathrm{RLBP}}, W_{\mathrm{DLBP}}\right]. \tag{4}$$

3.4. Computation of the DWT-DRLBP Descriptor. After computing the local DRLBP patterns of each channel $Ch \in \{Cb, Cr\}$ from all subbands $sb \in \{\mathrm{LL}, \mathrm{LH}, \mathrm{HL}, \mathrm{HH}\}$,

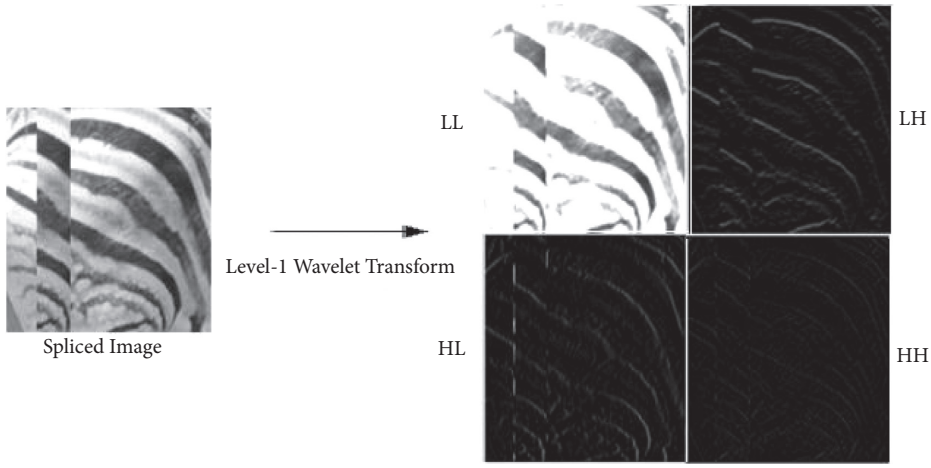

Figure 4: Decomposition of a given image into LL, LH, HL, and HH subbands using single level 2D DWT.

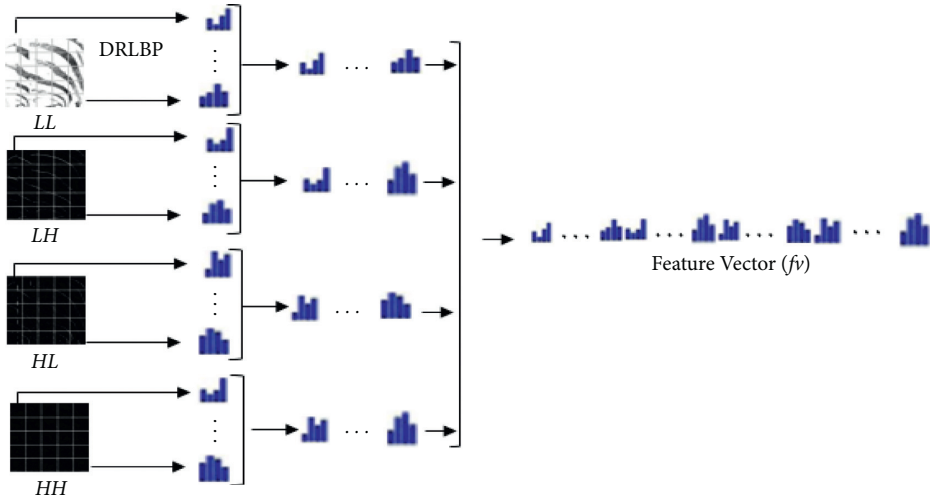

Figure 5: Encoding of spatially localized changes that occurred due to splicing using the DWT-DRLBP descriptor.

the histogram of all subbands is concatenated to form the DRLBP descriptor (fv). The whole process of the computation of fv is given in Algorithm 1. The descriptor fv computes the overall structural changes without considering the spatial locations of image contents. The integration of the discriminative information and localized spatial changes into fv further enhances its discriminative potential. For this purpose, each channel of sample image is partitioned into K blocks (subblocks), $B_1, B_2, \ldots, B_K$, each subblock with $l \times m$ dimension such that $K(l \times m) = M \times N$. The descriptor fvB_i of each subblock B_i is computed.

At the end, the fvB_i of all subblocks is concatenated to represent the fv^{Ch} of a channel with respect to each subband $Sb \in \{\text{LL}, \text{LH}, \text{HL}, \text{HH}\}$ as represented in equation (6). Finally, the DWT-DRLBP descriptor is obtained to represent the sample image as described in

$$fv^{ch} = \left[fv^{\text{LL}}, fv^{\text{LH}}, fv^{\text{HL}}, fv^{\text{HH}}\right], \tag{5}$$

$$fv = \left[fv^{Cb}, fv^{Cr}\right]. \tag{6}$$

4. Performance Measures and Evaluation Methodology

To evaluate the performance of proposed image forgery detection technique three image databases were used. The performance evaluation techniques and datasets are described in this section.

4.1. Dataset Description. The performance of image forgery technique was evaluated using three datasets Columbia Color DVMM (DVMM) [11] and CASIA v1.0 and CASIA v2.0 benchmark datasets available publicly. Initially, we performed experiments on DVMM to evaluate the proposed method. CASIA v1.0 and CASIA v2.0 datasets were then used for further experiments and evaluation. DVMM dataset contains 183 authentic and 180 tampered images in TIFF format. The CASIA v1.0 dataset comprises 800 authentic and 921 spliced images. All tampered images are postprocessed using different geometric transformations. The CASIA v2.0 dataset contains 7,491 authentic and 5,123 forged images. We also evaluated the performance of proposed technique

on the combined dataset (the collection of abovementioned three datasets) to represent the generalization of proposed image forgery detection technique.

4.2. Evaluation Policy. The parameters of SVM were tuned with respect the training dataset. We achieved the best performance with RBF kernel. The RBF filter depends on further two parameters which are *regularized coefficient* and *gamma*. The performance of RBF filter entirely depends on the optimal combination of these two parameters. The *regularized coefficient* performs an important role in balancing the complexity of the model by achieving highest forgery detection accuracy, whereas the *gamma* parameter in RBF kernel is used to define the nonlinear mapping between two points; in case of lower *gamma* value the far away points are considered as closest points. For image splicing detection we tuned the RBF kernel with 2^5 and 2^{-5} for regularized coefficient and gamma, respectively, using grid-search method [31, 32]. We employed 10-fold cross validation in which the forged and authentic images are randomly divided into 10 folds of equal size. Ten performance measure values corresponding to the 10-folds are calculated and their average along with standard deviation (*std*) is reported as the performance of the system. The same procedure is repeated for each dataset.

4.3. Performance Measures. For evaluation, the forged images are considered as positive class while the authentic images are considered as negative class. We adopted the following performance evaluation techniques: accuracy, sensitivity, specificity, and false positive rate. Accuracy is the percentage of samples accurately predicted as forged or authentic to the total number test images, computed as follows:

$$\mathrm{ACC} = \frac{(\mathrm{TP} + \mathrm{TN})}{\mathrm{TP} + \mathrm{TN} + \mathrm{FN} + \mathrm{FP}} \times 100\%. \tag{7}$$

Here the symbol *TP* characterizes the number of samples that are forged, and the classifier also predicted them as forged. The symbol *TN* represents the number of images that are authentic, and the classifier also predicted them as authentic. Moreover, the symbol *FP* represents the number of images that were authentic and classifier predicted them as forged, and FN represents the number of images that were forged and the classifier predicted them as authentic.

True Positive Rate. The true positive rate is also called sensitivity, which represents the percentage of predicting a forged image as forged, calculated as

$$\begin{aligned}\mathrm{TPR} &= \mathrm{SN} \\ &= \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \times 100.\end{aligned} \tag{8}$$

True Negative Rate. The true negative rate is also called specificity, which represents the percentage of predicting a genuine image as genuine, computed as

$$\begin{aligned}\mathrm{TNR} &= \mathrm{SP} \\ &= \frac{\mathrm{TN}}{\mathrm{TN} + \mathrm{FP}} \times 100.\end{aligned} \tag{9}$$

False Positive Rate. The false positive rate represents the percentage of predicting the sample images as forged which are actually misclassified as authentic.

$$\mathrm{FPR} = (1 - \mathrm{TNR}) \times 100\%. \tag{10}$$

Parameter Tuning. The proposed system involves many parameters. Figure 5 illustrates the participating parameters. Tuning the parameters in a thorough manner to find the optimal set is not an easy task, which is considered as an optimization problem. From a practical point of view parameter setting is important. We determined empirically various parameter settings in this paper. After parameters tuning, the best parameters values used by proposed method are shown in Table 1.

5. Experimental Results and Discussion

The performance of proposed method on different benchmark datasets is given in Table 2. The ROC curves are shown in Figure 6. To evaluate the performance of image splicing techniques developed in this research, we applied the proposed technique on DVMM dataset. The DVMM dataset contains 180 normal images and 183 forged color images. The forged images are produced by tampering the authentic images by applying the crop-paste method of the vertical and horizontal strips.

5.1. Robustness on Geometric Transformations. Geometric transformations such as scaling (resizing), rotation, and deforming are applied normally in combination or individually on spliced regions to hide the cues of forgery. These transformations are applied on spliced region(s) in CASIA v1.0 and CASIA v2.0 datasets. Figure 7 shows the accuracy of the method against these transformations. When geometric transformations are applied on spliced region(s), the changes along the boundary turn into sharp edges (splicing artifacts), which are needed to be modeled properly. In general, the method performs well with respect to different geometric transformation, because splicing artifacts are modeled properly by DWT-DRLBP descriptor.

5.2. Robustness on Spliced Region(s) Size. Splicing regions are detected by exploring variations of intrinsic features, which are usually consistent in unaltered images. The method is explored on small, medium, and large spliced region(s). Figure 8 shows the results with these sizes. It is fact that local inconsistencies of spliced region(s) are useful in exposing forgery, which is exposed effectively using DTW-DRLBP descriptor.

(1) RGB image I, the number K of blocks

a) Convert I to YCbCr
b) DWT-DRLBP descriptor fv

(2) for each channel $\mathbf{Ch} \in \{\mathbf{Cb}, \mathbf{Cr}\}$ of image I
(3) a) Apply 2D-DWT on Ch, Sb ∈ [LL, LH, HL, HH]
(4) end for
(5) S $\mathbf{b} = \mathbf{HH}$
(6) Divide S $\mathbf{b}$ into $\mathbf{K}$ blocks: $\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_\mathbf{K}$
(7) for each block $\mathbf{B_k}, \mathbf{k} = 1, 2, \ldots, \mathbf{k}$
(8) Compute DRLBP histogram $\mathbf{fv_k^{sb}}$
(9) $fv^{Sb} = [fv_1^{Sb}, fv_2^{Sb}, \ldots, fv_K^{Sb}]$
(10) $fv^{Ch} = [fv^{LL}, fv^{LH}, fv^{HL}, fv^{HH}$
(11) $fv = [fv^{Cb}, fv^{Cr}]$
(12) end for

Algorithm 1: Computation of DWT-DRLBP.

Table 1: The optimal parameters set of the proposed method.

Preprocessing	Color channel/s Block division	Cb and Cr Nonoverlapped
DRLBP	P	8
	R	1
	Mapping type	$u2$
Classification	SVM kernel	RBF

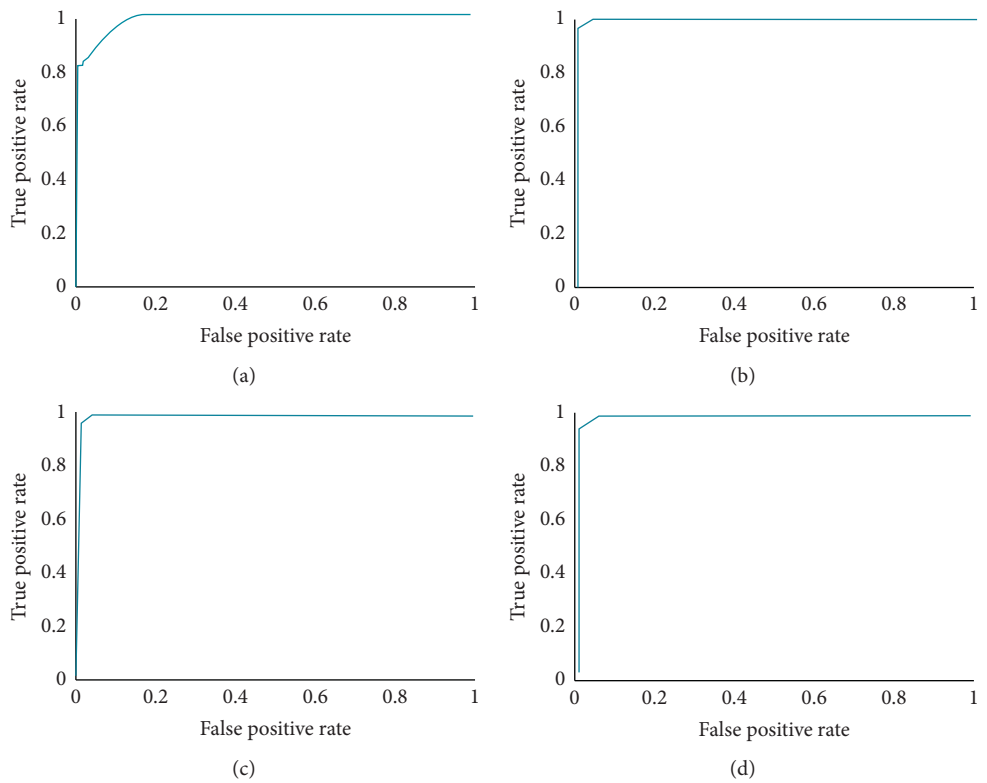

Figure 6: ROC curves on datasets: (a) DVMM, (b) CASIA v1.0, (c) CASIA v2.0, and (d) combined.

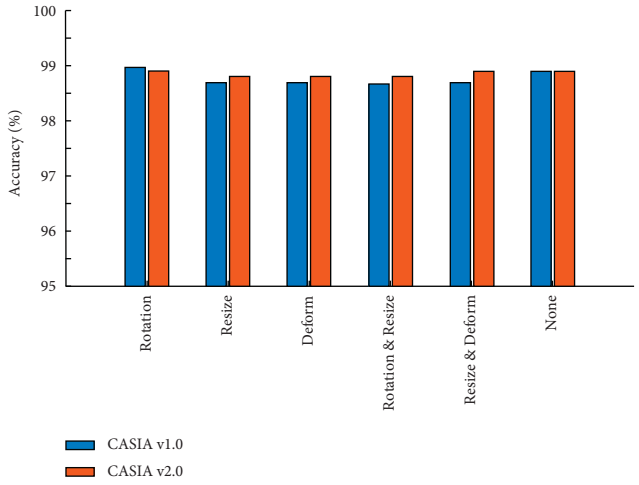

Figure 7: The proposed method accuracy on geometric transformations.

5.3. Robustness on Spliced Region(s) Shape. Splicing of different types of shapes is very common to gain illegal benefits. This section explores the effect of spliced region shapes on the performance. CASIA v1.0 and CASIA v2.0 datasets contain the four region shapes of the spliced part(s) that are circular (CR), rectangular (RECT), triangular (TRI), and arbitrary (ARB). Figure 8 shows the results with theses shapes. The method is robust on different shapes of spliced region(s).

5.4. Robustness on JPEG Images. The performance of proposed technique was evaluated on the JPEG images taken from CASIA v1.0 and CASIA v2.0 datasets and achieved 98% accuracy. JPEG compression is performed by applying DCT quantization. When splicing is performed in JPEG images the forgery occurs in the form of block mismatching and blocks are not aligned with their neighbors which causes extraneous edges. The proposed techniques achieved high forgery detection accuracy because it properly explored the inconsistencies in the spliced image using DWT-DRLBP descriptor.

5.5. Comparison with State-of-the-Art Methods. In this section we compared the results achieved in this research with the state-of-the-art image splicing technique for image forgery detection. Table 3 demonstrates the performance of state-of-the-art methods only on the corresponding datasets, because they achieved best results either on CASIA v1.0 or CASIA v2.0 or DVMM. It demonstrates that the proposed technique outperforms the state-of-the-art techniques with respect to every performance evaluation criterion. It can also be noted that the proposed approach performed significantly on combined dataset, which witnessed the generalization of the proposed technique. Overall, the method has high accuracy and true positive rate, while maintaining low false positive rate as compared to other state-of-the-art methods.

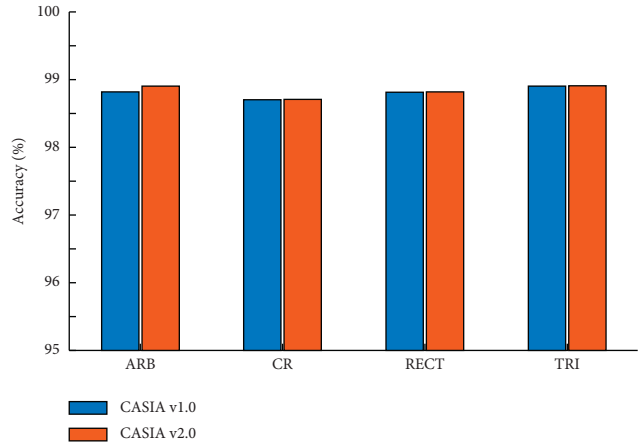

Figure 8: The proposed method accuracy on spliced region(s) shape.

Table 2: Performance of image forgery detection.

Dataset used	*ACC*	*TPR*	*FPR*	*AUC*
DVMM	97.21	97.87	3.88	0.98
CASIA v1.0	98.59	99.34	1.24	0.99
CASIA v2.0	98.88	99.32	0.96	0.99
Combined	98.95	99.91	2.05	0.99

Table 3: Comparison with recent state-of-the-art image splicing detection methods.

Approaches	Dataset used	*ACC*	*TPR*	*FPR*	*AUC*
Proposed	DVMM	97.21	97.87	3.88	0.98
	CASIA v1.0	98.59	99.34	1.24	0.99
	CASIA v2.0	98.33	97.32	0.96	0.99
	Combined	98.95	99.91	2.05	0.99
[5]	DVMM	96.39	97.92	4.46	0.97
	CASIA v1.0	94.89	92.30	2.77	0.94
	CASIA v2.0	97.33	98.50	3.47	0.97
[31]	DVMM	91.14	93.07	16.14	—
	CASIA v1.0	96.17	97.65	6.84	—
	CASIA v2.0	97.86	98.82	2.79	—
[32]	Composite	93.21	—	—	—
[6]	CASIA v1.0	90.18	93.00	2.11	—
	CASIA v2.0	96.21	93.00	2.90	—
	Composite	94.64	93.00	7.20	—
[33]	CISE	93.36	92.99	1.89	—
[34]	CASIA v1.0	94.29	—	—	0.93
	CASIA v2.0	96.52	—	—	0.97
	DVMM	94.17	—	—	0.93
[18]	CASIA v1.0	95.4	—	—	—
	CASIA v2.0	95.6	—	—	—
	DVMM	94.8	—	—	—
[19]	CASIA v1.0	95.4	—	—	—
	CASIA v2.0	95.6	—	—	—
	DVMM	94.8	—	—	—
[35]	CASIA v2.0				
[20]	CASIA v2.0	99.54	95		

6. Conclusion

To represent a test image for authentication, we employed DWT-DRLBP descriptor for feature extraction. Chroma components of a test image are decomposed into subbands

using single level DWT to exploit splicing inconsistencies. A robust texture descriptor DRLBP is employed to capture the detailed statistics from these subbands. DWT-DRLBP descriptor makes the proposed method capable enough to detect splicing image forgery even in the presence of postprocessing operations. Performance of DWT-DRLBP descriptor is obtained and examined by employing SVM classifier with 10-fold cross validation. Three publicly available benchmark datasets were used for experiments and evaluation. Our proposed method achieved 98.95% accuracy on combined dataset and is robust as compared to other state-of-the-art methods. These results also endorsed the success and robustness of DWT-DRLBP descriptor, used to model inconsistencies in images caused by splicing forgery. Furthermore, SVM with RBF kernel classified any given image as authentic or spliced and finally ensured the excellent accuracy of results. The future work is to localize the spliced region(s) to boost the trust on results and to measure the degree of splicing.

Data Availability

Data used for this study and simulation will be provided upon request to the reviewer for validation.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the present study.

Acknowledgments

The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia, for funding this work through Project no. "375213500." Also, the authors would like to extend their sincere appreciation to the central laboratory at Jouf University for supporting this study.

References

[1] M. K. Abdolmaleki, M. S. Riasi, M. Enayati et al., "A digital imaging method for evaluating the kinetics of vapochromic response," *Talanta*, vol. 209, Article ID 120520, 2020.

[2] N. L. Iacobici, M. I. Frigura, H. E. Filipescu, M. Nen, F. M. I. Frigura, and M. Iorga, "Digital imaging processing and reconstruction for general applications," in *Proceedings Of the IEEE 18th World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pp. 231–234, Herl'any, Slovakia, January 2020.

[3] A. Khurshid, H. Zulfiqar, and H. Muhammad, "Copy-move and splicing image forgery detection and localization techniques: a review," *Australian Journal of Forensic Sciences*, vol. 49, no. 3, pp. 281–307, 2017.

[4] X. Zhao, J. Li, S. Li, and S. Wang, "Detecting digital image splicing in chroma spaces," in *Proceedings of the International workshop on digital watermarking*, pp. 12–22, Berlin, Germany, October 2010.

[5] P. Xunyu, "Digital image forensics with statistical analysis," *Handbook Of Digital Forensics of Multimedia Data and Devices*, John Wiley & Sons, NJ, USA, 2015.

[6] E. Mahmoud and Z. Hongli, "Two-stage keypoint detection scheme for region duplication forgery detection in digital images," *Journal of Forensic Sciences*, vol. 63, no. 1, pp. 102–111, 2018.

[7] G. Muhammad, M. H. A. Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," *Machine Vision and Applications*, vol. 25, no. 4, pp. 985–995, 2014.

[8] J. Goh and V. L. L. Thing, "A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection," *International Journal of Electronic Security and Digital Forensics*, vol. 7, no. 1, pp. 76–104, 2015.

[9] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," in *Proceedings of the IEEE Global Conference on Signal and Information Processing*, pp. 253–256, Austin, TX, USA, September 2013.

[10] G. H. Min and H. H. Dong, "Identification method for digital image forgery and filtering region through interpolation," *Journal of Forensic Sciences*, vol. 59, no. 5, pp. 1372–1385, 2014.

[11] W. Jinwei, N. Qiye, L. Guangjie, L. Xiangyang, and K. J. Sunil, "Image splicing detection based on convolutional neural network with weight combination strategy," *Journal Information Security and Applications*, vol. 54, pp. 1–8, 2020.

[12] A. Costanzo, I. Amerini, R. Caldelli, and M. Barni, "Forensic analysis of SIFT keypoint removal and injection," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 9, pp. 1450–1464, 2014.

[13] T. T. Ng, S. F. Chang, and Q. Sun, "A Data Set of Authentic and Spliced Image Blocks," *ADVENT Technical Report #203-2004-3*, pp. 6–9, Columbia University, NY, USA, 2004.

[14] J. Dong and W. Wang, "CASIA image tampering detection evaluation databases," in *Proceedings of the Signal and Information Processing*, pp. 422–426, Beijing, China, 2015.

[15] T. T. Ng, S. F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," in *Proceedings of the international symposium on circuits and systems*, pp. 688–691.

[16] F. Hsu and S. Chang, "Detecting image splicing using geometry invariants and camera characteristics consistency," in *Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 549–552, Toronto, ON, Canada, 2006.

[17] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection," in *Proceedings of the 9th ACM Workshop on Multimedia & Security*, pp. 51–62.

[18] W. Wang, J. Dong, and T. Tan, "Image tampering detection based on stationary distribution of Markov chain," in *Proceedings of the 17th IEEE international conference on image processing*, pp. 2101–2104, Hong Kong, China, December 2010.

[19] X. Zhao, S. Li, S. Wang, J. Li, and K. Yang, "Optimal chroma-like channel design for passive color image splicing detection," *EURASIP Journal on Applied Signal Processing*, vol. 2012, pp. 1–11, 2012.

[20] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," *Signal, Image and Video Processing*, vol. 11, no. 1, pp. 81–88, 2017.

[21] N. T. Pham, J. Lee, G. Kwon, and C. Park, "Efficient image splicing detection algorithm based on markov features," *Multimedia Tools and Applications*, vol. 78, no. 9, Article ID 12405, 2019.

[22] H. Jalab, T. Subramaniam, R. Ibrahim, H. Kahtan, and N. Noor, "New texture descriptor based on modified fractional entropy for digital image splicing forgery detection," *Entropy*, vol. 21, no. 4, pp. 371–385, 2019.

[23] R. C. Gonzalez and R. E. Woods, *Digital image processing*Vol. 4, Addison-Wesley, MA, USA, 1992.

[24] R. Salloum, Y. Ren, and C.-C. Jay Kuo, "Image splicing localization using a multi-task fully convolutional network (mfcn)," *Journal of Visual Communication and Image Representation*, vol. 51, pp. 201–209, 2018.

[25] X. Bi, Y. Wei, B. Xiao, and W. Li, "Rru-net: the ringed residual u-net for image splicing forgery detection," in *Proceedings of the the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, June 2019.

[26] X. Wang, H. Wang, S. Niu, and J. Zhang, "Detection and Localization of Image Forgeries Using Improved Mask Regional Convolutional Neural Network," *Mathematical Biosciences and Engineering*, vol. 16, pp. 4581–4593, 2019.

[27] Y. Wu, W. Abd-Almageed, and P. Natarajan, "Busternet: detecting copy-move image forgery with source/target localization," in *Proceedings of the European Conference on Computer Vision (ECCV)*, pp. 168–184, Munich, Germany, September 2018.

[28] A. Satpathy, X. Xudong Jiang, and H. L. How-Lung Eng, "LBP-based edge-texture features for object recognition," *IEEE Transactions on Image Processing*, vol. 23, no. 5, pp. 1953–1964, 2014.

[29] C. Cortes and V. Vapnik, "Support-vector networks," *Machine Learning*, vol. 20, no. 3, pp. 273–297, 1995.

[30] C. C. Chang and C. J. Lin, "LIBSVM: a library for support vector machines," *ACM Transactions on Intelligent Systems and Technology*, vol. 27, no. 3, pp. 21–27, 2011.

[31] C. W. Hsu, C. C. Chang, and C. J. Lin, *A Practical Guide to Support Vector Classification*, National Taiwan University, Taipei, Taiwan, 2003.

[32] M. Sokolova, N. Japkowicz, and S. Szpakowicz, "Beyond accuracy, F-score and ROC: a family of discriminant measures for performance evaluation," in *Proceedings of the Australasian joint conference on artificial intelligence*, pp. 1015–1021, Berlin, Germany, January 2006.

[33] X. Zhao, S. Wang, S. Li, and J. Li, "Passive image-splicing detection by a 2-D noncausal Markov model," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 25, no. 2, pp. 185–199, 2014.

[34] M. Hussain, S. Qasem, G. Bebis, G. Muhammad, H. Aboalsamh, and H. Mathkour, "Evaluation of image forgery detection using multi-scale weber local descriptors," *The International Journal on Artificial Intelligence Tools*, vol. 24, no. 4, pp. 1–28, 2015.

[35] 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 Journal on Image and Video Processing*, vol. 2016, no. 1, pp. 30–39, 2016.