Multimedia Tools and Applications (2020) 79:32037–32063
https://doi.org/10.1007/s11042-020-09275-w

A passive approach for the detection of splicing forgery in digital images

Navneet Kaur[1] · Neeru Jindal[1] · Kulbir Singh[1]

Received: 9 August 2019 / Revised: 7 May 2020 / Accepted: 26 June 2020 /
Published online: 25 August 2020

Abstract

With the technology progress, a plethora of freely accessible software has questioned the authenticity of digital images. This field is continuously creating challenges for researchers to ascertain the integrity of images. Hence, there is a need to improve the performance of forgery detection algorithms from time to time. This paper is focused on the detection of splicing forgery because it is one of the most frequently used image manipulation techniques. In the proposed scheme, Markov features in both Discrete Wavelet Transform (DWT) and Local Binary Pattern (LBP) domains are extracted and combined for the detection of image splicing. Three-level DWT is applied to the source image by the means of discrete Haar wavelet. The image is split in to high and low-frequency sub-bands after applying one level DWT. Furthermore, low-frequency sub-band is decomposed twice to obtain three-level DWT, which leads to more information and less amount of noise. The efficacy of the proposed scheme has been appraised on six benchmark datasets i.e. CASIA v2.0, DVMM, IFS-TC, CASIA v1.0, Columbia, and DSO-1. Moreover, the SVM classifier is trained to classify the images as tampered or authentic. The effectiveness of the proposed scheme is evaluated based on various performance parameters such as accuracy, sensitivity, specificity, and informedness. The proposed results show improved accuracy i.e. 99.69%, 99.76%, 97.80%, 98.61%, 96.90%, and 92.50% on CASIA v1.0, CASIA v2.0, DVMM, Columbia, IFS-TC, and DSO-1, respectively, in comparison to other existing approaches.

Keywords Accuracy · Discrete wavelet transform · Local binary pattern · Markov features · Splicing forgery

✉ Kulbir Singh
ksingh@thapar.edu

Navneet Kaur
navneetbrar5@gmail.com

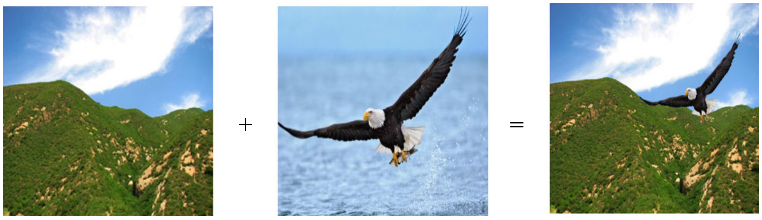
Neeru Jindal
neeru.jindal@thapar.edu

Extended author information available on the last page of the article

1 Introduction

Digital images have become an essential portion of our day-to-day life since they provide prosperous information. Due to a large number of photo-editing software such as Adobe Photoshop, GNU Image Manipulation Program (GIMP), etc., digital images can be easily manipulated for the user's interest [16]. For example, in the medical field, physicians make a diagnosis based on images. Since medical images deal with a large amount of money, these images get manipulated for claiming medical insurance [43–46]. So, it creates a necessity for advanced methods to determine the legitimacy and truthfulness of digital images used in law, military, science, medical, journalism, and other images of extreme importance. Intrusive (active) and Non-intrusive (passive) techniques are used to authenticate the images. In intrusive methods, the information is inserted into the image, for instance, digital watermark and signature. Various watermark techniques [1–4, 49] have been proposed, which are used for verifying the authenticity of the images and detection of forgery. The major shortcoming of these techniques is that it involves special software or hardware either to extract authentication information from the images or to insert authentication information into the images. Although in the past, researchers preferred digital watermarking and digital signature algorithms, however, in recent times, non-intrusive techniques have become more popular since it does not insert any secondary data into the image. Moreover, these techniques authenticate the images by examining the intrinsic properties of the images. Two common types of non-intrusive procedures are Copy-Move Forgery (CMF) as well as splicing forgery. In CMF, one portion of the image is copied, and inserted in the analogous image to obscure some significant data. In splicing forgery, one portion is removed and inserted in a different image to generate a new image [16, 29, 50]. An illustration of splicing forgery is given in Fig. 1. In splicing, to generate a forged image, regions are generally compressed, resampled, and blurred. As a result, spliced images are being used for malicious purposes, since image splicing can be performed with ease and it is difficult to detect forged images by human eyes. Thus, emerging reliable splicing detection techniques to determine the genuineness of images has become a significant issue. This motivates the researchers to introduce various procedures to detect the splicing forgery. The major idea of different image splicing detection approaches is to detect the region of irregularities with features of the image [18, 35].

Recently, several effective approaches have been introduced to upgrade the performance of splicing forgery detection. He et al. [18] fused the Markov features in a Discrete Wavelet Transform (DWT) as well as the Discrete Cosine Transform (DCT) domain. Even though the paper demonstrated the legitimacy of the Markov feature, but still needs improvement in the accuracy rate. Zhang et al. [47] introduced the forgery detection approach based on Local



(i) Authentic images (ii) Spliced image

Fig. 1 An illustration of splicing forgery

Binary Patterns (LBP) by applying multi-size block DCT (MBDCT) coefficients. In this, DCT and LBP are combined, and improved accuracy was achieved. To meet the day to day forgery challenges, there is further demand for a more accurate method. The proposed scheme aims at improving the detection accuracy rate. Zhang et al. [48] detected splicing forgery by extracting the Markov features in the Contourlet transform and DCT domain. The Contourlet transform features illustrate the dependence of positions between the Contourlet sub-band coefficients. Suthiwan et al. [41] used Markov in the Multi-Block DCT (MBDCT) domain to detect the splicing forgery and artifacts are created due to post-processing in the dataset. El-Alfy et al. [15] proposed image splicing forgery detection procedure by extracting Markov features in spatial as well as the DCT domain. Sheng et al. [36] and Zhang et al. [51] extracted Markov features in Discrete Octonion Cosine Transform (DOCT) domain and block DWT domain, respectively using an SVM classifier. Prakash et al. [34] used BDCT and the enhanced threshold for the extraction of features. These techniques cause difficulty in finding the correlation among the pixels. So, there is a need to improve correlation among the pixels to avoid the problem of degradation of image quality.

Zhao et al. [52] introduced an approach to model an image as a 2D non-casual signal. This model is applied to BDCT and discrete Meyer wavelet transform (DMWT) domain, and combined extracted features are used for classification. It is observed that this approach has a better detection rate but at the cost of the high dimensions of features. Shi et al. [37] treated the neighboring differences of BDCT coefficients of an image as a 1-D signal. The dependencies between neighboring nodes along a certain direction (horizontal or vertical) were modeled as a causal Markov model and the TPM, which was considered as a discriminative feature vector for SVM classification. Kirchner et al. [25] detected median filtering of JPEG compressed images using SPAM features and results demonstrate that it can be treated as a detector for image forgery detection. Agarwal et al. [5] extracted internal statistical properties using rotation invariant co-occurrence among LBP operator. Muhammad et al. [30] proposed an image forgery detection technique by using Steerable Pyramid Transform (SPT) along with LBP. SPT produces multi-oriented sub-bands and LBP histograms were evaluated from each sub-band, which were further concatenated to generate feature vector. Then, SVM has been used for classification. Dong et al. [13] detected splicing by extracting statistical features from image run-length and image edge statistics. Li et al. [28] introduced a technique based on Markov in quaternion DCT transform to detect the image splicing. Both intra-block and inter-block correlation have been extracted in the QDCT domain, and finally, SVM has been used to classify the authentic and spliced images. Alahmadi et al. [8] proposed a technique based on LBP and DCT to detect the forgeries present in the image. The technique converts LBP code blocks into the DCT domain, and finally, standard deviation has been evaluated and fed to the SVM classifier. Agarwal et al. [6] used the Undecimated Wavelet Transform (UWT) to highlight the details of the image and then applied the Markov process to extract the features. Hussain et al. [20] examined the effect of two texture descriptors, multi-scale LBP, and multi-scale WLD for the robust detection of splicing forgery. The experimental results show that multi-scale WLD performed superior to multi-scale LBP. Alahmadi et al. [7] applied 2D-DCT in the LBP domain to extract discriminative localized features. Kumar et al. [27] applied Markov in BDCT and DMWT domain, and enhanced threshold method. The flaw of this method is the loss of details of feature vectors because of the thresholding process. Moreover, it was shown in [27] that the detection performance was quite low, i.e. the attained highest detection accuracy was 88.43% for the DVMM dataset. Jalab et al. [21] detected splicing forgery by proposing a texture descriptor based on approximated Machado fractional entropy

(AMFE). Though it attains better results, but it is not robust to post-processing operations like JPEG compression. Kanwal et al. [23] introduced an overlapping block-based approach for the detection of image splicing forgery. This approach extracted features using Ostu based enhanced local ternary pattern (OELTP) and energy was used to reduce the dimensionality of the features. Nevertheless, this approach was not computationally effective because of the overlapping block-based approach. Several approaches for image splicing forgery detection have been proposed in the literature but still, there is a need for improvement in detection accuracy rate. The proposed approach deals with the detection of image splicing forgery with an improved accuracy rate as well as reduced running time. Moreover, it is robust against post-processing operation i.e. JPEG compression.

As discussed earlier, a lot of procedures had been proposed in the previous years by the researchers for detecting the image splicing forgery and this progression seems to be never-ending. So, it is difficult to discuss all the procedures in the paper. Thus, the trends of literature analysis in the field of image splicing forgery detection has been demonstrated in Fig. 2. Since the search strategy is a significant point of the survey process, therefore, the semantic scholar has been considered to gather the appropriate literature. It has been observed that this field is still in its progressive stage and has become a topic of interest for many researchers.

The previous approaches [22, 31, 38] has used the combination of LBP and DWT in applications like image retrieval, face recognition, object recognition. Also, in the prior work, the image splicing forgery is detected either by the fusion of LBP and DWT [24, 53] or combination of Markov and DWT [39, 51], but, according to the best knowledge of the authors, the combination of Markov, LBP, and DWT has not been yet used in any application. Thus, in the proposed method, Markov features in both DWT and LBP domains are extracted and combined to detect the image splicing forgery efficiently. Since image splicing produces sharp edges in a forged image, therefore capturing the forgery introduced artifacts is the key for image splicing detection. So, the edges introduced by forgery are different from their neighbors, the relationships among the spliced part and normal part can be used to expose image forgery. The proposed method uses Markov TPM to describe these relationships. Furthermore, DWT is used because the wavelet analysis is good in capturing the localized changes in the images that are created by splicing operation. Also, DWT has better spatial and frequency resolution than other transforms like DCT and DFT. In contrast, LBP is used as it is an effective texture operator that captures the local deviations in the texture of forged images because the original texture of the image gets distorted when manipulation is performed.

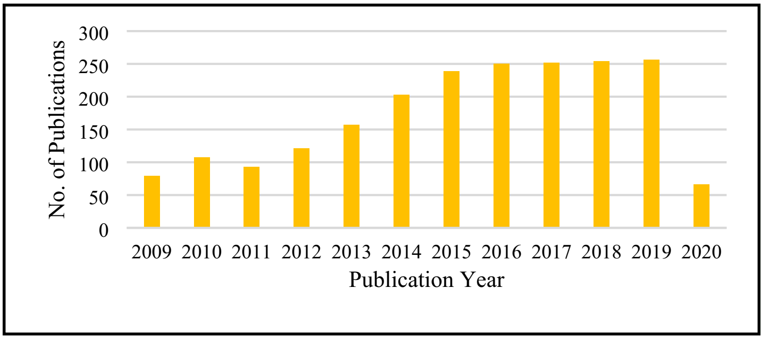


Fig. 2 Trends of literature analysis of image splicing forgery detection in the past decade

Consequently, the proposed technique based on Markov is effective in image splicing forgery detection.

The technical contributions of the proposed work are:

- Inspired by the strong capability of Markov TPM in characterizing pixel correlation, Markov features from both LBP and DWT domains are extracted and combined, for the first time, to the best knowledge of the authors.
- During the creation of image splicing forgery, there are abrupt changes that are highlighted by using a standard deviation filter in the proposed approach.
- The experimental results performed on six datasets indicate that the proposed approach offers better results than the existing techniques in terms of accuracy, TNR, TPR, and informedness as presented in Table 5.
- The comparison between existing state-of-the-art techniques and the proposed technique is given in Table 6.
- Also, the run time analysis is evaluated to authenticate the effectiveness of the proposed work as shown in Table 7.
- To validate the robustness of the proposed method, JPEG compression is applied and superior results are attained in comparison to the existing techniques.
- Furthermore, a statistical analysis test using ANOVA is performed to confirm the efficacy of the proposed scheme.

The remaining paper is structured as follows, the proposed technique is described in detail in Section 2. Section 3 illustrates the experimental results. Finally, the efficacy of the proposed technique is concluded in Section 4.

2 Proposed methodology

In this paper, the Markov process is applied after the LBP and DWT domains. Then, features from both domains are combined and normalized. The features that are being extracted rely on the perception that falsification alters the association pattern among the pixels. Consequently, features are extracted from the DWT domain and fused with the LBP domain's features. In

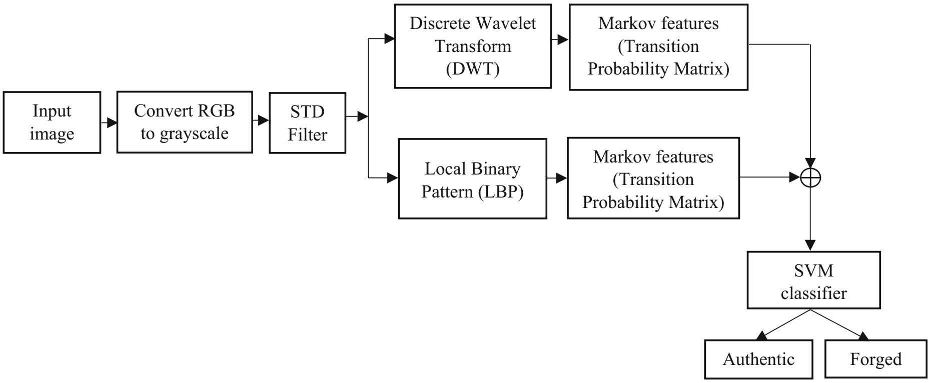

Input image
Convert RGB to grayscale
STD Filter
Discrete Wavelet Transform (DWT)
Markov features (Transition Probability Matrix)
Local Binary Pattern (LBP)
Markov features (Transition Probability Matrix)
⊕
SVM classifier
Authentic
Forged

Fig. 3 The framework of the proposed scheme for image splicing detection

both domains, statistical fluctuations are demonstrated through the Markov procedure. The layout of the proposed algorithm is described in Fig. 3.

2.1 Pre-processing

Pre-processing operations are executed on images before going to the next step. In this step, the RGB image Z of size $W \times V$ is changed to the grayscale image as given below [16]:

$$Z = 0.299R + 0.587G + 0.114B \tag{1}$$

where, R, G, and B are red, green, and blue components of the image Z, correspondingly.

2.2 STD filter

After the pre-processing, the standard deviation (STD) filter is being used to highlight the inconsistencies in the forged images. The STD filter is chosen because of its ability to measure the inconsistencies in the spliced images since intensity level changes at the edge of a spliced image by a huge value. Moreover, the edges of the spliced part are different from the other part of the image, so, the relation between the spliced part and the normal part can be used to reveal image splicing forgery. Thus, the STD filter is used as it is capable of recognizing those relations in the images since it is the best measure of variation.

This filter changes the value of each pixel in the image with that of the standard deviation of its neighbors, along with itself. In spliced images, the portion which is cut and pasted in the image to generate forgery is being highlighted using the STD filter [5, 26, 40]. Since the STD filter is used to eradicate the isolated noise points in the image, consequently, the details of edges in the spliced image are preserved using STD filtering. In contrast, other filters are more sensitive to noise, in case of edge detection. For example, in Fig. 4 the bird is removed from an image and inserted into another image to generate a forgery. It can be observed from Fig. 4 that the standard deviation filter can detect the edges of the spliced part more smoothly as compared to other filters like variance filter, skewness filter, and kurtosis filter. Thus, the proposed technique uses the STD filter to highlight the abrupt changes occurring in the spliced images.

2.3 Discrete wavelet transform (DWT)

The study of wavelet works well at grasping the short-term or localized change in signals. Some variety of wavelet families are Haar, Daubechies, Coiflet, Symlets, and Meyer. In this paper, DWT is applied by using a discrete Haar wavelet since it is a fast, memory-efficient and conceptually simple type of wavelet. According to the observations, the information concerning the edges which contains much of the image information is kept in these DWT

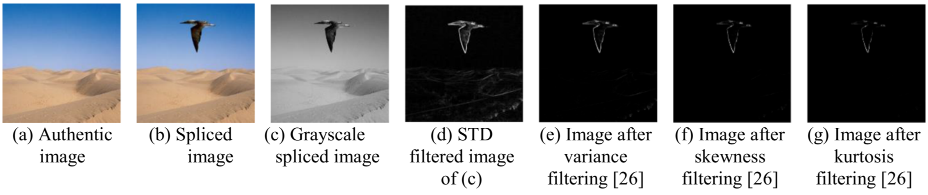

(a) Authentic image
(b) Spliced image
(c) Grayscale spliced image
(d) STD filtered image of (c)
(e) Image after variance filtering [26]
(f) Image after skewness filtering [26]
(g) Image after kurtosis filtering [26]

Fig. 4 Example of the Standard deviation filter

sub-bands. Initially, discussing first level DWT, it divides an input image into four sub-band images. Each sub-band consists of high-frequency bands as well as low-frequency bands: HL, LH, LL, and HH. Here, LL denotes low-frequency sub-band (approximation coefficient) and the other three (LH, HL, and HH) are high-frequency sub-bands (detailed coefficients) in different directions i.e. vertical, horizontal and diagonal, congruently. In third level decomposition, low-frequency sub-band is further decomposed twice to diminish the image dimensions and to extract features. Moreover, the decomposition of low-frequency sub-band leads to more information as well as less noise. The DWT conducts decomposition as well as the reconstruction of signals using scaling function $\gamma(t)$ and basic wavelet function $\xi(t)$. The original signals are approximated using scaling function and detailed variations are detected by basic function, which is given as follows [11, 39].

$$\gamma(t) = \sum_n a(n)\sqrt{2}\xi(2t{-}n) \tag{2}$$

$$\xi(t) = \sum_n b(n)\sqrt{2}\xi(2t{-}n) \tag{3}$$

Also, the scaling function is used to evaluate the basic wavelet function. $a(n)$ and $b(n)$ are coefficients of the filter, their relation is indicated in eq. (4). In this transform, $b(n)$ and $a(n)$ are almost equivalent to low pass as well as high pass filter.

$$a(n) = (-1)^n b(m{-}n{-}1) \tag{4}$$

Here, m denotes the length of the filter and n is number of levels. The decomposition of the wavelet transform is depicted in eq. (5) and (6).

$$eA1(l) = \sum_n b(n{-}2l)R(n) \tag{5}$$

$$eD1(l) = \sum_n a(n{-}2l)R(n) \tag{6}$$

$R(n)$ is an original signal and $eA1(l)$ is an approximation coefficient that preserves the low-frequency data of $R(n)$. The detailed coefficient which preserves the high-frequency data of $R(n)$ is denoted as $eD1(l)$. DWT has been used to detect the splicing forgery because it has the proficiency to scale the image in various resolution at various positions. Other transforms like DCT and DFT are full-frame transforms. Henceforth, the entire image is affected by any change in the coefficients of both transforms. But, DWT has spatial frequency locality, which means if the signal is embedded it will affect the image locally. Hence a wavelet transform provides both spatial and frequency descriptions for an image.

2.4 Local binary pattern (LBP)

LBP is an effective texture operator that captures the local deviations in the smoothness of altered images. In this technique, every pixel is labeled by the neighboring pixel’s relative gray levels. The value of the pixel is assigned as one if the neighboring pixel’s gray level is greater or equivalent to the middle pixel, otherwise, the value of the pixel is assigned as zero. Finally, the binary pattern is obtained for each center pixel. The weighted sum of pattern bits is called the LBP code. The LBP operator is calculated using eq. (7) as shown beneath [42, 47]:

$$L(x,y)=\sum_{q=0}^{q-1}Z\left(h_q-h(x,y)\right)2^q \tag{7}$$

where 'q' is total pixels in the spherical region of the radius R, $h(x,y)$ is the amount of center pixel at (x,y), h_q is q^{th} pixel in the region and $Z(h_q-h(x,y))$ is threshold function.

$$Z\left(h_q-h(x,y)\right)=\begin{Bmatrix}1 & \left(h_q-h(x,y)\right)\geq 0\\ 0 & \left(h_q-h(x,y)\right)<0\end{Bmatrix} \tag{8}$$

The original smoothness of the image is falsified in the cases when the image is counterfeit. As the LBP has proficiency in capturing the texture differences, it is used in the proposed approach to discover the forged as well as authentic images.

2.5 2-D difference arrays

The features that differentiate falsification are determined by the artifacts produced at the image's edges through the tampering procedure. Because of this purpose, the connection among neighboring pixels is captured by evaluating the differences in minor diagonal (M), vertical (V), horizontal (H) and main diagonal (D) directions for LBP as well as DWT coefficients. The difference arrays $L_z(x,y)$, $z\in\{V,H,D,M\}$for LBP is calculated by [9]:

$$L_H(x,y)=L(x,y)-L(x+1,y) \tag{9}$$

$$L_V(x,y)=L(x,y)-L(x,y+1) \tag{10}$$

$$L_D(x,y)=L(x,y)-L(x+1,y+1) \tag{11}$$

$$L_M(x,y)=L(x+1,y)-L(x,y+1) \tag{12}$$

where, $L(x,y)$ is calculated LBP code, $1\leq x\leq R_x$, $1\leq y\leq R_y$, $R_x\times R_y$is the size of the image. For DWT based Markov features, the differences are evaluated in all four directions in an analogous way as that of LBP. Here $L(x,y)$ is replaced by $W(x,y)$ in above-given equations to get $W_z(x,y)$, $z\in\{V,H,D,M\}$for DWT.

2.6 Markov transition probability matrix (TPM)

The process of Markov is a proficient tool for feature extraction and it works proficiently by identifying the relationship of the features. As stated in the theory of random process, the Markov TPM is a tool that is used to describe the relationships between the spliced portion and the normal portion of the forged image. Therefore, Markov based feature is a type of measure which can reveal the statistical changes produced by splicing. Since image splicing produces sharp edges in a forged image, therefore capturing the forgery introduced artifacts is the key for image splicing detection. So, the edges introduced by forgery are different from their "neighbors", the relationships among the spliced part and normal part can be used to expose image forgery. Consequently, techniques based on Markov are effective in image splicing problems. Initially, the STD filter is applied to the input image, which partially highlights the inconsistencies of tampering artifacts. Therefore, Markov TPM is used to discover the forged regions in images by examining the inconsistencies of tampering artifacts, completely. Since applying the Markov process to difference array leads to dimensionality reduction of Markov TPM, so the Markov process is applied to the difference arrays instead of directly applying to the image or coefficients 2-D array. The TPMs which obtained from the difference arrays of both LBP and DWT domain, capture pixels or coefficients correlations to detect spliced artifacts. The general block diagram of Markov feature extraction is given in Fig. 5 and the difference arrays for minor diagonal (M), vertical (V), horizontal (H) and main diagonal (D) are shown in Fig. 6. The equations of difference arrays for all the directions have been given in section 2.5 [15, 37].

The difference arrays of both LBP and DWT domains are limited to $[-T, +T]$. If $L(x, y)$ or $W(x, y)$ is lesser than $-T$, or larger than T, it is indicated by $-T$ or T, congruently as given in the following eq. [9].

$$Z_z(x, y) = \begin{cases} T & F_z(x, y) > +T \\ -T & F_z(x, y) < -T \\ F_z(x, y) & otherwise \end{cases} \tag{13}$$

where, $F_z(x, y)$ is either $L_z(x, y)$ or $W_z(x, y)$, for $z \in \{V, H, D, M\}$. The T constraints the number

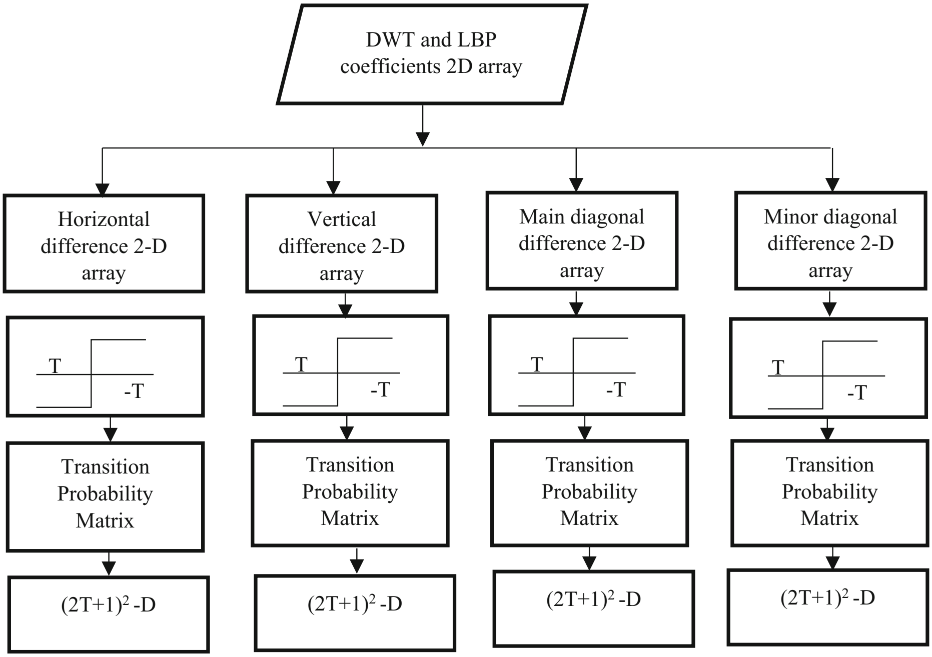

DWT and LBP
coefficients 2D array
Horizontal difference 2-D array
Vertical difference 2-D array
Main diagonal difference 2-D array
Minor diagonal difference 2-D array
T
-T
T
-T
T
-T
T
-T
Transition Probability Matrix
Transition Probability Matrix
Transition Probability Matrix
Transition Probability Matrix
(2T+1)² -D
(2T+1)² -D
(2T+1)² -D
(2T+1)² -D

Fig. 5 Block diagram of Markov feature extraction procedure

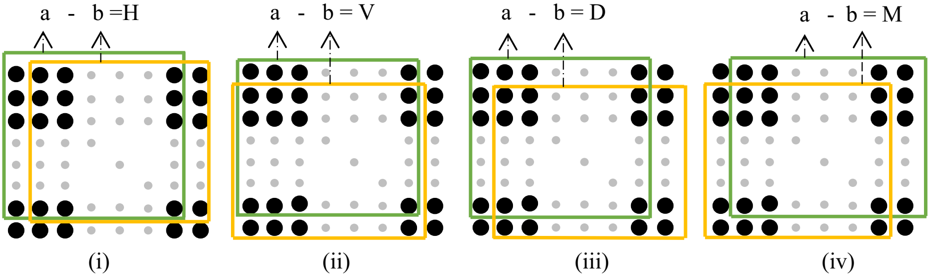


Fig. 6 Difference 2-D array: (i) Horizontal difference 2-D array (H), (ii) Vertical difference 2-D array (V), (iii) Main diagonal difference 2-D array (D), and (iv) Minor diagonal difference 2-D array (M)

of states required by the data. In the proposed scheme, the value T is set to 4 to maintain the balance between computational efficacy as well as classifier performance. The process of Markov is categorized by TPM. A total number of elements in each direction for one-step TPM is $(2T+1) \times (2T+1)$. The achieved TPM for H, V, D and M directions are given in the following eqs. [24]:

$$P\left[Z_h(x+1,y) = q|Z_h\left(x,y=p\right)\right] = \frac{\sum_{x=1}^{R_x-1}\sum_{y=1}^{R_y}\delta\left(Z_h(x,y)=p,Z_h\left(x+1,y\right)=q\right)}{\sum_{x=1}^{R_x-1}\sum_{y=1}^{R_y}\delta(Z_h(x,y)=p)} \tag{14}$$

$$P\left[Z_v(x,y+1) = q|Z_v\left(x,y=p\right)\right] = \frac{\sum_{x=1}^{R_x}\sum_{y=1}^{R_y-1}\delta\left(Z_v(x,y)=p,Z_v\left(x,y+1\right)=q\right)}{\sum_{x=1}^{R_x}\sum_{y=1}^{R_y-1}\delta(Z_v(x,y)=p)} \tag{15}$$

$$P\left[Z_d(x+1,y+1) = q|Z_d\left(x,y=p\right)\right] = \frac{\sum_{x=1}^{R_x-1}\sum_{y=1}^{R_y-1}\delta\left(Z_d(x,y)=p,Z_d\left(x+1,y+1\right)=q\right)}{\sum_{x=1}^{R_x-1}\sum_{y=1}^{R_y-1}\delta(Z_d(x,y)=p)} \tag{16}$$

$$P\left[Z_m(x,y+1) = q|Z_m\left(x+1,y=p\right)\right] = \frac{\sum_{x=1}^{R_x-1}\sum_{y=1}^{R_y-1}\delta\left(Z_m(x+1,y)=p,Z_m\left(x,y+1\right)=q\right)}{\sum_{x=1}^{R_x-1}\sum_{y=1}^{R_y-1}\delta(Z_m(x+1,y)=p)} \tag{17}$$

where, $p, q \in \{-T, -T+1, \ldots, 0, \ldots, T-1, T\}$, $R_x \times R_y$ is the dimensionality of the image. If the arguments are satisfied $\delta(\cdot) = 1$, else $\delta(\cdot) = 0$ as shown in the following equation:

$$\delta(A = p, B = q) = \begin{cases} 1 & A = p, B = q \\ 0 & otherwise \end{cases} \tag{18}$$

After evaluating the Markov from both the domains i.e. LBP and DWT at $T = 4$, the feature vector is generated. Then, this feature vector is applied to SVM classifier for the classification. Moreover, the computational complexity is reduced and detection performance is improved.

2.7 SVM classification

The support vector machine (SVM) is a standard classifier depending on the knowledge of the hyperplane. The optimal separation hyperplane which differentiates the positive pattern from the negative pattern is found by using Lagrangian multipliers. Also, it can grasp feature vectors spaces both linearly as well as nonlinearly separable. The authentic images are marked as +1 and forged images as −1, which is two-way classification and can be resolved by SVM.

```
Pseudocode for the proposed scheme
Input- Image (Authentic/Forged)
Output- Detection outcome whether the image is forged or authentic
procedure
    Input image
    if the image is colored
        Convert into a grayscale
    else
        Go to the next step
    end if
Apply STD filter to the input image
/* Compute LBP Markov-based features in all four directions: minor diagonal $(M)$, diagonal $(D)$, and horizontal $(H)$, vertical $(V)$ */
Compute LBP of the obtained image
    for $z \in \{V, H, D, M\}$
        Calculate the difference matrix $L_z$
        Apply thresholding
        Compute $TPM_z^{LBP}$
    end for
/* Compute DWT Markov-based features in all four directions: $H, V, D$ and $M$ */
Compute DWT of the obtained image
    for $z \in \{V, H, D, M\}$
        Calculate the difference matrix $W_z$
        Apply thresholding
        Compute $TPM_z^{DWT}$
    end for
Combine all $TPM_z^{LBP}$ and $TPM_z^{DWT}$ into a feature vector
Apply SVM to classify (Authentic/Forged)
end procedure
```

3 Experimental results and discussion

The proposed scheme is implemented using MATLAB R2017b (9.9.0.713579). The experimentation is carried out using Processor i.e. Intel(R) Core (TM) i5-4210U CPU @ 2.4 GHz with the memory of 4.00 GB on Microsoft Window 8.1.

3.1 Description of datasets

In this segment, all the experimentation is accomplished to estimate the efficacy of the proposed algorithm. The benchmark datasets are used in the experiment analysis which is discussed below. Figure 7 illustrates an example of images from each dataset and Table 1 illustrates certain characteristics of these datasets.

- *CASIA v1.0:* The CASIA image tampering detection evaluation dataset (CITDE) offers a more puzzling as well as faithful image for the detection of tampering. The dataset comprises 800 authentic and 921 forged images [14].
- *CASIA v2.0:* This dataset comprises of 7491 authentic as well as 5123 forged images. It involves 9 categories, classified as animal, scene, architecture, plant, nature, indoor, character, article, and texture [14].
- *Columbia Uncompressed Image Splicing Detection Evaluation Dataset:* It encloses 363 total images, out of which 183 are authentic images, else is forged. The images are in uncompressed formats i.e. BMP and TIFF. The images involve indoor sights, for instance, bookshelf, computer, or desks [19].
- *DVMM:* It is contributed by Columbia University to appraise the detection approaches. It has 933 authentic and 912 forged images. The tampering operation in this dataset has been created by cutting and pasting procedure across boundaries of the object or perpendicular/parallel strips, from a similar image or a dissimilar image [32].
- *IFS-TC:* This dataset was initially used in international competition planned by IFS-TC. It encompasses 1150 forged and 1050 authentic images [10].
- *DSO-1:* It comprises 100 authentic and 100 forged images. The dataset comprises both interiors as well as outside images. The fake images are generated by implanting one or more than one person in the original image. Various procedures such as alteration in color and illumination are executed with the motive of making realistic forged images [12].

3.2 Performance parameters

The efficacy of the procedure is evaluated using several numbers of performance parameters like Detection Accuracy (*Accuracy*), recall (*R*), F_2 score (F_2), True Positive Rate (*TPR*), F_1 score (F_1), precision (*P*), True Negative Rate (*TNR*), Informedness (*Inf*), Markedness (*Mkd*), and Mathews correlation coefficient (*MCC*). F_1 score is a parameter which merges both recall and precision in a single value. F_2 score is an average of recall as well as precision. *TPR*, also called sensitivity, is the possibility of identifying a forged image as forged. *TNR*, also called specificity, which is the possibility of identifying an authentic image as authentic. On the other hand, Accuracy is the proportion of summation of true positives and true negatives to the overall

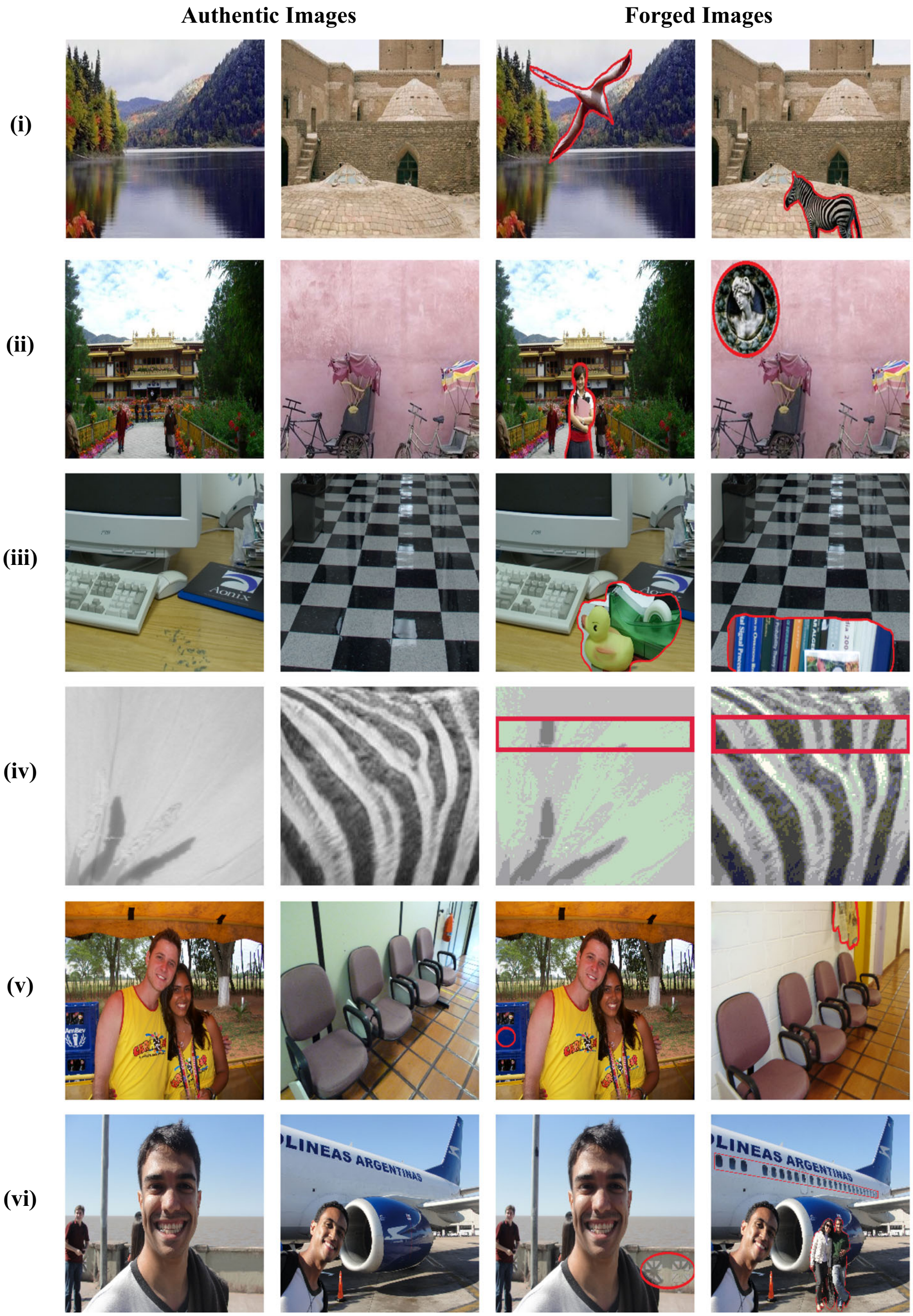


Fig. 7 Example of authentic and forged images from various datasets (i) CASIA v1.0 (ii) CASIA v2.0 (iii) Columbia (iv) DVMM (v) IFS-TC (vi) DSO-1

images used in the experiment. *MCC* is the correlation coefficient among predicted and actual classes for the classifier. Informedness (*Inf*) states the probability that the

Table 1 Characteristics of evaluated datasets

Dataset	No. of Images			File Format	Image Size
	Authentic	Forged	Total		
CASIA v1.0 [14]	800	921	1721	JPG	384×256
CASIA v2.0 [14]	7491	5123	12,614	JPG, TIFF, BMP	240×160 to 900×600
Columbia [19]	183	180	363	TIFF, BMP	757×568 to 1152×768
DVMM [32]	933	912	1845	BMP	128×128
IFS-TC [10]	1050	1150	2200	PNG	1024×768 to 2848×2144
DSO-1 [12]	100	100	200	PNG	2048×1536

classifier is informed about the condition and Markedness (*Mkd*) specifies the probability that condition is marked by the classifier. These terms are described in equations underneath [15, 17, 33].

$$P = \frac{T_P}{T_P + F_P} \tag{19}$$

$$TPR = R = Sensitivity = \frac{T_P}{T_P + F_N} \tag{20}$$

$$TNR = Specificity = \frac{T_N}{T_N + F_P} \tag{21}$$

$$F_1 = 2\frac{P.R}{P + R} \tag{22}$$

$$F_2 = 5\frac{P\cdot R}{4\cdot P + R} \tag{23}$$

$$Accuracy = \frac{T_p + T_N}{T_p + T_N + F_p + F_N} \tag{24}$$

$$MCC = \frac{T_P \times T_N - F_P \times F_N}{\sqrt{((T_P + F_P)(T_P + F_N)(T_N + F_P)(T_N + F_N))}} \tag{25}$$

$$Informedness = TPR + TNR - 1 \tag{26}$$

$$Markedness = \frac{T_P}{T_P + F_P} + \frac{T_N}{T_N + F_N} - 1 \tag{27}$$

where, T_P is total images which are perfectly identified as forged, F_P is total images incorrectly identified as forged, F_N is the number of missed forged images, T_N is total authentic images perfectly identified as authentic. Furthermore, a brief exposition of how parameters are chosen in the experiments of the proposed scheme is also given in this paper. The proposed scheme comprises different parameters such as LBP parameters, and a threshold value of Markov i.e. T. The extensive experiments have been performed on CASIA v1.0 with different LBP parameters (q, R) to discover the set that results in the best performance; here, q is total pixels in the spherical region of the radius R [7, 8]. From the experimentations, it has been observed from Fig. 8, that LBP parameters $q = 8$, $R = 1$ give the best performance with a high accuracy rate. Therefore, the next experiments are executed using these optimal values of LBP parameters.

Moreover, to select suitable values for T, few factors should be taken into account. If the value of the threshold is taken too small, it is hard to capture the spliced artifacts. On the other hand, if the value of the threshold is too large, then the dimensionality of feature vectors will be very large, as a result, the computational cost might be uncontrollable. Thus, the choice of T becomes a trade-off between detection accuracy and computational cost of the algorithm. In most of the papers [18, 28, 36, 48] using the Markov feature, the threshold value is set to 4, so, empirically, we choose $T = 4$ in our simulation.

3.3 Experimental results

As discussed earlier, six datasets are used to evaluate the proposed scheme. Meanwhile, in almost all datasets, the number of forged images are more than the authentic images, and vice-versa, so a balance is maintained between the authentic and forged images. Thus, images are randomly chosen such that an equal number of both the images are selected for the detection. The images are specified with the equivalent label, which is used for training the classifier. On the other side, the images used for the testing purpose are specified with no label and it is used to authenticate the algorithm's efficacy. For appraising the performance of the proposed scheme, 80% of images are taken for training and 20% images are taken for testing. A confusion matrix outlines the classifier's performance with respect to testing data. For instance, there are 800 genuine and 921 forged images in the CASIA v1.0 data set. To maintain balance 800 authentic and 800 forged images are taken for experimentation, so total there are 1600 images for CASIA v1.0. According to 80:20 proportion for training and testing, 1280 images

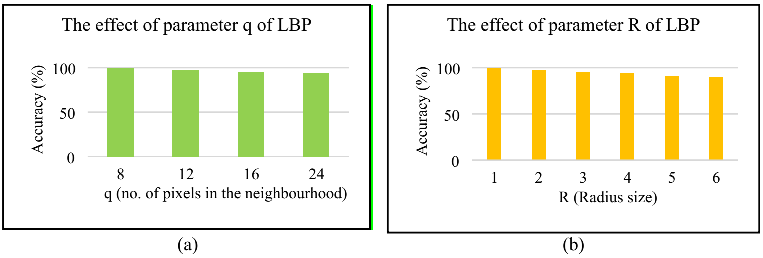


Fig. 8 Effect of LBP parameters (**a**) q (**b**) R on the performance

Table 2 Confusion matrices for the respective datasets

CASIA v1.0	Predicted Negative	Predicted Positive
Actual Negative	159	1
Actual Positive	0	160

CASIA v2.0	Predicted Negative	Predicted Positive
Actual Negative	1022	3
Actual Positive	2	1023

Columbia	Predicted Negative	Predicted Positive
Actual Negative	36	0
Actual Positive	1	35

DVMM	Predicted Negative	Predicted Positive
Actual Negative	179	3
Actual Positive	5	177

IFS-TC	Predicted Negative	Predicted Positive
Actual Negative	204	6
Actual Positive	7	203

DSO-1	Predicted Negative	Predicted Positive
Actual Negative	18	2
Actual Positive	1	19

are used in training the classifier and 320 images are used for testing purposes. Therefore, the confusion matrix is created based on 320 images to visualize the accuracy of the classifier by comparing actual and predicted classes. The confusion matrix for testing images of all the datasets i.e. CASIA v1.0, CASIA v2.0, Columbia, DVMM, IFS-TC, and DSO-1 is given in Table 2 from left to right, respectively.

The value of different performance metrics on all the datasets are specified in Table 3. The graphical representation for the performance parameters on all the datasets i.e. CASIA v1.0, CASIA v2.0, Columbia, DVMM, IFS-TC, and DSO-1 has been depicted in Fig. 9.

Several experiments have been carried out on six mentioned datasets. Moreover, the results of the combined Markov features of both LBP and DWT have been compared with LBP and DWT Markov features individually as shown in Table 4 on the respective datasets.

Table 4 reveals that significant results are attained when Markov features are extracted and combined from both the domains i.e. LBP and DWT. The graphical representation of the results obtained on all the datasets for various features such as LBP, DWT, and the combination of LBP and DWT is shown in Fig. 10.

From the observations, Markov features in the LBP domain perform better than Markov features in the DWT domain for the DVMM dataset. Furthermore, the combination of both domains attains improved results in comparison to individual domains. Also, CASIA v1.0, IFS-TC, CASIA v2.0, DSO-1, and Columbia datasets have been used. For Columbia and

Table 3 Performance parameters of the proposed method on various datasets

Parameters	CASIA v1.0	CASIA v2.0	Columbia	DVMM	IFS-TC	DSO-1
Accuracy (%)	99.69	99.76	98.61	97.80	96.90	92.50
TPR (%)	100	99.80	97.22	97.25	96.67	95.00
TNR (%)	99.38	99.71	100	98.35	97.14	90.00
F_1 score (%)	99.69	99.76	98.59	97.79	96.90	94.06
F_2 score (%)	99.88	99.79	97.77	97.49	96.76	92.47
Precision (%)	99.38	99.71	100	98.33	97.13	90.48
MCC (%)	99.38	99.51	97.26	95.61	93.81	85.11
Inf (%)	99.37	99.51	97.22	95.60	93.81	85.00
Mkd (%)	99.38	99.51	97.30	95.62	93.81	85.21

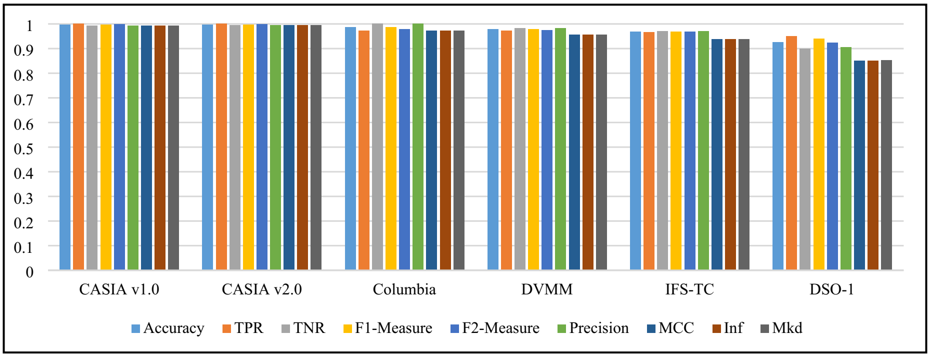


Fig. 9 Graphical representation of performance parameters on datasets

CASIA v1.0 dataset, the LBP based Markov features attain better results in comparison to DWT based Markov features in terms of accuracy and specificity. When merging DWT and LBP, there is an improvement in detection performance. Even though DVMM, CASIA v1.0 as well as Columbia dataset, is extensively used, but the size of these datasets is not large. So, to authenticate the performance of the proposed approach on a larger dataset, the same technique is utilized for CASIA v2.0. In this, Markov features in DWT perform better in comparison to Markov features in LBP.

Nevertheless, the finest performance is observed in combining features from both the domains. Also, two more datasets have been used to carry out the experimentation i.e. IFS-TC and DSO-1 datasets. The manipulation of these datasets is done by cutting and pasting various degrees of photorealism. To check the results on a very small dataset, DSO-1 is used which comprises 100 authentic and 100 forged images. The LBP based features perform superior to DWT features with higher accuracy for this dataset. Moreover, the combination of

Table 4 Results for datasets with various features

Datasets	Features	Accuracy (%)	TPR (%)	TNR (%)	Precision (%)	F_1 score (%)	F_2 score (%)	MCC (%)	Inf (%)	Mkd (%)
CASIA v1.0 [14]	LBP	86.25	85.00	87.50	87.18	86.08	85.43	72.52	72.50	72.55
	DWT	77.81	99.38	56.25	69.43	81.75	91.48	61.65	55.62	68.33
	LBP + DWT	**99.69**	**100**	**99.38**	**99.38**	**99.69**	**99.88**	**99.38**	**99.37**	**99.38**
CASIA v2.0 [14]	LBP	78.49	84.20	72.78	75.57	79.65	82.32	57.35	56.98	57.73
	DWT	86.83	**99.90**	73.76	**99.90**	88.34	94.94	76.31	73.66	79.06
	LBP + DWT	**99.76**	99.80	**99.71**	99.71	**99.76**	**99.79**	**99.51**	**99.51**	**99.51**
Columbia [19]	LBP	88.89	86.11	91.67	91.18	88.57	87.08	77.90	77.78	78.02
	DWT	81.94	86.11	77.78	79.49	82.67	84.70	64.11	63.89	64.34
	LBP + DWT	**98.61**	**97.22**	**100**	**100**	**98.59**	**97.77**	**97.26**	**97.22**	**97.30**
DVMM [32]	LBP	93.65	88.33	**98.90**	**98.76**	93.26	90.24	87.77	87.23	88.31
	DWT	93.13	96.15	90.11	90.67	93.33	95.01	86.42	86.26	86.58
	LBP + DWT	**97.80**	**97.25**	98.35	98.33	**97.79**	**97.47**	**95.61**	**95.60**	**95.62**
IFS-TC [10]	LBP	73.57	63.81	83.33	79.29	70.71	66.40	48.07	47.14	49.01
	DWT	72.62	**98.57**	46.67	64.89	78.26	89.30	52.93	45.24	61.92
	LBP + DWT	**96.90**	96.67	**97.14**	**97.13**	**96.90**	**96.76**	**93.81**	**93.81**	**93.81**
DSO-1 [12]	LBP	85.00	85.00	85.00	85.00	85.00	85.00	70.00	70.00	70.00
	DWT	82.50	95.00	70.00	76.00	84.44	90.48	67.13	65.00	69.33
	LBP + DWT	**92.50**	**95.00**	**90.00**	**90.48**	**94.06**	**92.47**	**85.11**	**85.00**	**85.21**

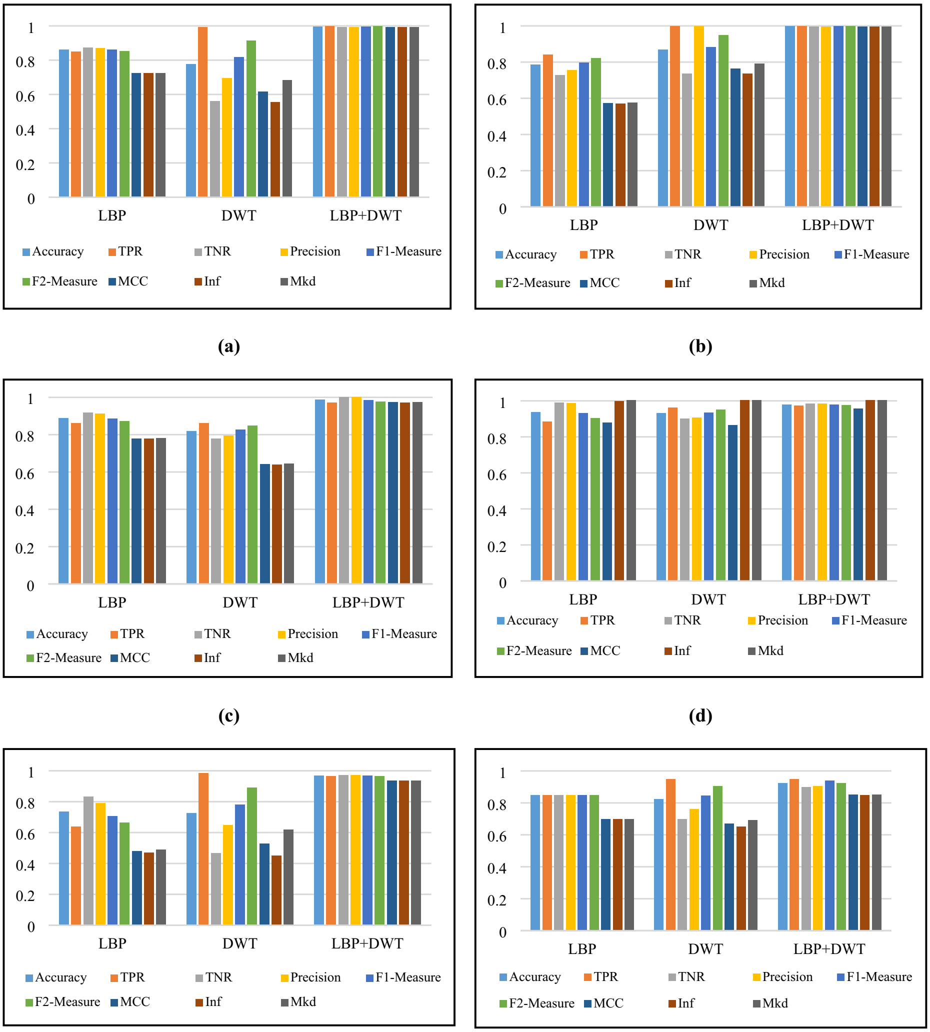
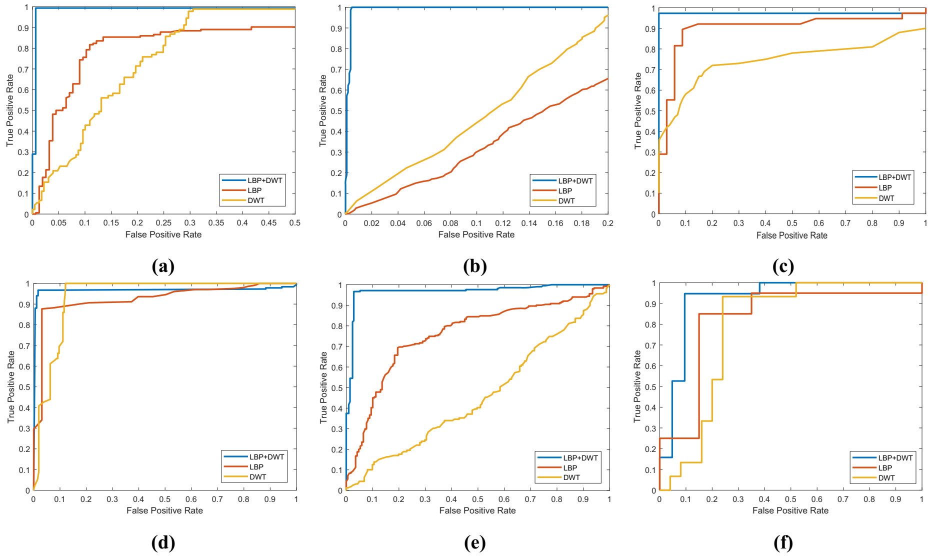


Fig. 10 Graphical representation of results evaluated for various features on (**a**) CASIA v1.0 (**b**) CASIA v2.0 (**c**) Columbia (**d**) DVMM (**e**) IFS-TC (**f**) DSO-1 datasets

both features exceeds the detection accuracy rate in comparison to individual features. The Receiver Operating Characteristic (ROC) curve is plotted to visualize the performance of the classifier. Moreover, it is used to describe the progressions of TPR as well as False Positive Rate (FPR). TPR represents the number of forged images that were perfectly identified as forged. Similarly, FPR represents the number of forged images that were wrongly classified as authentic. The ROC curves for LBP, DWT, and combined Markov features for all the datasets are shown in Fig. 11. The ROC curves for CASIA v1.0 and CASIA v2.0 dataset are zoomed for better visualization.

From Fig. 11, it is observed that the ROC curves for combined features are closer to the upper left corner which depicts the highest accuracy. The performance of the classifier is calculated by using LBP as well as DWT based Markov features separately as well as in the



(a) (b) (c)

(d) (e) (f)

Fig. 11 ROC curves for various features evaluated on (**a**) CASIA v1.0 (**b**) CASIA v2.0 (**c**) Columbia (**d**) DVMM (**e**) IFS-TC (**f**) DSO-1 datasets

combination of both. From Table 4 as well as ROC curves for respective datasets, it is clear that a combination of Markov features from both LBP and DWT domains provides better results in comparison to their individual performances. The accuracy achieved by fusing both LBP as well as DWT domains for datasets i.e. CASIA v1.0, CASIA v2.0, Columbia, DVMM, IFS-TC, and DSO-1 is 99.69%, 99.76%, 98.61%, 97.80%, 96.90%, and 92.50%, respectively.

3.4 Comparative analysis of the proposed scheme with existing schemes

To exhibit the efficacy of the proposed scheme, the comparison of performance parameters of the proposed scheme is carried out with some existing image splicing detection techniques as shown in Table 5. The ROC curve is plotted to visualize the performance of the classifier. The ROC curve that is close to the upper left corner indicates the highest performance of the proposed scheme. The comparison of ROC curves for all the datasets has been given in Fig. 12. The ROC curves have been zoomed for better visualization for CASIA v1.0 and CASIA v2.0 datasets. Moreover, the difference between the state-of-the-art techniques and the proposed technique has been given in Table 6.

From Table 5, it is revealed the proposed scheme outperforms the existing techniques in terms of performance metrics like accuracy, sensitivity, specificity, and informedness. As shown in Fig. 12, the ROC curve of the proposed scheme for all the datasets is closer to the upper left corner which depicts that it attains a better accuracy rate in comparison to other existing procedures. It is observed from the experimental results, that fusing Markov TPM features in LBP as well as DWT domains outperforms with regard to sensitivity, specificity, and accuracy. Moreover, the proposed scheme is compared with other techniques and attains excellent detection performance on CASIA v1.0, DVMM, CASIA v2.0, IFS-TC, Columbia, and DSO-1 Datasets.

Table 5 Comparison of performance parameters of the proposed scheme with existing schemes

Datasets	Techniques	Accuracy (%)	TPR (%)	TNR (%)	Inf (%)
CASIA v1.0 [14]	Alahmadi et al. [8]	97.50	96.75	98.24	94.99
	Muhammad et al. [30]	94.89	95.15	93.91	89.06
	Hussain et al. [20]	94.29	—	—	—
	Sheng et al. [36]	98.77	—	—	—
	Hakimi et al. [53]	97.21	—	—	—
	Kanwal et al. [23]	98.25	—	—	—
	Proposed scheme	**99.69**	**100**	**99.38**	**99.37**
CASIA v2.0 [14]	Alahmadi et al. [8]	97.50	98.31	96.88	95.19
	Muhammad et al. [30]	97.33	98.50	96.53	95.03
	He et al. [18]	89.76	—	—	—
	Prakash et al. [34]	96.68	95.77	97.52	93.29
	Sheng et al. [36]	97.59	—	—	
	Jalab et al. [21]	99.50	95.00	99.00	94.00
	Kanwal et al. [23]	97.59	—	—	—
	Proposed scheme	**99.76**	**99.80**	**99.71**	**99.51**
DVMM [32]	He et al. [18]	93.55	93.28	93.83	87.11
	He et al. [18]	90.07	89.92	90.21	80.13
	He et al. [18]	86.50	87.58	85.39	72.97
	Zhang et al. [51]	89.88	92.50	87.31	79.81
	El-Alfy et al. [15]	96.83	96.83	96.84	93.67
	Zhang et al. [47]	89.93	90.92	89.30	80.22
	Dong et al. [13]	84.36	83.23	85.53	68.76
	Zhao et al. [52]	93.36	92.99	93.75	86.74
	Shi et al. [37]	90.15	90.01	90.31	80.32
	Kumar et al. [27]	88.43	—	—	—
	Proposed scheme	**97.80**	**97.25**	**98.35**	**95.60**
Columbia [19]	Agarwal et al. [5]	93.81	—	—	—
	Alahmadi et al. [7]	96.60	—	—	—
	Kanwal et al. [23]	96.66	—	—	—
	Proposed scheme	**98.61**	**97.22**	**100**	**97.22**
IFS-TC [10]	He et al. [18]	91.87	95.30	89.02	84.32
	He et al. [18]	81.96	79.81	83.75	63.56
	Zhang et al. [48]	84.53	84.49	84.57	69.06
	Zhang et al. [51]	92.10	95.66	89.14	84.80
	Li et al. [28]	89.61	91.38	88.14	79.52
	Proposed scheme	**96.90**	**96.67**	**97.14**	**93.81**
DSO-1 [12]	Agarwal et al. [5]	85.31	—	—	—
	Agarwal et al. [6]	88.33	86.79	**91.44**	78.23
	Proposed scheme	**92.50**	**95.00**	90.00	**85.00**

It has been observed from Table 6 that the effectiveness of the proposed technique is validated on six datasets which are larger in number as compared to other state-of-art techniques. As a result, the proposed method attains better results with several performance parameters. Furthermore, most of the existing techniques do not perform run time analysis, statistical analysis, as well as they, are not robust against post-processing operations. On the other hand, the proposed approach overcomes these drawbacks by validating the performance with run time analysis, statistical analysis, and post-processing operation.

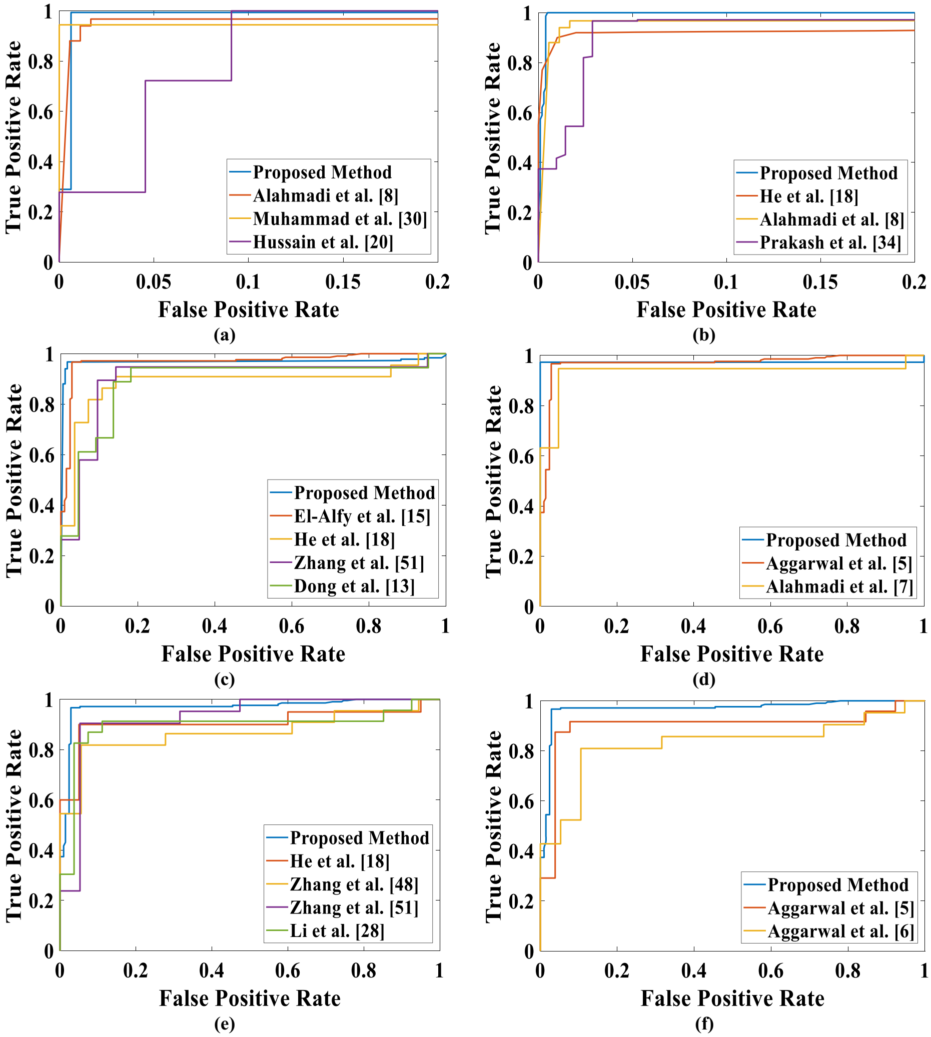


Fig. 12 Comparative analysis of ROC curves for the proposed scheme evaluated on (**a**) CASIA v1.0 (**b**) CASIA v2.0 (**c**) DVMM (**d**) Columbia (**e**) IFS-TC (**f**) DSO-1 datasets

3.5 Run time analysis of the proposed approach

In this section, the run time analysis of the proposed approach for the detection of splicing forgery is evaluated on all the six mentioned datasets. Table 7 demonstrates the average running time of the proposed approach. The execution time is different for each dataset since it depends on the different sizes of images as well as the total number of images present in the dataset. The average run time of the proposed approach attained for CASIA v1.0, CASIA v2.0, Columbia, DVMM, IFS-TC, and DSO-1 is 0.372, 0.508, 2.478, 0.110, 4.482, and 2.748 secs per image, respectively. The average run time of the DVMM dataset is lowest than the other five datasets as each image in this dataset is of small size i.e. 128×128. On the other hand, the

Table 6 Comparison of the proposed technique with other state-of-art techniques

	Datasets used	Performance parameters	Pre-processing	Feature extraction	Run time analysis	Post-processing operation	Statistical analysis
Jalab et al. [21]	CASIA v2.0	Accuracy, TPR, TNR	Color conversion, non-overlapping blocks	AMFE	__	__	__
Kanwal et al. [23]	CASIA v1.0, CASIA v2.0, Columbia	Accuracy, TPR, TNR	Color conversion, overlapping blocks	OELTP	__	__	__
Kumar et al. [27]	DVMM	Accuracy, TP, TN	Non-overlapping blocks	Markov in BDCT and DMWT domain	__	__	__
Sheng et al. [36]	CASIA v1.0, CASIA v2.0	Accuracy	Color conversion, non-overlapping blocks	DOCT	Evaluated	__	__
Prakash et al. [34]	CASIA v2.0	Accuracy, TPR, TNR	Color conversion, non-overlapping blocks	BDCT+ ZM-polar	__	__	__
Zhang et al. [51]	DVMM, IFS-TC	Accuracy, TPR, TNR	__	Markov in BDWT	__	__	__
Alahmadi et al. [8]	CASIA v1.0, CASIA v2.0, Columbia	Accuracy, TPR, TNR	Color conversion, overlapping blocks	LBP + DCT	__	__	__
Proposed Technique	CASIA v1.0, CASIA v2.0, DVMM, Columbia, IFS-TC, DSO-1	Accuracy, TPR, TNR, F_1 score, F_2 score, Precision, Mathews correlation coefficient (MCC), Informedness, Markedness	Color conversion, STD filter to highlight inconsistencies in the image	Markov in LBP and DWT domain	Evaluated	JPEG compression	ANOVA

Table 7 Run time analysis of the proposed approach on different datasets

Datasets	Image Size	Total number of images	Running Time (secs/image)
CASIA v1.0 [14]	384×256	1721	0.372
CASIA v2.0 [14]	240×160 to 900×600	12,614	0.508
Columbia [19]	757×568 to 1152×768	363	2.478
DVMM [32]	128×128	1845	0.110
IFS-TC [10]	1024×768 to 2848×2144	2200	4.482
DSO-1 [12]	2048×1536	200	2.748

IFS-TC dataset has large-sized images, thus it takes maximum processing time to execute the proposed algorithm. For small dataset i.e. DSO-1, the proposed approach performs higher than the other four datasets. Meanwhile, CASIA v1.0 and CASIA v2.0 datasets take slightly less time to execute as compared to Columbia, IFS-TC, and DSO-1 datasets. It is observed from Table 7 that the average run time of the proposed approach increases significantly either with the increase in the total number of images or the size of images.

3.6 Robustness test

In this section, post-processing operation i.e. JPEG compression is applied on the DVMM dataset to validate the robustness of the proposed technique. The JPEG compression level can be measured by the quality factor. The higher quality factors mean high quality (i.e., less compression) and vice versa. The proposed method has extracted Markov features from DWT and LBP domain. He et al. [18] fused the Markov features in a Discrete Wavelet Transform (DWT) as well as the Discrete Cosine Transform (DCT) domain. Zhao et al. [52] extracted features from BDCT and discrete Meyer wavelet transform (DMWT) domain. Shi et al. [37] treated the neighboring differences of BDCT coefficients of an image as a 1-D signal and Kirchner et al. [25] have used SPAM features. After performing the experiments, the detection accuracies of the existing detection techniques [18, 25, 37,

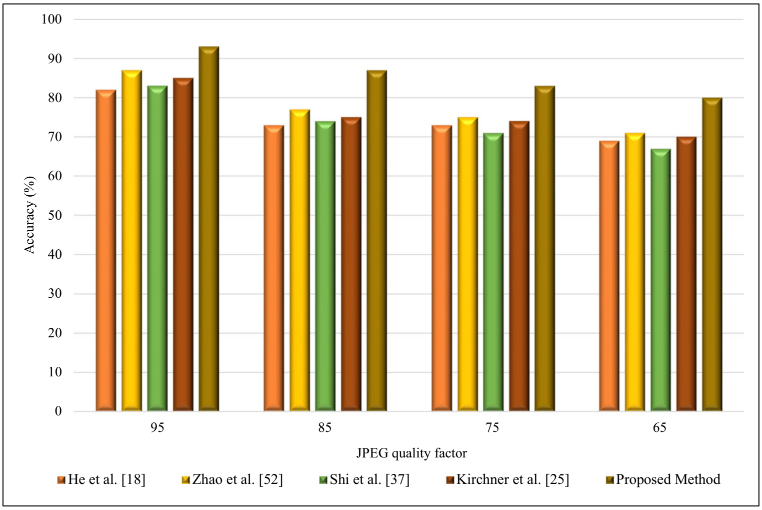


Fig. 13 Detection results for JPEG compression

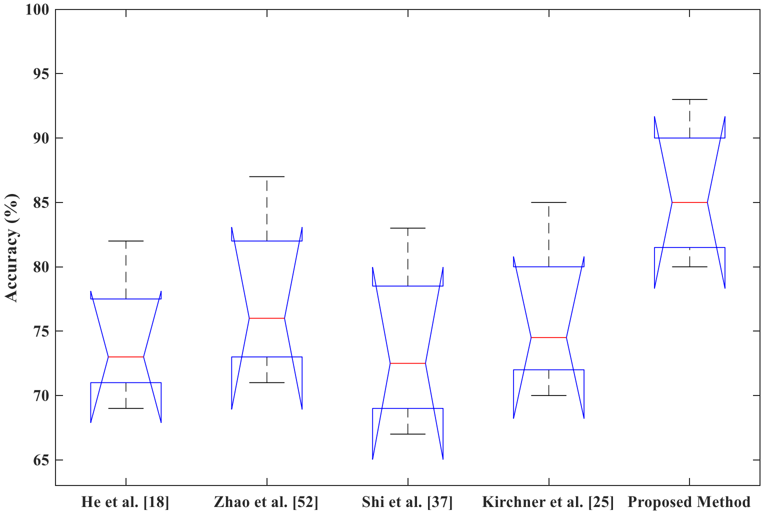


Fig. 14 Statistical analysis of detection accuracy for different techniques, when tested against JPEG compression

52] and the proposed method are evaluated as shown in Fig. 13. It has been observed from Fig. 13 that with the decrease in the quality factor, the detection accuracies of all the techniques decrease. The proposed method with different JPEG quality factors outperforms the other existing methods, which shows that the proposed approach is robust against post-processing operation i.e. JPEG compression.

The value of detection accuracy for different quality factors for various techniques has been compared by Analysis of Variance (ANOVA). The ANOVA is used to figure out whether there is any statistical significant difference among the means of two or more independent techniques. The ANOVA test is performed on the achieved results of the proposed technique and existing techniques such as He [18], Zhao [52], Shi [37], and Kirchner [25]. Figure 14 shows the statistical analysis of detection accuracy for different techniques when tested against JPEG compression. From Fig. 14, it has been analyzed that the whiskers (which indicate the maximum and minimum values) of the proposed technique reaches nearly to 100, which is higher than the other existing techniques, and also, the values of the median are better than the existing techniques at 95% confidence level. It has been observed from the representation of the data in Fig. 14 that the existing detection techniques are much weaker than the proposed technique.

4 Conclusion

A passive forgery detection methodology is proposed to validate the detection of splicing forgery. At the outset, the STD filter is used to highlight the irregularities in the forged images. Further, Markov features are extracted from LBP and DWT domains separately and combined, to detect the image splicing forgery. Then, the SVM classifier is used to evaluate the effectiveness of the algorithm. Accuracy is calculated on six different datasets i.e. CASIA v1.0, DVMM, CASIA v2.0, IFS-TC, Columbia, and DSO-1. The proposed technique attains 99.69% and 99.76% accuracy on CASIA v1.0 and CASIA v2.0, 97.80%, and 98.61% accuracy on DVMM and Columbia datasets, and 96.90% and 92.50% accuracy on IFS-TC, and DSO-1, respectively. The experimental results show that fusing Markov features from LBP and DWT domains leads to improvement in terms of detection accuracy, sensitivity, specificity, and informedness in comparison to other existing techniques. Moreover, the robustness of the proposed method is validated for JPEG compression, and efficacy is confirmed by performing the statistical analysis test using ANOVA. In future work, it has been planned to localize the tampering regions in the spliced images. Moreover, the authentication of medical images has acquired less attention in the research community. Since the medical images are misrepresented by some people to claim medical loans, the concerned patient may face social embarrassment or disappointed, while other people may achieve an illegal benefit. So, this field needs more attention to attain the trust of patients as well as to avoid their embarrassment. Thus, the proposed scheme can be extended and applied to medical images in the future work so that it will be beneficial for the society as well as the research community.

References

1. Abdallah EE, Hamza AB, Bhattacharya P (2007) Spectral graph-theoretic approach to 3D mesh watermarking. In: Proceedings of graphics interface, pp 327–334
2. Abdallah EE, Hamza AB, Bhattacharya P (2007) Improved image watermarking scheme using fast Hadamard and discrete wavelet transforms. J Electron Imaging 16(3):033020
3. Abdallah EE, Hamza AB, Bhattacharya P (2009) Watermarking 3D models using spectral mesh compression. Signal Image Video Process 3(4):375–389
4. Abdallah EE, Otoom AF, Abdallah AE, Bsoul M, Awwad S (2019) A hybrid secure watermarking scheme using nonnegative matrix factorization and FastWalsh-Hadamard transform. J Appl Secur Res 1:1–14
5. Agarwal S, Chand S (2016) Texture operator based image splicing detection hybrid technique. In: proceedings of international conference on Computational Intelligence & Communication Technology (CICT), pp 116-120
6. Agarwal S, Chand S (2016) Image forgery detection using Markov features in undecimated wavelet transform. In: ninth international conference on contemporary computing (IC3), pp 1-6
7. Alahmadi AA, Hussain M, Aboalsamh H, Muhammad G, Bebis G (2013) Splicing image forgery detection based on DCT and local binary pattern. In: proceedings of global conference on signal and information processing (GlobalSIP), pp 253-256
8. Alahmadi A, Hussain M, Aboalsamh H, Muhammad G, Bebis G, Mathkour H (2017) Passive detection of image forgery using DCT and local binary pattern. Signal Image Video Process 11(1):81–88
9. Chen C, Shi YQ (2008) JPEG image steganalysis utilizing both intrablock and interblock correlations. In: IEEE international symposium on circuits and systems (ISCAS 2008), pp 3029-3032
10. Cozzolino D, Gragnaniello D, Verdoliva L (2014) Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques. In: proceedings of international conference on image processing (ICIP), pp 5302-5306
11. Crouse MS, Nowak RD, Baraniuk RG (1998) Wavelet-based statistical signal processing using hidden Markov models. IEEE Trans Signal Process 46(4):886–902
12. De Carvalho TJ, Riess C, Angelopoulou E, Pedrini H, de Rezende RA (2013) Exposing digital image forgeries by illumination color classification. IEEE Trans Inf Forensics Secur 8(7):1182–1194
13. Dong J, Wang W, Tan T, Shi YQ (2008) Run-length and edge statistics based approach for image splicing detection. In: International workshop on digital watermarking, pp 76–87
14. Dong J, Wang W, Tan T (2013) Casia image tampering detection evaluation database. In: proceedings of China Summit & International Conference on signal and information processing (ChinaSIP), pp 422-426
15. El-Alfy ES, Qureshi MA (2017) Robust content authentication of gray and color images using lbp-dct markov-based features. Multimed Tools Appl 76(12):14535–14556
16. Emam M, Qi H, Xiamu N (2016) PCET based copy-move forgery detection in images under geometric transforms. Multimed Tools Appl 75(18):11513–11527
17. Fan J, Chen T, Kot AC (2017) EXIF-white balance recognition for image forensic analysis. Multidim Syst Sign Process 28(3):795–815

18. He Z, Lu W, Sun W, Huang J (2012) Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recogn 45(12):4292–4299
19. Hsu YF, Chang SF (2006) Detecting image splicing using geometry invariants and camera characteristics consistency. In: Proceedings of International Conference on Multimedia and Expo, pp 549–552
20. Hussain M, Saleh SQ, Aboalsamh H, Muhammad G, Bebis G (2014) Comparison between WLD and LBP descriptors for non-intrusive image forgery detection. In: proceedings of international symposium on innovations in intelligent systems and applications (INISTA), pp 197-204
21. Jalab HA, Subramaniam T, Ibrahim RW, Kahtan H, Noor NF (2019) New texture descriptor based on modified fractional entropy for digital image splicing forgery detection. Entropy 21(4):371–379
22. Jeyasudha A, Priya K (2016) Object recognition based on LBP and discrete wavelet transform. Int J Adv Signal Image Sci 2(1):24–30
23. Kanwal N, Girdhar A, Kaur L, Bhullar JS (2020) Digital image splicing detection technique using optimal threshold based local ternary pattern. Multimed Tools Appl 23(1):1–8
24. Kaur M, Gupta S (2016) A passive blind approach for image splicing detection based on DWT and LBP histograms. In: International symposium on security in computing and communication, Singapore, Springer, pp 318–327
25. Kirchner M, Fridrich J (2010) On detection of median filtering in digital images. Proc SPIE Electron Imaging Media Forensic Secur II 7541:1–12
26. Kumar V, Gupta P (2012) Importance of statistical measures in digital image processing. Int J Emerg Technol Adv Eng 2(8):56–62
27. Kumar A, Prakash CS, Maheshkar S, Maheshkar V (2019) Markov feature extraction using enhanced threshold method for image splicing forgery detection. In: Smart Innovations in Communication and Computational Sciences, pp 17–27
28. Li C, Ma Q, Xiao L, Li M, Zhang A (2017) Image splicing detection based on Markov features in QDCT domain. Neurocomputing 228:29–36
29. Mayer O, Stamm MC (2018) Accurate and efficient image forgery detection using lateral chromatic aberration. IEEE Trans Inf Forensics Secur 13(7):1762–1777
30. Muhammad G, Al-Hammadi MH, Hussain M, Bebis G (2014) Image forgery detection using steerable pyramid transform and local binary pattern. Mach Vis Appl 25(4):985–995
31. Muqeet MA, Holambe RS (2019) Local binary patterns based on directional wavelet transform for expression and pose-invariant face recognition. Appl Comput Inf 15(2):163–171
32. Ng TT, Chang SF, Sun Q (2004) A data set of authentic and spliced image blocks. Columbia University, ADVENT Technical Report, pp 203–2004
33. Powers DM (2011) Evaluation: from precision recall and f-measure to roc informedness markedness and correlation. J Mach Learn Technol 2(1):37–63
34. Prakash CS, Kumar A, Maheshkar S, Maheshkar V (2018) An integrated method of copy-move and splicing for image forgery detection. Multimed Tools Appl 77(20):26939–26963
35. Roy A, Bhalang Tariang D, Subhra Chakraborty R, Naskar R (2018) Discrete cosine transform residual feature based filtering forgery and splicing detection in JPEG images. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp 1552–1560
36. Sheng H, Shen X, Lyu Y, Shi Z, Ma S (2018) Image splicing detection based on Markov features in discrete octonion cosine transform domain. IET Image Process 12(10):1815–1823
37. Shi YQ, Chen C, Chen W (2007) A natural image model approach to splicing detection. In: proceedings of the 9th workshop on multimedia & security, pp 51-62
38. Srivastava P, Khare A (2017) Integration of wavelet transform, local binary patterns and moments for content-based image retrieval. J Vis Commun Image Represent 42(1):78–103
39. Su B, Yuan Q, Wang S, Zhao C, Li S (2014) Enhanced state selection Markov model for image splicing detection. EURASIP J Wirel Commun Netw 2014(7):1–10
40. Sun XW, Li YJ, Chen Y (2008) Application of local standard deviation filtering in image processing [J]. Electron Opt Control 15(9):32–34
41. Sutthiwan P, Shi YQ, Su W, Ng TT (2010) Rake transform and edge statistics for image forgery detection. In: IEEE international conference on multimedia and expo (ICME), pp 1463-1468
42. Vaishnavi D, Subashini TS (2016) Recognizing image splicing forgeries using histogram features. In: proceedings of international conference on big data and Smart City (ICBDSC), pp 1-4
43. Yu H, He F, Pan Y et al (2016) An efficient similarity-based level set model for medical image segmentation. J Adv Mech Syst, Manuf 10(8):JAMDSM0100-JAMDSM0100
44. Yu H, He F, Pan Y (2018) A novel region-based active contour model via local patch similarity measure for image segmentation. Multimed Tools Appl 77(18):24097–24119
45. Yu H, He F, Pan Y (2019) A novel segmentation model for medical images with intensity inhomogeneity based on adaptive perturbation. Multimed Tools Appl 78(9):11779–11798

46. Yu H, He F, Pan Y (2020) A scalable region-based level set method using adaptive bilateral filter for noisy image segmentation. Multimed Tools Appl 79(9):5743–5765
47. Zhang Y, Zhao C, Pi Y, Li S (2012) Revealing image splicing forgery using local binary patterns of DCT coefficients. In: Communications, Signal Processing, and Systems, pp 181–189
48. Zhang Q, Lu W, Weng J (2016) Joint image splicing detection in DCT and Contourlet transform domain. J Vis Commun Image Represent 40:449–458
49. Zhang H, Wang C, Zhou X (2017) Fragile watermarking based on LBP for blind tamper detection in images. J Inf Process Syst 13(2):385–399
50. Zhang Z, Wang C, Zhou X (2018) A survey on passive image copy-move forgery detection. J Inf Process Syst 14(1):6–31
51. Zhang Q, Lu W, Wang R, Li G (2018) Digital image splicing detection based on Markov features in block DWT domain. Multimed Tools Appl 77(23):31239–31260
52. Zhao X, Wang S, Li S, Li J (2015) Passive image-splicing detection by a 2-d noncausal markov model. IEEE Trans Circuits Syst Video Technol 25(2):185–199
53. Hakimi F, Hariri M, GharehBaghi F (2015) Image splicing forgery detection using local binary pattern and discrete wavelet transform. In 2nd international conference on knowledge-based engineering and innovation. Tehran, IEEE, pp 1074–1077

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

Navneet Kaur[1] • **Neeru Jindal**[1] • **Kulbir Singh**[1]

[1] Electronics and Communication Engineering Department, Thapar Institute of Engineering and Technology, Patiala, Punjab, India