Pattern Anal Applic (2015) 18:713–723
DOI 10.1007/s10044-014-0396-4

INDUSTRIAL AND COMMERCIAL APPLICATION

Combining spatial and DCT based Markov features for enhanced blind detection of image splicing

E-Sayed M. El-Alfy · Muhammad Ali Qureshi

Received: 9 December 2013 / Accepted: 22 July 2014 / Published online: 6 August 2014

Abstract Nowadays, it is extremely simple to manipulate the content of digital images without leaving perceptual clues due to the availability of powerful image editing tools. Image tampering can easily devastate the credibility of images as a medium for personal authentication and a record of events. With the daily upload of millions of pictures to the Internet and the move towards paperless workplaces and e-government services, it becomes essential to develop automatic tampering detection techniques with reliable results. This paper proposes an enhanced technique for blind detection of image splicing. It extracts and combines Markov features in spatial and Discrete Cosine Transform domains to detect the artifacts introduced by the tampering operation. To reduce the computational complexity due to high dimensionality, Principal Component Analysis is used to select the most relevant features. Then, an optimized support vector machine with radial-basis function kernel is built to classify the image as being tampered or authentic. The proposed technique is evaluated on a publicly available image splicing dataset using cross validation. The results showed that the proposed technique outperforms the state-of-the-art splicing detection methods.

E-Sayed M. El-Alfy: On leave from the College of Engineering, Tanta University, Egypt.

E.-S. M. El-Alfy (✉)
College of Computer Sciences and Engineering, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia
e-mail: alfy@kfupm.edu.sa

M. A. Qureshi
Electrical Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia

Keywords Multimedia security · Image forensics · Authentication · Forgery detection · Image splicing · Markov features · Support vector machine

1 Introduction

Photographs are widely used as a rich and clear information source in many areas including forensic investigation, medical imaging, journalism, and e-services. But with the increased growth of technology and availability of powerful image editing software packages like Adobe Photoshop and Corel Draw, it is getting easier to manipulate and distribute forged images that are difficult to authenticate visually. The digital image world is tremendously populated with tampered contents and it increases day by day. Image forgery can alter the semantic content of the image and thus can have a severe negative social impact, e.g. a person can appear in an awkward situation or be accused by crimes which he/she never committed. This can lead to catastrophic consequences when people mistrust the authenticity of the images.

Image splicing deals with cut and paste from one or more images to create fake images which did not happen in reality. Figure 1 shows two examples of incidents of forged images. The first example shows splicing from two images to create a third image, a news photo of John Kerry, a former democratic candidate for US presidency, with Jane Fonda, a Hollywood actress and anti-war activist [22]. This photo was manipulated in 2004 during the American presidential election campaign to raise the question about John Kerry's patriotism. The second example has been recently published in an Egyptian newspaper; a forged photograph showing Mubarak (President of Egypt at the time of the event) leading the Middle Eastern peace talks

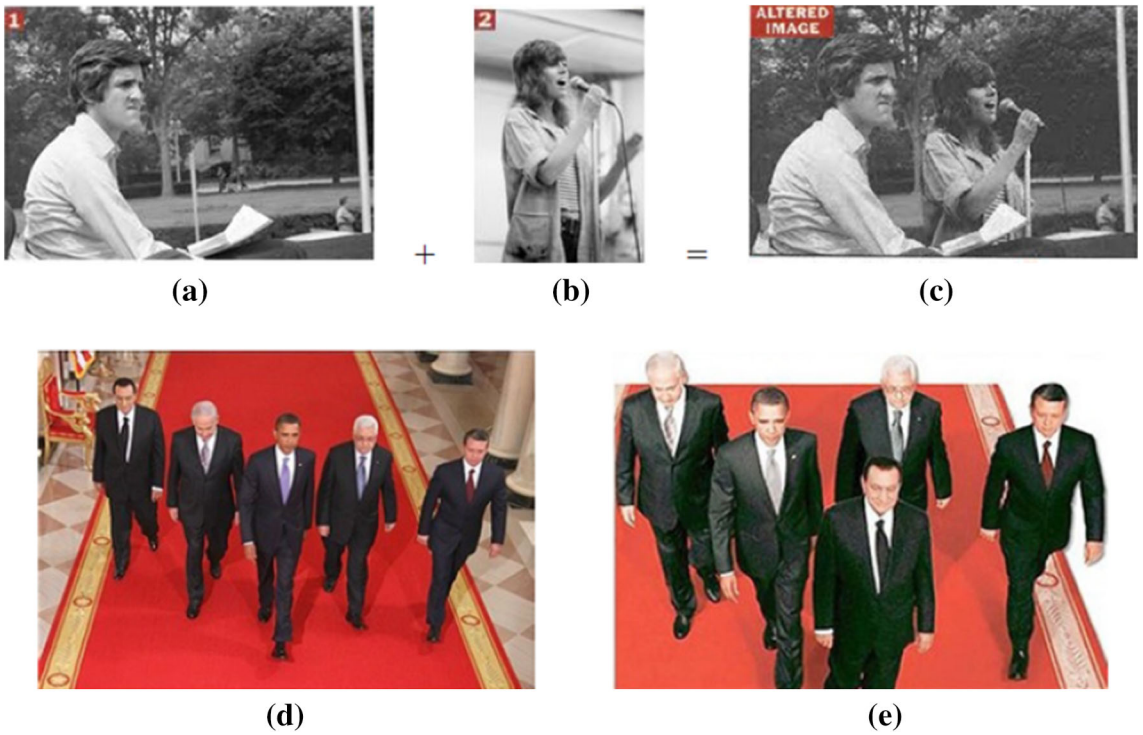

Fig. 1 Examples of tampered images: **a** Original image of a former presidential candidate (John Kerry), **b** original image of an actress and anti-war activist (Jane Fonda), **c** forged image of John Kerry with Jane Fonda, **d** original image with Obama leading the pack, **e** forged image with Mubarak leading the pack

while in fact the US President Obama was walking ahead leading the pack. It demonstrates splicing within the same image (also known as copy-move forgery).

Due to the advances and sophistication in image forgery, it is becoming crucial to develop more reliable and efficient image forensic methods that can differentiate tampered images from authenticated images. A number of methods have been proposed in the literature which can be classified as being active or passive/blind. In active methods, a watermark or signature is embedded in the source image to be used later to check the credibility of the image [2, 7]. Embedding is performed by either the acquisition device (such as a digital camera) or an authorized person. This can limit its application as most digital cameras and other image acquisition devices may not have watermarking capabilities. Moreover, the image quality can be degraded by the embedded watermark. On the other hand, passive or blind methods do not need prior information about the original image but they use the traces left by the forgery operation [1, 21].

In this paper, we present a technique for the blind detection of image splicing based on Markov features and support vector machine (SVM) classifiers. Unlike earlier work, e.g. [24], we not only extract Markov features in DCT domain but also in spatial domain. Merging features from both domains has helped the detection technique to achieve better results in terms of accuracy, specificity and sensitivity. To reduce the dimensionality of the search space, we used PCA to select the most relevant features for constructing the computational model.

The organization of the paper is as follows. Section 2 gives some preliminary background and reviews work related to different splicing detection methods. Section 3 describes the details about the proposed technique including feature extraction and reduction, and pattern classification. In Sect. 4, experimental work is described and simulation results are discussed and compared. Finally, Sect. 5 concludes the paper and Sect. 6 highlights the originality and contribution of the paper.

2 Related work

A lot of research has been carried out to detect image forgery. Ng and Chang [18] and Ng et al. [19], motivated by the work of Farid [10] on detecting human speech splicing, proposed a model using high-order bi-coherence features (both phase and magnitude) to detect image splicing. Bi-coherence is a normalized bi-spectrum of three harmonically related Fourier frequencies of a signal and are effective for the detection of discontinuity caused by splicing. This method was tested on Columbia Image Splicing Detection Evaluation Dataset [20]. However, due

to the difference of statistical distributions of audio signals from digital images, the obtained results were not satisfactory with a maximum detection accuracy of 72 %.

Dong et al. [9] investigated the coherency and discontinuity in image pixel correlation in the tampered image using features based on image run-length representation and sharp image characteristics with 76.52 % detection accuracy of the the Columbia University dataset which was further improved by He et al. [14, 15].

In [11], Farid et al. used high-order wavelet features and applied SVM for classification between photorealistic images and photographic images where photorealistic means images created using editing tools. Fu et al. [12] generated features by exploiting the non-linearity and non-stationarity nature of splicing operation using Hilbert–Huang Transform (HHT). In addition, moments of characteristic functions were calculated and used as features in wavelet domain at various decomposition levels of the spliced image. Both of these features were used with SVM for classification between spliced and authentic images. The detection accuracy of that method was 80.15 %.

In [6], Chen et al. proposed 2D phase congruency and moments of characteristic functions in the wavelet domain as robust features to detect the sharp transitions in terms of edges, lines and corners introduced during splicing. The dimension of the feature vector was 120 out of which 96 were moment-based and 24 were phase-related features. The algorithm was tested on the Columbia University dataset with detection accuracy of 82.32 %. In [24], Shi et al. suggested a model using moments and Markov statistical features. Moment features were based on 1D and 2D moments of characteristic functions as an improved version of the method used in steganalysis [23]. These moments based features are computationally expensive. The overall efficiency and effectiveness of the scheme were due to the Markov features in the DCT domain. The detection accuracy of this method was evaluated as 91.87 % on the Columbia University dataset.

To adapt to JPEG compression which can attenuate the characteristics of local correlation patterns, Li et al. [17] proposed a model using color filter array (CFA) interpolation. The frequency characteristics of the posterior probability map are calculated and combined then compared to a threshold to classify the image as tampered or not. Zhao et al. [25] used a conditional co-occurrence probability matrix (CCPM) to detect splicing. PCA was used to reduce the dimensionality of features. Their approach performed well in block DCT (BDCT) domain as well as Markov features.

In [26], Zhongwei et al. used enhanced Markov features calculated from the transition probability matrices [24] to capture the inter-block correlation among DCT blocks in addition to intra-block correlation as discussed in [5]. Similar to moment features as discussed in [23], Markov random process is effective in determining these statistical changes occurred due to the splicing operation [24]. More features in wavelet domain were also calculated. To make it computationally efficient, feature dimension is reduced using SVMRFE, a recursive feature elimination technique using SVM and weight magnitude as a ranking criterion [13]. For classification between authentic and forged images, SVM with Radial-basis function (RBF) kernel was used. Comparison with other state of the art methods, the highest accuracy achieved was 93.55 %.

3 The proposed technique

The task of classifying an image from a group of authenticated and tampered images is casted as a two-class pattern recognition problem. Since splicing operation changes the smoothness, regularity, continuity and/or periodicity, correlations among the pixels of authenticated images also change. The distinguishing features are captured by a Markov process in both spatial and DCT domains. The proposed technique uses a pre-labelled dataset to construct a computational model capable of detecting image splicing. It starts with feature extraction to represent each image in the dataset with a feature vector. Then, it applies PCA to reduce the dimensionality of the vector space and to select the most relevant features for detecting clues of changes due to splicing. Using supervised learning, an optimized support vector machine is trained using a Gaussian radial basis function kernel to generate a score between 0 and 1 which is compared with a decision threshold to declare authentic or tampered. The details of these steps are explained in the following subsections.

3.1 Feature extraction

A key issue in pattern recognition is feature extraction which should provide a set of discriminative features with low correlation to each other. For image splicing detection, the extracted features depend on the observation that splicing changes the correlation pattern among pixels. In our case, we extract features from spatial domain and merge them with features extracted in the DCT domain. In each domain, we model the statistical changes through a Markov process. The outline for calculating these features is shown in Fig. 2 and the details are described next.

3.1.1 Block DCT

The image is first divided into non-overlapping blocks and the DCT coefficients are computed for each block. The

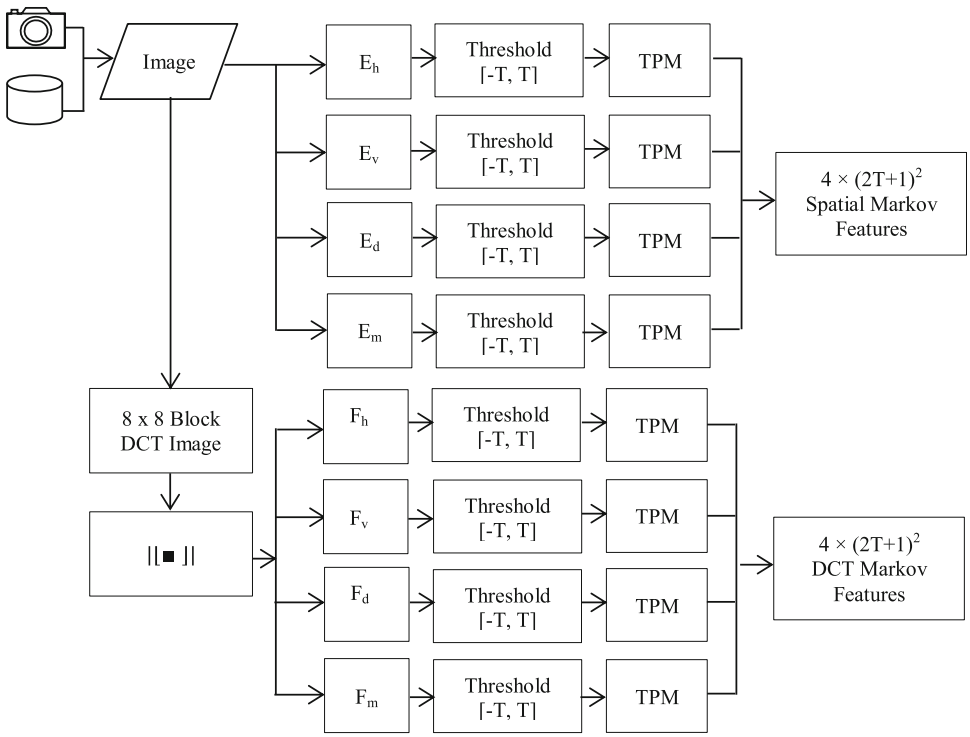

Fig. 2 Block diagram for the Markov features extraction process

DCT coefficients are then truncated to integer absolute values and stored in BDCT 2D array $F(u,v)\ \forall u,v$ which has the same size as the original image $I(u,v)\ \forall u,v$.

3.1.2 Difference 2D arrays

Since the splicing operation introduces sharp edges in the tampered image, and splicing detection methods are basically based on capturing the artifacts introduced in the edges. For this purpose, the edge images are calculated in horizontal, vertical, major diagonal and minor diagonal directions. Any suitable edge detection algorithm can be used but here for simplicity we preferred to subtract the pixel value from its neighboring pixel value in all directions to get the edge images using Eqs. (1–4):

$$E_h(u,v) = I(u,v) - I(u+1,v); \quad 1 \le u \le S_u - 1, 1 \le v \le S_v \tag{1}$$

$$E_v(u,v) = I(u,v) - I(u,v+1); \quad 1 \le u \le S_u, 1 \le v \le S_v - 1 \tag{2}$$

$$E_d(u,v) = I(u,v) - I(u+1,v+1); \quad 1 \le u \le S_u - 1, 1 \le v \le S_v - 1 \tag{3}$$

$$E_m(u,v) = I(u+1,v) - I(u,v+1); \quad 1 \le u \le S_u - 1, 1 \le v \le S_v - 1 \tag{4}$$

where $I(u,v)\ \forall u,v$ is the source image in the spatial domain and S_u, S_v denote the dimensions of the spatial image. Figure 3 shows a numerical example to illustrate calculation of the 2D difference arrays in all directions.

For DCT based Markov features, difference arrays for truncated absolute DCT coefficients are calculated in all directions in a similar manner to spatial domain using Eqs. (5–8). The difference 2D arrays reflect the correlation between DCT coefficients with its neighbors.

$$F_h(u,v) = F(u,v) - F(u+1,v) \quad 1 \le u \le S_u - 1, 1 \le v \le S_v \tag{5}$$

$$F_v(u,v) = F(u,v) - F(u,v+1) \quad 1 \le u \le S_u, 1 \le v \le S_v - 1 \tag{6}$$

$$F_d(u,v) = F(u,v) - F(u+1,v+1) \quad 1 \le u \le S_u - 1, 1 \le v \le S_v - 1 \tag{7}$$

$$F_m(u,v) = F(u+1,v) - F(u,v+1) \quad 1 \le u \le S_u - 1, 1 \le v \le S_v - 1 \tag{8}$$

where $F(u,v)\ \forall u,v$ is the absolute value of BDCT 2D array.

3.1.3 Thresholding

To reduce the dimension of the transition probability matrix (TPM), to be calculated in the next subsection, a threshold T is assumed and the elements of the difference arrays above and below $+T$ and $-T$ are set to $+T$ and $-T$, respectively, using Eq. (9):

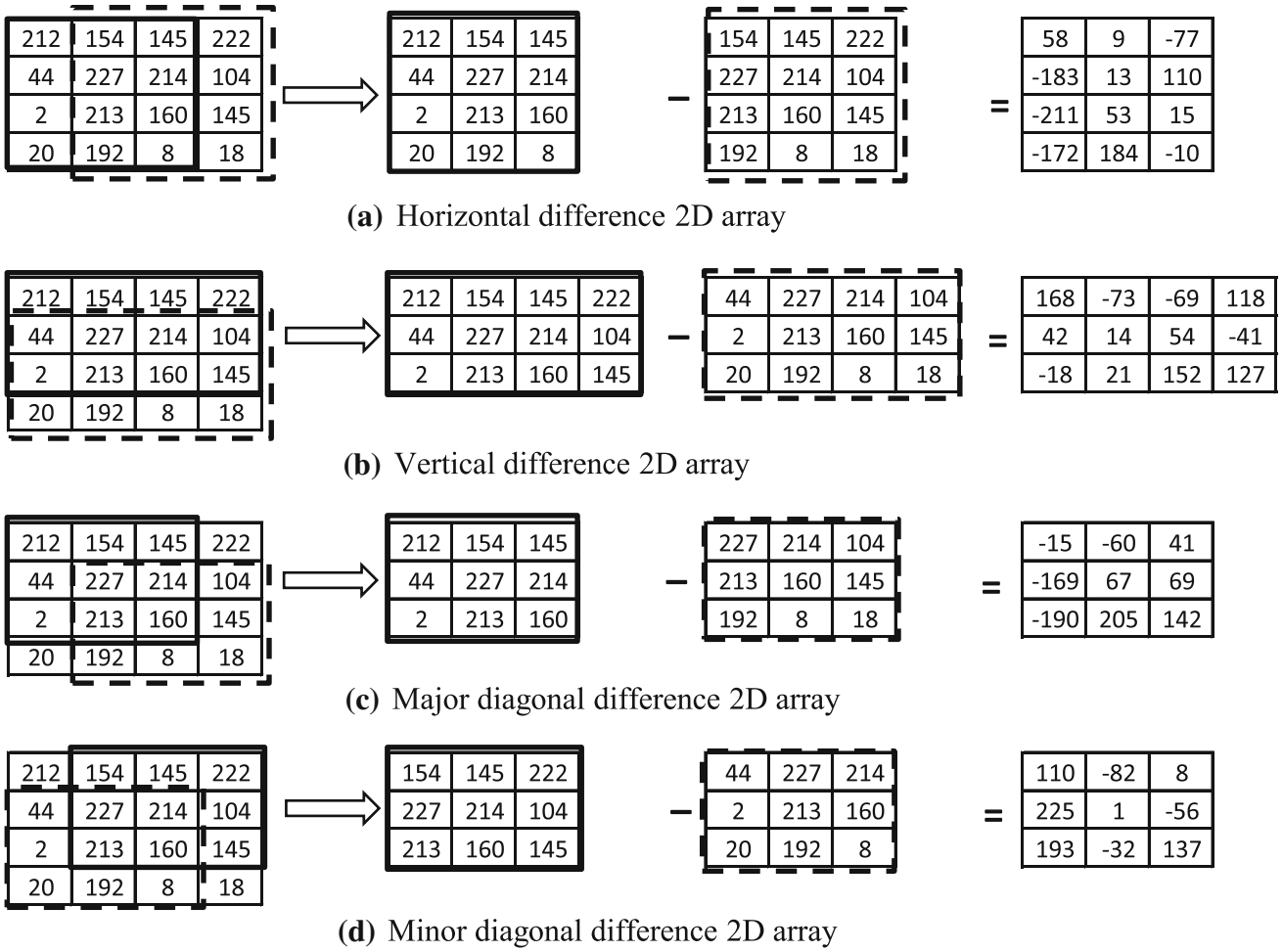

Fig. 3 Example for calculating the difference arrays. **a** Horizontal difference 2D array, **b** vertical difference 2D array, **c** major diagonal difference 2D array and **d** minor diagonal difference 2D array

$$T(u,v) = \begin{cases} +T & X(u,v) \geq +T \\ -T & X(u,v) \leq -T \\ X(u,v) & \text{Otherwise} \end{cases} \quad (9)$$

where $X(u,v)$ stands for $E_h(u,v)$, $E_v(u,v)$, $E_d(u,v)$, $E_m(u,v)$, $F_h(u,v)$, $F_v(u,v)$, $F_d(u,v)$, or $F_m(u,v)$. Hence, the values of the difference arrays of DCT coefficients and edge images, are limited to the range $[-T,+T]$ with only $(2T+1)$ possible values. This is an important step to reduce the feature vector space dimensionality as well as the computational complexity. Special care must be taken in selecting the threshold value T, which should not be too small or too large. As T increases, the number of elements in the TPM matrix increases and hence the complexity increases. Moreover, changes resulting from the edges in the original image will interfere with that from the splicing operation and the detection performance will deteriorate. In our experimental, we tried different values for T starting from 2 to 15 and we found that the best accuracy occurred at $T = 4$. So, we preferred to select a threshold to be either 3 or 4 to have a compromise between computational efficiency and classifier performance.

3.1.4 One-step transition probability matrix (TPM)

After thresholding, the elements are now integers between $[-T,+T]$ and can be modelled as a finite-state machine (FSM) to capture inter-pixel dependencies within DCT blocks and edge image pixels. A Markov random process is used as a tool to describe this correlation. The Markov process can be characterized by a transition probability matrix (TPM) computed from the thresholded arrays. Here, we used the one-step TPM. Consequently, this matrix has $(2T+1) \times (2T+1)$ elements for each direction. We used these elements as features; hence, the total number of Markov features in all directions for a spatial image is $4 \times (2T+1) \times (2T+1)$ and similar number for DCT

Table 1 Number of Markov features as given by $4 \times (2T+1)^2$

	$T=3$	$T=4$	$T=5$	$T=8$
Spatial	196	324	484	1,156
DCT	196	324	484	1,156
Total	392	648	968	2,312

based Markov features. As shown in Table 1, this number increases dramatically with the increase of T.

The one-step transition probability matrices in horizontal, vertical, major diagonal and minor diagonal directions are calculated using Eqs. (10)–(13):

$$P[T_h(u+1,v)=j|T_h(u,v)=i]=\frac{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v}\delta(T_h(u,v)=i,T_h(u+1,v)=j)}{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v}\delta(T_h(u,v)=i)} \quad (10)$$

$$P[T_v(u,v+1)=j|T_v(u,v)=i]=\frac{\sum_{u=1}^{S_u}\sum_{v=1}^{S_v-2}\delta(T_v(u,v)=i,T_v(u,v+1)=j)}{\sum_{u=1}^{S_u}\sum_{v=1}^{S_v-2}\delta(T_v(u,v)=i)} \quad (11)$$

$$P[T_d(u+1,v+1)=j|T_d(u,v)=i]=\frac{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v-2}\delta(T_d(u,v)=i,T_d(u+1,v+1)=j)}{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v-2}\delta(T_d(u,v)=i)} \quad (12)$$

$$P[T_m(u,v+1)=j|T_h(u,v)=i]=\frac{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v-2}\delta(T_m(u+1,v)=i,T_m(u,v+1)=j)}{\sum_{u=1}^{S_u-2}\sum_{v=1}^{S_v-2}\delta(T_m(u+1,v)=i)} \quad (13)$$

where

$$\delta(A=i,B=j)=\begin{cases}1 & A=i,B=j\\ 0 & \text{Otherwise}\end{cases}$$

$$\forall i,j\in\{-T,-T+1,\ldots,0,\ldots,T-1,T\}.$$

3.2 Feature reduction

The most discriminative features are selected using Principal Component Analysis (PCA). It converts the feature vectors into a lower-dimensional space by taking the largest eigenvalues from the covariance matrix. The resulting features are those which have the highest contribution in the variance in the data. For example, when $T=3$ and $T=4$, the number of Markov features are 392 and 648, respectively. Using PCA, we have reduced these numbers to 30, 50, 100 and 150 dimensions.

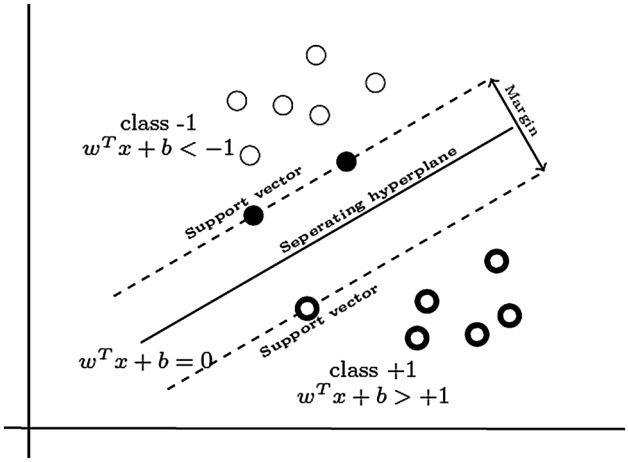

Fig. 4 SVM decision hyperplane

3.3 Tampering detection

After the features have been extracted and the most relevant have been selected, we built an optimized SVM as a classifier. SVM has gained great importance in pattern recognition in a variety of fields [3, 4, 8, 16]. The underlying idea of SVM is to map the feature space into a higher-dimensional space where data points become linearly separable using a kernel function. The training algorithm of SVM constructs a maximum margin hyper-plane in the new space of mapped features to separate the data points; as illustrated in a 2D example in Fig. 4. The closest points to the hyper-plane are called support vectors. The optimal separation hyper-plane is found by solving a constrained optimization problem using the Lagrangian multipliers.

SVM can handle feature vectors spaces whether they are linearly or non-linearly separable. We have represented training data as pairs x_i, ω_i where $x_i \in R^N$ is the feature vector, N represents the feature dimensions and $\omega_i = \pm 1$ for two class patterns. In our case, we considered $\omega_i = +1$ for spliced images and $\omega_i = -1$ for authenticated images.

For the linearly separable case, SVM looks for a hyper-plane $H : w^T y + b = 0$ and two hyper-planes $H_1 : w^T y + b = 1$ and $H_2 : w^T y + b = -1$ parallel to, and with equal distances to H with the condition that there are no data points between H_1 and H_2 and the distance between H_1 and H_2 is maximized, where w and b are the parameters to be optimized (see Fig. 4). For the non-linearly separable case, input feature vectors are transformed in to a higher-dimensional space, by using a kernel function, where a linear hyper-plane is located. There are three common kernels: polynomial, radial-basis function (RBF) and

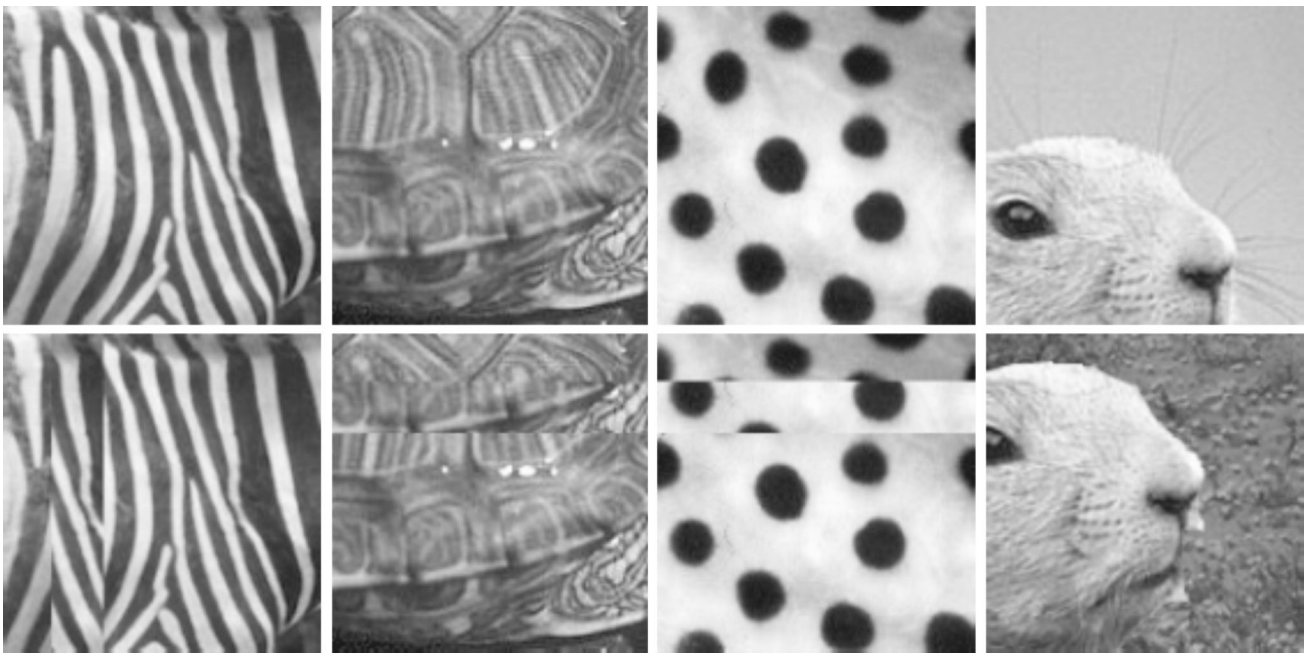

Fig. 5 Examples of images from DVMM: authentic images (*top row*) and tampered images (*bottom row*)

sigmoid. The Gaussian RBF kernel is selected in our work because of its good performance.

4 Evaluation

4.1 Dataset description

For our proposed methodology, Markov features are calculated and classified on a publicly available and well renowned image dataset, the Columbia Image Splicing Detection Evaluation Dataset. This dataset is created by Digital Video and Multimedia Lab (DVMM) at Columbia university [20]. It consists of 1,845 images of diverse content from which 933 are authentic and 912 are spliced images. These images are gray-scaled in bitmap format with dimension 128×128. The splicing operation has been carried out by cut-and-paste along object boundaries or horizontal/vertical strips, from the same or other image. Figure 5 shows some example images from this dataset; authentic images are in the top row whereas spliced images are in the bottom row.

4.2 Experimental settings

The experimental procedure for the proposed methodology is summarized in the block diagram as shown in Fig. 6. It starts by reading the authentic and spliced images from the dataset one by one. Then, the Markov features in both spatial and DCT domains are calculated. The transition probability matrix is calculated using the threshold T for all directions. The class label is appended in the last column of the feature vector. The dimensionality of the feature space is reduced using PCA. After that, tenfold cross-validation is used to avoid bias in the classification process. The dataset is randomized and divided into ten blocks. Then training occurs on nine blocks and tested on the remaining block then it repeats 9 more times taking a different block for testing each time. The total numbers of Markov features for spatial as well as DCT domain for certain threshold are listed in Table 1 for various values of T.

We utilized the LIBSVM [4] library with MATLAB to build the SVM classifier with RBF kernel for our experimental work. To tune the SVM parameters, we used tenfold grid search. An example of the grid search is shown in Fig. 7 for $T = 4$ and $N = 50$. The SVM model attained from training the SVM classifier is then used for predicting the class labels for the testing data.

4.3 Performance metrics

The detection performance is first evaluated in terms of the detection accuracy (Acc), true positive rate (TPR) and true negative rate (TNR). We have considered spliced image as positive and authentic image as negative. TPR and TNR are also known as sensitivity and specificity, respectively. The metrics are calculated as follows:

$$\mathrm{Acc} = \frac{(\mathrm{TP} + \mathrm{TN})}{(\mathrm{TP} + \mathrm{TN} + \mathrm{FN} + \mathrm{FP})} \tag{14}$$

$$\mathrm{TPR} = \frac{\mathrm{TP}}{(\mathrm{TP} + \mathrm{FN})} \tag{15}$$

$$\mathrm{TNR} = \frac{\mathrm{TN}}{(\mathrm{TN} + \mathrm{FP})} \tag{16}$$

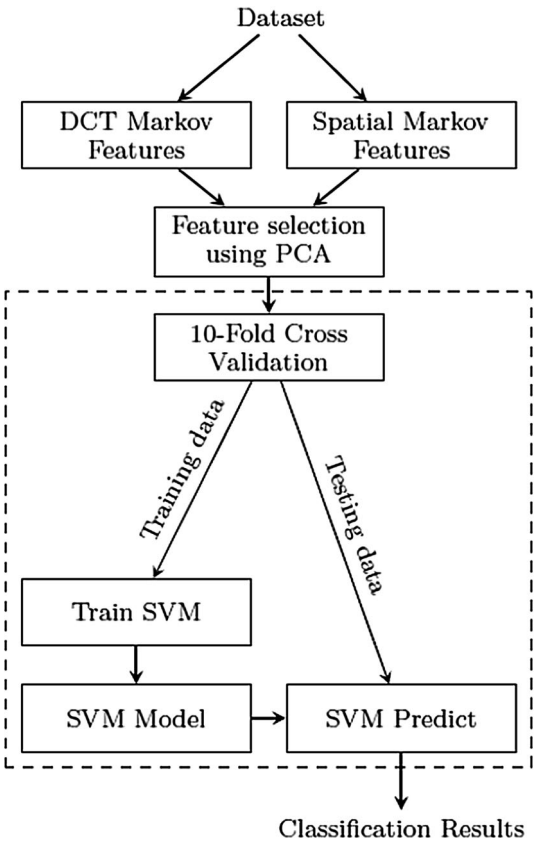

Fig. 6 Experimental procedure block diagram

where TP, TN, FP, and FN stand for true positive (tampered predicted as tampered), true negative (authentic predicted as authentic), false positive (authentic predicted as tampered), and false negative (tampered predicted as authentic), respectively.

We also used the Receiver Operating Curve (ROC) and the Area Under the Curve (AUC) to plot the changes in TPR and FPR as the decision threshold changes from 0 to 1.

4.4 Experiments and results

The classifier performance is evaluated using spatial and DCT Markov features individually as well as a combination of both for different values of the threshold T. Table 2 shows the tenfold cross validation results for $T = 3$ and $T = 4$ for different dimensions $N = 150, 100, 50$, and 30 in terms of accuracy (Acc), true positive rate (TPR), true negative rate (TNR), and area under the curve (AUC). The results show that as using DCT based Markov features has better performance than spatial domain based features. Moreover, when both domains are combined, the results have improved significantly. Reducing the feature space from 150 to 30 does not degrade much the performance when using combined features. The best performance is attained when $N = 50$. Increasing T from 3 to 4 slightly improves the results. The ROC curves depicting the changes of the FPR versus TPR are shown in Fig. 8 for spatial, DCT and combined based Markov features. These results are averaged over 20 runs of the experiment. The ROC curve for combined features is very close to the upper-left corner indicating the highest performance with

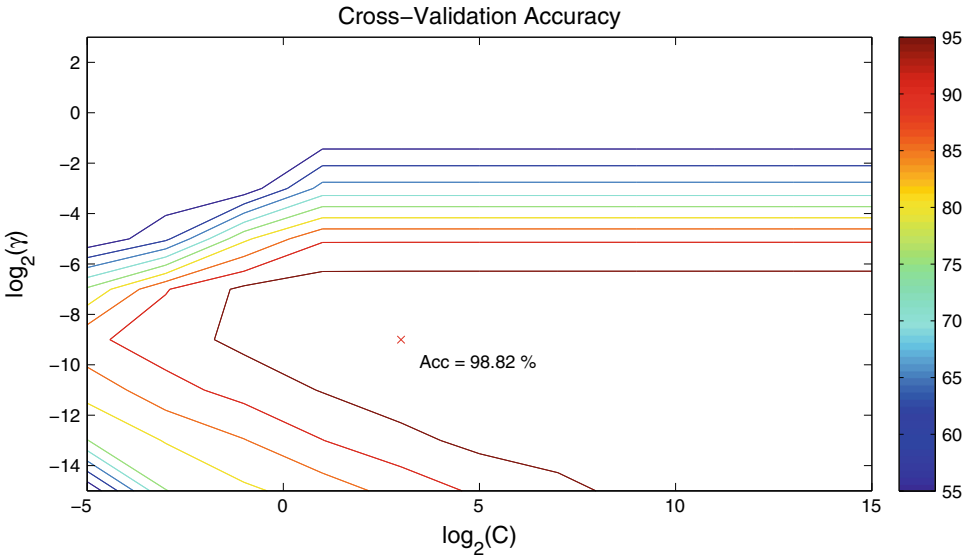

Fig. 7 Grid search for tuning the SVM parameters for $T = 4$

Table 2 Summary of results for Markov features with threshold $T = 3$ and 4

Feature	Dimensions	$T = 3$				$T = 4$			
		Accuracy	TPR	TNR	AUC	Accuracy	TPR	TNR	AUC
Spatial	150	0.7752	0.7796	0.7709	0.8543	0.7615	0.7666	0.7565	0.8378
	100	0.7737	0.7840	0.7636	0.8455	0.7708	0.7774	0.7643	0.8537
	50	0.7740	0.7902	0.7582	0.8371	0.7741	0.7874	0.7612	0.8575
	30	0.7642	0.7833	0.7456	0.8346	0.7668	0.7873	0.7467	0.8425
DCT	150	0.8883	0.9062	0.8708	0.9528	0.8940	0.9056	0.8826	0.9573
	100	0.8864	0.9055	0.8676	0.9430	0.8958	0.9071	0.8847	0.9579
	50	0.8818	0.9040	0.8601	0.9483	0.8927	0.9074	0.8784	0.9577
	30	0.8775	0.9016	0.8539	0.9509	0.8940	0.9089	0.8795	0.9547
Spatial + DCT	150	0.9831	0.9862	0.9801	0.9986	0.9869	0.9889	0.9849	0.9993
	100	0.9815	0.9852	0.9779	0.9980	0.9881	0.9905	0.9860	0.9989
	50	0.9825	0.9868	0.9783	0.9976	0.9882	0.9906	0.9859	0.9989
	30	0.9803	0.9843	0.9764	0.9978	0.9847	0.9894	0.9801	0.9986

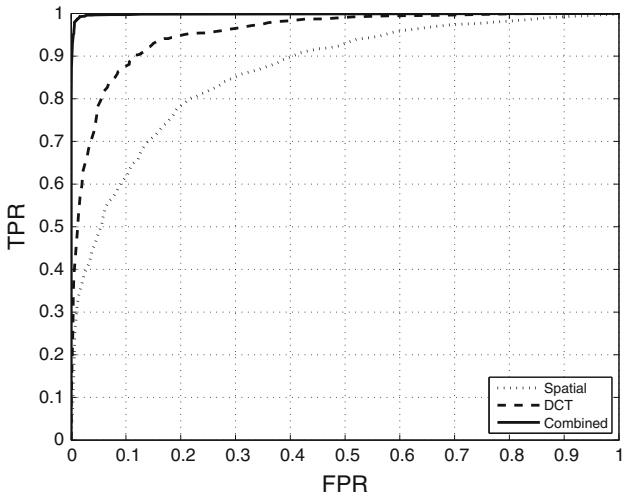

Fig. 8 ROC curves for Markov features with threshold $T = 4$ and $N = 50$

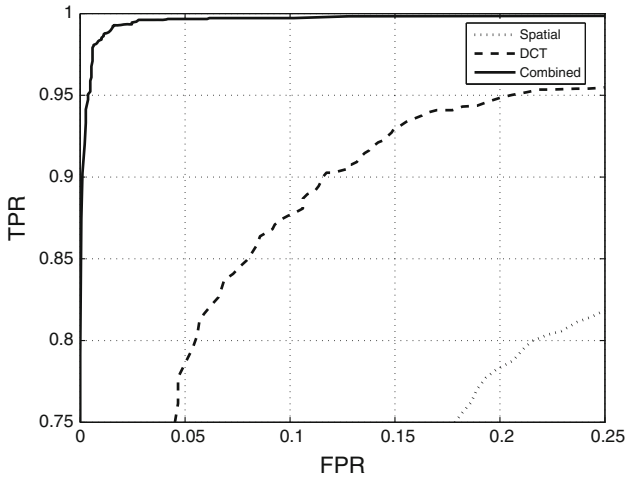

Fig. 9 Zoom-in of the *upper left part* of Fig. 8

area under the curve closer to 1. To clearly show the differences, the upper-left part of Fig. 8 is zoomed-in and the resulting plot is shown in Fig. 9.

Table 3 compares the proposed technique with $T = 4$ and $N = 50$ with other state-of-the-art methods in the literature on the same dataset. These results demonstrate the better performance of the proposed method yet at a reduced feature space. Figure 10 compares the ROC curves of the proposed technique with $T = 4$ and $N = 50$ with the best methods given in Table 3. We also tested other values of the threshold T and the attained accuracies are drawn in Fig. 11. This supports the choice of $T = 4$. We also tested our proposed technique to classify the original and forged images given in Fig. 1 and it was able to classify them correctly.

5 Conclusion

A blind technique for image splicing detection is proposed and evaluated in this paper. The idea is to combine Markov features calculated from edge images in the spatial domain and difference array of block DCT coefficients of the image. Feature reduction using PCA and an optimized SVM with RBF kernel as a classifier have proved an efficient combination. The results show that detection accuracy is tremendously increased when spatial features are combined with DCT based features. The test results validate the performance of our method as compared to the highest detection accuracy attained up till now from existing tampering detection methods on the same dataset and with the only 50 features which is also the lowest dimension used so for. The performance is assessed and compared in terms of detection

Table 3 Comparison with other methods

Methods	Dimensions	Accuracy (%)
Dong et al. [9]	61	76.52
Fu et al. [12]	110	80.15
Chen et al. [6]	120	82.32
Shi et al. [24]	266	91.87
He et al. [26]	100	93.55
Our method	50	98.82

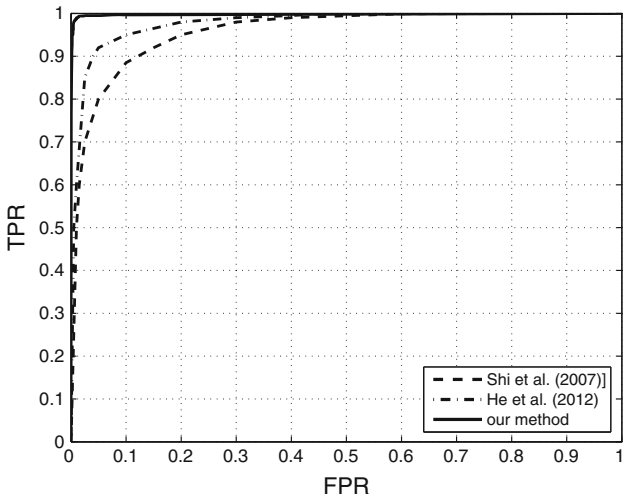

Fig. 10 ROC curves for the proposed technique with $T = 4$ and $N = 50$ as compared to the best methods in the literature given in Table 3

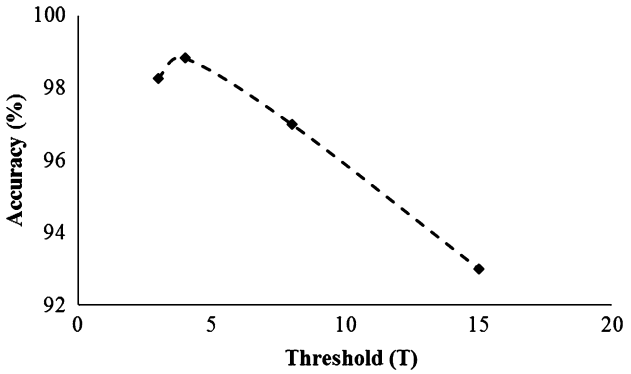

Fig. 11 Impact of varying T on the accuracy; only values at $T = 3, 4, 8$ and 15 are drawn

accuracy, true positive rate and true negative rate, ROC curve, and area under the ROC curve. With 50 features, the combined approach is able to achieve 98.82 % accuracy, 99.06 % TPR, 98.59 % TNR and 99.89 % AUC.

6 Originality and contribution

This paper proposes a novel effective method for image content authentication against image splicing forgery. With the wide availability of powerful editing tools and massive digital content online, this problem is becoming important due to its catastrophic consequences on authenticity. The essence of the proposed method is blind detection of image change by extending the Markov transition probability features from both spatial and frequency domains to reveal the dependencies between adjacent pixels when there is a change due to splicing. The characterization of each image by integrating various types of features can significantly lead to improving the tampering detection rate. However, due to the increased dimensionality of the feature, we applied PCA to select the most relevant features before building the detection model. We then developed an optimized support vector machine with RBF kernel to improve the detection accuracy. The experimental results demonstrated that the new method can yield considerably better detection performance, with more than 98 % accuracy, even with less number of features as compared with the state-of-the-art splicing detection methods tested on the same dataset.

Acknowledgments The authors would like to acknowledge the support provided by the Deanship of Scientific Research (DSR) at King Fahd University of Petroleum & Minerals (KFUPM) for funding this work through the Intelligent Systems Research Group (ISRG) under project No. RG1113-1&2.

References

1. Birajdar GK, Mankar VH (2013) Digital image forgery detection using passive techniques: a survey. Digit Invest 10(3):226–245
2. Borges PVK, Mayer J (2006) Analysis of position based watermarking. Pattern Anal Appl 9(1):70–82
3. Burges CJ (1998) A tutorial on support vector machines for pattern recognition. Data Min Knowl Discov 2(2):121–167
4. Change CC, Lin CJ (2010) Libsvm a library for support vector machines. http://www.csie.ntu.edu.tw/cjlin/libsvm. Accessed May 2013
5. Chen C, Shi YQ (2008) Jpeg image steganalysis utilizing both intrablock and interblock correlations. In: IEEE international symposium on circuits and systems (ISCAS), pp 3029–3032
6. Chen W, Shi YQ, Su W (2007) Image splicing detection using 2-d phase congruency and statistical moments of characteristic function. Proceeding of SPIE, San Jose
7. Cox IJ, Miller ML, Bloom JA (2002) Digital watermarking. Morgan Kaufmann Publishers Inc. San Francisco, CA
8. Cristianini N, Shawe-Taylor J (2000) An introduction to support vector machines and other kernel-based learning methods. Cambridge university press, Cambridge
9. Dong J, Wang W, Tan T, Shi YQ (2009) Run-length and edge statistics based approach for image splicing detection. In: Kim H-J, Katzenbeisser S, Ho ATS (eds) Digital watermarking. Springer, Berlin, pp 76–87
10. Farid H (1999) Detecting digital forgeries using bispectral analysis. In: Technical report. ftp://publications.ai.mit.edu/ai-publications/pdf/AIM-1657.pdf

11. Farid H, Lyu S (2003) Higher-order wavelet statistics and their application to digital forensics. In: Computer vision and pattern recognition workshop (CVPRW03), vol 8, pp 94–94
12. Fu D, Shi YQ, Su W (2006) Detection of image splicing based on Hilbert–Huang transform and moments of characteristic functions with wavelet decomposition. In: Shi YQ, Jeon B (eds) Digital watermarking. Springer, Berlin, pp 177–187
13. Guyon I, Weston J, Barnhill S, Vapnik V (2002) Gene selection for cancer classification using support vector machines. Mach Learn 46(1–3):389–422
14. He Z, Sun W, Lu W, Lu H (2011) Digital image splicing detection based on approximate run length. Pattern Recogn Lett 32(12):1591–1597
15. He Z, Lu W, Sun W (2012) Improved run length based detection of digital image splicing. In: Digital forensics and watermarking, pp 349–360
16. Hearst MA, Dumais S, Osman E, Platt J, Scholkopf B (1998) Support vector machines. IEEE Intell Syst Appl 13(4):18–28
17. Li L, Xue J, Wang X, Tian L (2013) A robust approach to detect digital forgeries by exploring correlation patterns. Pattern Anal Appl 1–15
18. Ng TT, Chang SF (2004) A model for image splicing. Proc IEEE Int Conf Image Process 2:1169–1172
19. Ng TT, Chang SF, Sun Q (2004) Blind detection of photomontage using higher order statistics. In: Proceedings of international symposium on circuits and systems (ISCAS), vol 5, pp 688–691
20. Ng TT, Chang SF, Sun Q (2004) A data set of authentic and spliced image blocks. In: ADVENT technical report, Columbia University, pp 203–204
21. Qazi T, Hayat K, Khan S, Madani S, Khan I, Koodziej J, Li H, Lin W, Yow KC, Xu CZ (2013) Survey on blind image forgery detection. Image processing. IET 7(7):660–670
22. Redi JA, Taktak W, Dugelay JL (2011) Digital image forensics: a booklet for beginners. Multimed Tools Appl 51(1):133–162
23. Shi YQ, Xuan G, Zou D, Gao J, Yang C, Zhang Z, Chai P, Chen W, Chen C (2005) Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network. In: IEEE international conference on multimedia and expo ICME
24. Shi YQ, Chen C, Chen W (2007) A natural image model approach to splicing detection. In: Proceedings of the 9th workshop on multimedia and security, pp 51–62
25. Zhao X, Wang S, Li S, Li J (2012) A comprehensive study on third order statistical features for image splicing detection. Digit Forensics Watermarking 243–256
26. Zhongwei H, Lu Wei Sun W (2012) Digital image splicing detection based on markov features in DCT and DWT domain. Pattern Recogn 45(12):4292–4299