Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 171 (2020) 369–378

Procedia Computer Science

www.elsevier.com/locate/procedia

Third International Conference on Computing and Network Communications (CoCoNet'19)

Image forgery detection based on statistical features of block DCT coefficients

Shilpa Dua[a,*], Jyotsna Singh[a], Harish Parthasarathy[a]

[a] *Multimedia Research Lab, NetaJi Subhas Institute of Technology, New Delhi, India-110078*

Abstract

Majority of the existing detection algorithms are able to deal with either type of forgery (splicing or copy-move). However, if we require a unified approach, we need to combine two previous works for each one of the alterations. In order to solve this problem, the authors present a new algorithm for the detection of splicing and copy-move forgery in the same instance. In this paper, a forgery detection technique is proposed which exploits the artifacts originated due to manipulations performed on JPEG encoded images. In JPEG compression technique, an image is divided into non-overlapping blocks of size 8×8 pixels and discrete cosine transform (DCT) coefficients are evaluated for each block independently. When a JPEG compressed image is tampered, there is a change in the statistical properties of AC components of block DCT coefficients. To capture this change, we propose to use standard deviation and count of non-zero DCT coefficients corresponding to each of the AC frequency components independently. The images are cropped by removing a few rows and columns from the top left corner and suggested features are evaluated for test image and its cropped version. The extracted feature vector is used with the support vector machine (SVM) for the classification of authentic and forged images. Experiments are conducted on a standard dataset of pre- and post-processed forged images CASIA v1.0 and v2.0 to consolidate the theoretical concept of the proposed technique. Also, the comparative analysis is performed to showcase better detection rates compared with the state-of-the-art methods.

Keywords: copy-move forgery ; cropping ; discrete cosine transform ; splicing forgery ; standard devivation ;

1. Introduction

In today's world, the problem of multimedia tampering is being alleviated with the wide accessibility of equipments and technology to every common man. The digital images are considered as the major infor-

∗. Corresponding author. Tel. : +91-9717588164.
E-mail address: er.shilpadua@gmail.com

10.1016/j.procs.2020.04.038

mation carriers in today's digital world. A huge increase in the number of manipulated pictures raises a question on the credibility of information when the images are utilized as some official, medical or financial records or presented as fundamental proof to impact the judgment in the court of law. Hence, figuring out the integrity of a digital image has become one of the major concern. Digital image forensics deals with the investigation of an image authenticity as well as with the presence of manipulation. Image manipulation techniques can be classified as splicing and copy-move forgery. Both of the techniques manipulate an image but they differ from one another according to their practices. The splicing forgery [1] is created by combining two or more images whereas the copy-move forgery (cmf) [2] is created by copying a part of an image and pasted on the same image itself.

Most of the digital images are stored in JPEG format. In JPEG compression, the image is divided into non-overlapping blocks of 8×8 pixels. For each block, the discrete cosine transform (DCT) is evaluated and quantized using a standard quantization matrix. As the block discrete cosine transform (BDCT) is the key operation in JPEG compression, any kind of tampering in the image creates disturbance in local statistics of block DCT coefficients. The change in the local statistics of block DCT coefficients can be captured and used as an indication of the presence of forgery. Shi et al. [3] proposed an image splicing detection algorithm based on a natural image model containing moments of the characteristic function of wavelet subbands and Markov transition probabilities of difference 2-D arrays. These 2-D arrays were generated by applying a multi-size block discrete cosine transform on a given test image. Another splicing detection technique was given by He et al. in [4]. They captured the inter- and intra-block correlation between block DCT coefficients by expanding the original Markov features generated from the transition probability matrices in the DCT domain. Further, three kinds of dependencies among wavelet coefficients across positions, scales and orientations were characterized by constructing more features in the DWT domain. In order to reduce the computational cost, feature selection method SVM-RFE was used. Li et al. [5] proposed an image splicing detection technique based on Markov features in Quaternion discrete cosine transform (QDCT) domain. The main aim of introducing the QDCT domain was to make use of the whole color information. They extracted expanded Markov features from intra-block and inter-block between block QDCT coefficients matrices. Further, image classification was performed by utilizing SVM with a large number of obtained features.

The other image forgery technique is termed as copy-move forgery in which a patch of an image is copied and pasted onto the same image with an aim to create duplication or to conceal some existing objects. Inspite of being one of the most common image alterations, it is difficult to detect copy-move forgery with naked eyes if it is done with care. Fridrich et al. [6] proposed the first technique to detect cmf in which the DCT coefficients based features are extracted from small overlapping image blocks. The tampered areas were detected by performing similarity checks between lexicographically sorted feature vectors. However, the approach led to a number of false matches, when applied to images containing large identical textured regions. The authors in [7] proposed a similar approach in which they also extracted DCT coefficients as features for different block sizes. But the techniques suffered from high computational complexity and improper detection of tampered areas when post-processing operations were applied to the tampered images. Cao et al. [8] proposed another DCT based approach in which the original image was divided into fixed-size blocks and discrete cosine transform (DCT) was performed on each block. Each DCT block was denoted by a circle block and four features were extracted in order to reduce the dimension of each block. Finally, a matching algorithm was applied to lexicographically sorted feature vectors. Hayat and Qazi in [9] suggested a cmf technique based on discrete wavelet transform (DWT) and DCT in which they extracted the approximation subband of DWT followed by the application of DCT to the overlapping image blocks. Further correlation coefficients were exploited for the comparison of the blocks. However, they have not evaluated the algorithm with different image operations.

All the techniques discussed so far, work well for either type of forgeries, copy-move or splicing. To best of our knowledge, very few techniques are reported in the literature which can work for both types of alterations. One of the integrated techniques proposed by Alahmadi et al. [10] exists which can perform copy–move and splicing forgery detection in the same instance. The method was based on local binary pattern (LBP) and discrete cosine transform (DCT). They transformed the LBP code of each block of the forged image into the

DCT domain and further evaluated the standard deviation of these DCT block coefficients. However, the technique was not evaluated for various post-processing operations. Recently, Prakash et al. [11] proposed another integrated technique for the detection of splicing as well as cmf. An enhanced threshold method based on Markov random process to extract the features from different color spaces was suggested in their study. However, they have not evaluated the scheme with a combined collection of authentic, spliced and cmf images for both of the datasets.

In this paper, we have presented a new integrated image forgery detection technique. The key idea is to exploit the variation in statistical properties of AC coefficients of the entire image by computing standard deviation and count of non-zero DCT coefficients corresponding to each AC frequency component independently. The suggested features are evaluated for the test image and its cropped version. The extracted feature vector is then used with the SVM classifier for identifying the modified/ unmodified images. The proposed scheme is experimented with various pre- and post-processed forged images available in the CASIA dataset [12], as showcased in the result section. We have compared our technique with all of the above-mentioned techniques in Section 3.3. The rest of the paper is organized as follows. Section 2 gives a detailed description of the proposed forgery detection algorithm and its mathematical explanation. In section 3, simulation results of the proposed approach are presented. Finally, Section 4 concludes the paper.

2. Proposed Forgery Detection Algorithm

This paper proposes a new forensic detector which is able to deal with either type of forgery (splicing or copy-move). Fig. 1 shows the structural outline of proposed forensic detector based on DCT-domain features. The detailed description of each step of the technique is discussed in the succeeding subsections. A systematic flow of proposed forgery detection method is stated in Algorithm 1.

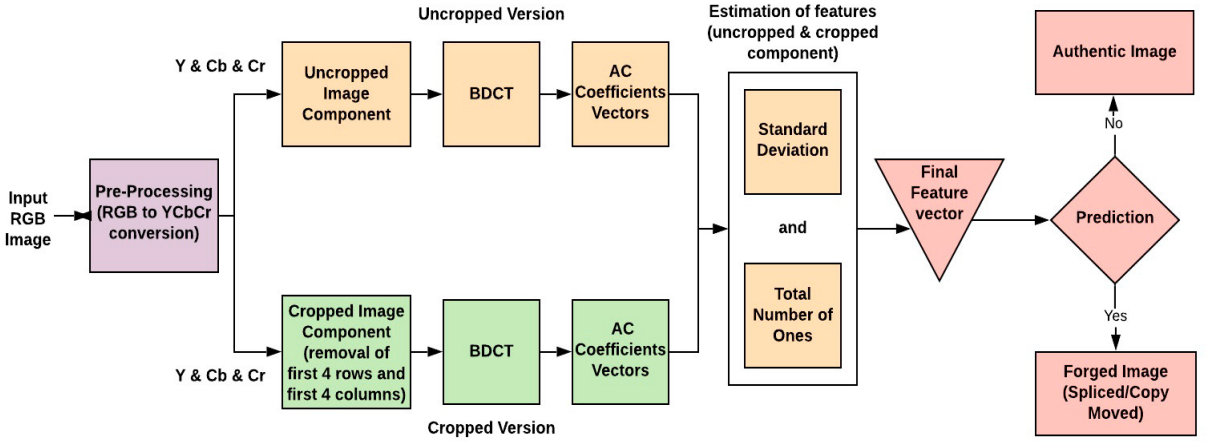


FIGURE 1. Design flow of the proposed forgery detection algorithm.

2.1. *Pre-processing*

In this study, the given test image is first converted into YCbCr color space in which Y denotes the luminance component, Cb and Cr are the representatives of the chroma channels. In YCbCr color model, most of the image information is contained in Y channel which results in better recognition of the luminance component over chroma components by human eyes. As most of the tampering traces are hidden in the chroma channels, one may consider an altered image as authentic due to the sensitivity of human vision. Hence, this paper exploits all of the three channels Y, Cb, and Cr and the Final feature is created by combining all of the extracted features from Y, Cb, and Cr components.

Algorithm 1: Classification of Authentic vs Forged Images

Input : Suspicious Image
Output: Classification Result(Authentic/Forged Image (either splicing or Copy-move))

Procedure
Convert RGB Image into YCbCr color space
for *each color sub-image (Y, Cb, Cr)* **do**
  Divide the sub-image into N non-overlapping blocks of size 8×8
  Apply DCT on each block
  for *each block* **do**
    Remove DC coefficient
    Arrange rest of the 63 AC coefficients of block into a column vector :
    $A_i = [a_{2,i}, a_{3,i} \cdots a_{64,i}]^T, \quad 1 \leq i \leq N$
  end
  Concatenate column vector of all N blocks of sub-image to form one matrix of size 63 × N :
  $M_A = [A_1 A_2 \cdots A_N] = \begin{bmatrix} a_{2,1} & a_{2,2} & \cdots & a_{2,N} \\ a_{3,1} & a_{3,2} & \cdots & a_{3,N} \\ \vdots & \vdots & \cdots & \vdots \\ a_{64,1} & a_{64,2} & \cdots & a_{64,N} \end{bmatrix}$
  Compute row-wise standard deviation s_k and number of ones o_k, $2 \leq k \leq 64$ of matrix M_A for each frequency component
  Form vector of standard deviation, $S = [s_2, s_3 \cdots s_{64}]^T$ and one's, $O = [o_2, o_3 \cdots o_{64}]^T$
  Crop sub-image by removing four rows horizontally and four columns from top left corner
  Form vector of standard deviation, S_C and ones O_C for cropped sub-image
  Concatenate four vectors to obtain feature vector of sub-image :
  $F_{sub-image} = [S^T \quad O^T \quad S_C^T \quad O_C^T]$
end
Combine each of the sub-image feature vector to form final feature vector of the test image :
$F_V = [F_Y \quad F_{Cb} \quad F_{Cr}]$
Apply feature vector F_V to SVM classifier for detection of Authentic/Forged Image
end Procedure

2.2. Modeling the tampering traces in DCT domain

Let Q be a two-dimensional matrix representing the color sub-image (Y or Cb or Cr) of the given test image. The sub-image of size J × K is divided into N non-overlapping blocks of size 8 × 8 pixels and 2D-DCT operation is performed on each block. It is important to note that each DCT Block consists of one DC coefficient and 63 AC coefficients. In this study, the focus is only on the behavior of AC coefficients and the DC coefficient is excluded. For the sake of clarity, the AC coefficients of each block are arranged into a vector i.e.

$$A_i = [a_{2,i}, a_{3,i} \cdots a_{64,i}]^T, \quad i \in \{1, 2, \cdots N\} \tag{1}$$

here, A_i represents the vector of length 63 and $a_{k,i}$ is the respective AC coefficient (i.e. $1 \leq k \leq 63$) in the block i. X^T denotes the transpose of the vector X. Note that, our main aim is to analyze the behavior of the complete candidate image hence each frequency should be considered independently for all the N Blocks.

Accordingly, we define matrix M_A by concatenating AC coefficient vectors of each block as

$$M_A = [A_1\ A_2 \cdots A_N] = \begin{bmatrix} a_{2,1} & a_{2,2} & \cdots & a_{2,N} \\ a_{3,1} & a_{3,2} & \cdots & a_{3,N} \\ \vdots & \vdots & \cdots & \vdots \\ a_{64,1} & a_{64,2} & \cdots & a_{64,N} \end{bmatrix}_{63\times N} \tag{2}$$

here, each row of the matrix corresponds to the specific AC frequency of all blocks for the complete sub-image and conversely, each column is the representation of all AC coefficients for the corresponding block of the sub-image. Then, row-wise standard deviation s_k is computed and arranged as a vector given as

$$S = [s_2, s_3 \cdots s_{64}]^T \tag{3}$$

here, $s_k = 1.4826 * MAD(a_{k,i}, a_{k,i+1} \cdots a_{k,N})$ is the standard deviation of kth AC coefficient of all blocks. In a similar manner, number of ones o_k for each row are calculated and defined as a vector as

$$O = [o_2, o_3 \cdots o_{64}]^T \tag{4}$$

here, $o_k = \sum_{i=1}^{N} ((a_{k,i}, a_{k,i+1} \cdots a_{k,N}) == 1)$ is the total number of ones for the kth AC coefficient of all blocks. It is computed by applying signum function to each row of the matrix. Signum function can be expressed as

$$sgn(a) = \begin{cases} 1 & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ -1 & \text{if } a < 0 \end{cases} \tag{5}$$

Next step is to obtain the cropped version of the given sub-image by removing first 4 rows and 4 columns from top left corner. Then all the steps described above for uncropped version (i.e. (1)-(5)) are repeated to compute standard deviation vector S_c and one's vector O_c for each row of AC Coefficients matrix of cropped sub-image. The feature vector of sub-image is then derived as

$$F_{sub-image} = [S^T \quad O^T \quad S_C^T \quad O_C^T] \tag{6}$$

In order to obtain the final feature vector (F_V) of the candidate image, each of the feature vector obtained through three sub-images (Y, Cb and Cr) is concatenated as

$$F_V = [F_Y \quad F_{Cb} \quad F_{Cr}] \tag{7}$$

The test image under consideration may be a genuine or fake image (either spliced or copy-move forged). Fig. 2(a, b, c) shows an example of an authentic, copy-moved and spliced images respectively. Let, F_V^A, F_V^C

and F_V^S represents their corresponding feature vectors. The difference vectors are then computed as

$$D_V^{AC} = F_V^A - F_V^C \quad and \quad D_V^{AS} = F_V^A - F_V^S \tag{8}$$

here, D_V^{AC} denotes the difference between the authentic and copy-moved image feature vector and D_V^{AS} is the difference between authentic and spliced image feature vector. The corresponding histogram plots of both of the difference vector are presented in Fig. 2(d, e). It can be observed that there is a noticeable difference in the features in both cases. Hence proposed feature vector extracted from the test image is considered as a discriminative feature and can be exploited for image classification.

(a) (b) (c) (d) (e)

FIGURE 2. shows (a) authentic image (b) copy-moved image (c) spliced image (d,e) histogram plots of D_V^{AC} and D_V^{AS} respectively.

2.3. ***Image classification***

Detection of image forgery is a two-class problem i.e. authentic vs. forged (spliced or copy-moved). In our scheme, we have employed a support vector machine (svm) as an image classifier as it has shown promising performance results in many applications.

3. Simulation Results

This section first presents an overview of the image dataset and performance metrics. Then, an extensive set of experiments are carried out to examine the robustness of the proposed approach against forgery type, size of the altered region and various pre- and post-processing operations such as rotation, resizing, blurring, etc. Finally, a comparative analysis is performed to showcase the detection performance of the proposed detector in comparison to the existing detectors.

3.1. ***Image dataset***

The proposed approach is evaluated on tampered image dataset CASIA v1.0 and v2.0 [12] constructed by the Institute of Automation Chinese Academy of Sciences which is considered to be more challenging and realistic dataset for manipulation detection. In CASIA v1.0, there is a total of 1721 images in which 800 images are authentic and 921 images are tampered color images of size 384×256 and all are in JPEG format without any post-processing. On the other hand, CASIA v2.0 consists of multiple sized images with various post-processing applied across edges. CASIA v2.0 consists of 7491 authentic and 5123 forged color images with size varying from 240×160 to 900×600 pixels. Also, the images are available as uncompressed as well as in JPEG format with different quality factors.

3.2. ***Performance metrics***

The receiver operating characteristic (ROC) curve is used to visualize the classification ability of the proposed scheme and is plotted between true-positive rate (T_{PR}) and false-positive rate F_{PR} i.e. high true-positive rate (T_{PR}) and low false-positive rate (F_{PR}) depicts the higher classification ability as the apex

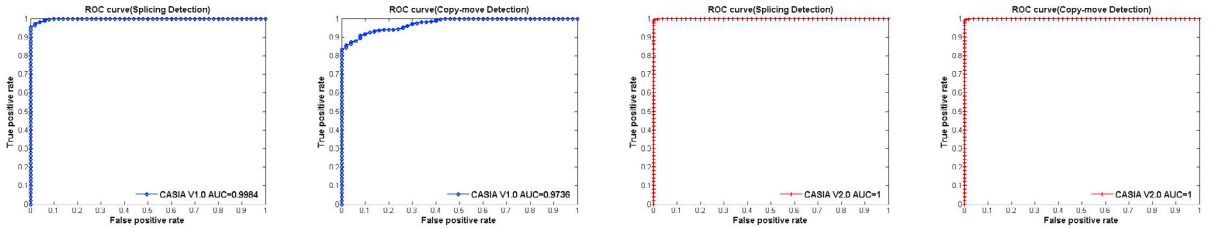
of the curve will be closer towards the top left corner. The commonly adopted performance measures are defined as

$$Accuracy = \frac{(TP+TN)}{(TP+TN+FN+FP)}, \quad T_{PR} = \frac{TP}{(TP+FN)}, \quad T_{NR} = \frac{TN}{(TN+FP)} \tag{9}$$

here, TP (true positive) is the number of forged images classified as forged; FN (false negative) is the number of forged images classified as authentic; TN (true negative) is the number of authentic images classified as authentic; and FP (false positive) is the number of authentic images classified as forged ones.

3.3. *Simulations*

— **Different types of forged images :**
In the first experiment, the overall performance of the proposed method is analysed with both kinds of tampering. For this, balanced sets of authentic as well as forged (spliced or copy-moved) images are constructed by selecting images from CASIA v1.0 and v2.0 dataset respectively. Fig. 3 shows the corresponding ROC curves of the proposed method. As can be inferred from the plots that the technique performs considerably well with CASIA v2.0 images altered by splicing as well as copy-move forgery. However, in the case of CASIA v1.0, the detection rate is comparable in the case of spliced images but degrades a bit in the case of cmf.



(a) (b) (c) (d)

FIGURE 3. ROC curves of (a) splicing and (b) copy-move forgery detection with CASIA v1.0 (c) splicing and (d) copy-move forgery detection with CASIA v2.0 image datasets respectively.

— **Different sizes of forged regions :**
In the next experiment, different sets of test images having different sizes of altered regions such as small, medium and large for both types of forgeries are evaluated.

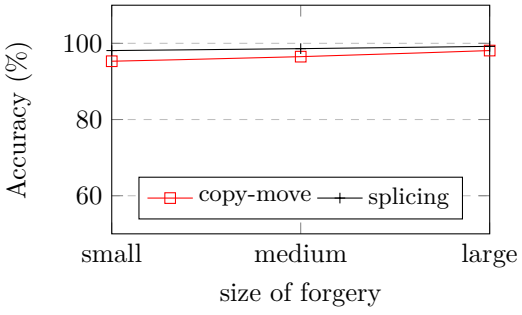


FIGURE 4. Detection performance of proposed method with CASIA v2.0 for different sizes of forgery.

Fig. 4 depicts the detection accuracy of the method in case of spliced as well as copy-moved images taken from casia v2.0 image dataset. It is evident from the plot that the detection rates are consistent irrespective of the size of the forged area.

— **Pre-processed forged images :**
To test the robustness of the proposed algorithm, the technique is tested against different types of pre-processing operations such as rotation (R), deformation (D), resizing (Rz) applied to the altered area before pasting it to the target image. Two different sets are created by selecting images from casia v1.0 and v2.0 dataset respectively. Fig. 5 (Left) shows the detection result of the proposed scheme. It can be analysed that the performance of our method is better in case of casia v2.0 with all operations. However, the detection rate deteriorates a bit in the case of CASIA v1.0.

— **Post-processed forged images :**
One method to conceal the forged region is to apply post-processing operations on the tampered image. The algorithm is also tested against post-processing operations such as blurring operation along the boundary (B) and blurring operation other than boundary area of the tampered region (O) applied after cut and paste operation. Fig. 5 (Right) shows the detection performance of the technique by performing experiments with CASIA v2.0. It is evident that the proposed detector is having comparable performance in the case of all operations for spliced as well as copy-move forged images.

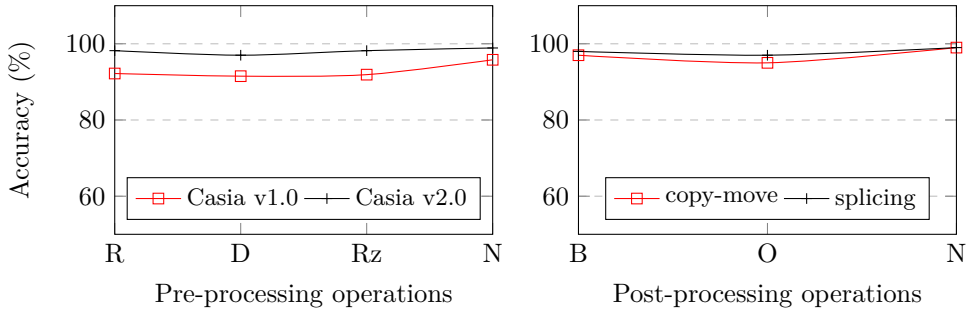


FIGURE 5. Detection performance of proposed method **Left :** with CASIA v1.0 and v2.0 for different pre-processing operations, **Right :** with CASIA v2.0 for different post-processing operations.

— **Comparative analysis :**
Next, the comparative performance of the proposed technique has been analysed in detail by comparing it with some of the pre-existing splicing detection techniques. Table 1 reports the detection rates with CASIA v2.0 image dataset. It can be observed from the table that the proposed scheme outperforms the other three methods by achieving excellent accuracy in discriminating authentic and spliced images.

TABLE 1. Comparative analysis of different splicing detection algorithms.

Methods	Detection Accuracy(%)
Shi et al. [3]	84.86
He and Lu et al [4]	89.76
Li et al. [5]	92.38
Our Method	99

To ensure the validity and fairness of the proposed algorithm, a comparison between our method and some state-of-the-art image duplication detection methods should be done. We have considered three already existing cmf detection algorithms. Their corresponding detection rates are reported in Table 2. As expected, the proposed method achieves much better detection accuracy with CASIA v2.0 as compare to other techniques in discriminating authentic and duplicated images.

Table 2. Comparative analysis of various duplication detection algorithms.

Techniques	Detection Accuracy(%)
Cao et al. [8]	72.77
Hayat et al. [9]	73.62
Prakash et al. [11]	87.5
Our Method	98

In this experiment, the comparative analysis is performed on the proposed method and some of the integrated techniques already reported in the literature. Alahmadi et al. [10] evaluated his method for splicing detection with both the datasets CASIA v1.0 and v2.0 respectively. They have also experimented with the mixed collection of both types of forged images taken from CASIA v1.0 and v2.0 dataset. Later, Prakash et al. [11] has proposed a forgery detection technique and analysed performance for spliced images taken from CASIA v1.0 and v2.0 and copy-move forged images from CASIA v1.0. We have evaluated our scheme for all the possible cases reported in Table 3. It can be seen that we have achieved better detection results with CASIA v2.0 for all the mentioned cases of forgery. However, there is a slight decline in accuracy for CASIA v1.0 forged images. In general, the technique performs considerably well and is able to detect both forgeries with good detection rates.

Table 3. Comparative analysis of proposed method with other pre-existing integrated methods.

	Spliced Images		Copy-Moved Images		Mixed Images	
Methods	Casia v1.0	Casia v2.0	Casia v1.0	Casia v2.0	Casia v1.0	Casia v2.0
Alahmadi et al. [10]	97.5	-	96.3	-	97.0	97.5
Prakash et. al. [11]	99.45	98.89	87.5	-	-	-
Our Method	96	99	92	98	93.2	98.3

Previous experiments were conducted by keeping in view the type of forgery. Next, we have evaluated the algorithm's performance by making a comparison between various classification techniques. A number of approaches exist in literature having diverse learning machines. Wu et al. [13] suggested an image forgery detection scheme named ManTra-Net which was a fully convolutional network. The technique performed self-supervised learning to learn robust image manipulation traces from 385 image manipulation types. In [14], the authors proposed an algorithm that exploits the characteristic footprints by different camera models left on images. Convolutional neural network (CNN) was utilized to extract characteristic camera model features from image patches. Further, the extracted features were analysed by iterative clustering techniques. Bunk et al. [15] proposed two different techniques for image forgery detection based on resampling artifacts with deep learning. Table 4 presents the comparative analysis of our method with the above-mentioned techniques utilizing different learning machines. It can be analysed from the table that the proposed method gives much better detection rates than the existing techniques in differentiating between authentic and forged images.

Table 4. Comparative analysis of of proposed scheme with other state of art schemes having diverse learning machines.

Learning Machines	Detection Accuracy(%)
Wu et al. (ManTra-Net) [13]	81.7
Bondi et al. (CNN) [14]	90.8
Bunk et al. (LSTM) [15]	94.86
Proposed approach (SVM)	99

4. Conclusion

This paper presented a new forensic detector which is able to deal with splicing as well as copy-move forgery at the same time. The detector captures the changes occurred in the statistical properties of AC components of block DCT coefficients when either type of forgery takes place. Standard deviation and count of non-zero DCT coefficients corresponding to each AC frequency coefficient are computed from the test image and its cropped version. The extracted features are utilized for classification by support vector machine (SVM). The experimental results showed that the technique performs considerably well with standard dataset CASIA for both kinds of forgeries ; the achieved average detection rates are above 93% and 98% with CASIA v1.0 and v2.0 datasets respectively. The technique was also evaluated with a number of pre- and post-processed forged images ; the attained results validate the fact that the proposed method is robust and consistent. In summary, the proposed method not only classifies unaltered images from altered ones effectively but also capable of dealing correctly with any kind of manipulation.

Références

[1] H. Farid, Exposing digital forgeries from jpeg ghosts, IEEE Transactions on Information Forensics and Security 4 (1) (2009) 154–160. doi:10.1109/TIFS.2008.2012215.

[2] S. Dua, J. Singh, H. Parthasarathy, Rotation angle estimation of an image using least square method, in : 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), 2016, pp. 296–300. doi:10.1109/SPIN.2016.7566707.

[3] Y. Q. Shi, C. Chen, W. Chen, A natural image model approach to splicing detection, in : Proceedings of the 9th Workshop on Multimedia & Security, MM&#38 ;Sec '07, ACM, New York, NY, USA, 2007, pp. 51–62. doi:10.1145/1288869.1288878. URL http://doi.acm.org/10.1145/1288869.1288878

[4] Z. He, W. Lu, W. Sun, J. Huang, Digital image splicing detection based on markov features in dct and dwt domain, Pattern Recogn. 45 (12) (2012) 4292–4299. doi:10.1016/j.patcog.2012.05.014.
URL http://dx.doi.org/10.1016/j.patcog.2012.05.014

[5] c. li, Q. Ma, L. Xiao, M. Li, A. Zhang, Image splicing detection based on markov features in qdct domain, Neurocomputing 228. doi:10.1016/j.neucom.2016.04.068.

[6] A. J. Fridrich, B. D. Soukal, A. J. Lukáš, Detection of copy-move forgery in digital images, in : in Proceedings of Digital Forensic Research Workshop, 2003.

[7] M. H. Alkawaz, G. Sulong, T. Saba, A. Rehman, Detection of copy-move image forgery based on discrete cosine transform, Neural Comput. Appl. 30 (1) (2018) 183–192. doi:10.1007/s00521-016-2663-3.
URL https://doi.org/10.1007/s00521-016-2663-3

[8] Y. Cao, T. Gao, L. Fan, Q. Yang, A robust detection algorithm for copy-move forgery in digital images, Forensic science international 214 (2011) 33–43. doi:10.1016/j.forsciint.2011.07.015.

[9] K. Hayat, T. Qazi, Forgery detection in digital images via discrete wavelet and discrete cosine transforms, Comput. Electr. Eng. 62 (C) (2017) 448–458. doi:10.1016/j.compeleceng.2017.03.013.
URL https://doi.org/10.1016/j.compeleceng.2017.03.013

[10] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, H. Mathkour, Passive detection of image forgery using dct and local binary pattern, Signal, Image and Video Processing 11. doi:10.1007/s11760-016-0899-0.

[11] C. S. Prakash, A. Kumar, S. Maheshkar, V. Maheshkar, An integrated method of copy-move and splicing for image forgery detection, Multimedia Tools Appl. 77 (20) (2018) 26939–26963. doi:10.1007/s11042-018-5899-3.
URL https://doi.org/10.1007/s11042-018-5899-3

[12] J. Dong, W. Wang, T. Tan, Casia image tampering detection evaluation database, 2013, pp. 422–426. doi:10.1109/ChinaSIP.2013.6625374.

[13] Y. Wu, W. AbdAlmageed, P. Natarajan, ManTra-Net : Manipulation tracing network for detection and localization ofimage forgeries with anomalous features, in : Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2019.

[14] L. Bondi, S. Lameri, D. Guera, P. Bestagini, E. Delp, S. Tubaro, Tampering detection and localization through clustering of camera-based cnn features, 2017, pp. 1855–1864. doi:10.1109/CVPRW.2017.232.

[15] J. Bunk, M. J. Bappy, T. M. Mohammed, L. Nataraj, A. Flenner, B. Manjunath, S. Chandrasekaran, A. Roy-Chowdhury, L. Peterson, Detection and localization of image forgeries using resampling features and deep learning, 2017. doi:10.1109/CVPRW.2017.235.