Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 31, Issue 4, 2020 DOI: http://doi.org/10.23851/mjs.v31i4.899

Research Article **Open Access**

Image Splicing Detection Based on Noise Level Approach

Mohammed K. Alshwely*, Saad N. Alsaad

Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, IRAQ

*Contact email: mohammed.kassem1@outlook.com

Article Info

Received
04/09/2020

Accepted
26/10/2020

Published
20/12/2020

ABSTRACT

The rapid development in technology and the spread of editing image software has led to spread forgery in digital media. It is now not easy by just looking at an image to know whether the image is original or has been tampered. This article describes a new image splicing detection method based on noise level as a major feature to detect the tempered region. Principal Component Analysis (PCA) is exploited to estimate the noise of image and the K-means clustering for authentic and forged region classification. The proposed method adopts Columbia Uncompressed Image Splicing Dataset for evaluation and effectiveness. The experimental results for 360 images demonstrate that the method achieved an 83.33% for detecting tampered region this percentage represent a promising result competed with Stat-of-art splicing detection methods.

KEYWORDS: Splicing, Image Forgery Detection, Digital Forensics, PCA, K-Means, Noise Estimation And Multimedia Security.

الخلاصة

أدى التطور السريع في التكنولوجيا وانتشار برامج تحرير الصور إلى انتشار التزوير في الوسائط الرقمية. لذلك ليس من السهل الآن بمجرد النظر إلى صورة معرفة ما إذا كانت الصورة أصلية أو تم العبث بها. توضح هذه المقالة طريقة جديدة لاكتشاف تركيب الصور استنادًا إلى مستوى الضوضاء كميزة رئيسية لاكتشاف المنطقة المزورة. يتم استغلال تحليل المكونات الرئيسية (PCA) لتقدير ضوضاء الصورة ومصنف K-means لتصنيف المنطقة الأصلية والمزورة. حيث اعتمدت هذه الطريقة على الصور غير المضغوطة من قاعدة بيانات كولومبيا من اجل التقييم والفاعلية. توضح النتائج التجريبية لـ 360 صورة ان هذه الطريقة قد حققت نتيجة نسبة 83.33% في قابلية الكشف عن التزوير حيث تمثل هذه النسبة نتيجة واعدة تتنافس مع الطرق الحديثة للكشف عن التزوير في الصور.

INTRODUCTION

With the unfold of mobile devices and social networks, it's simple to acquire photos and share them on the web at anytime and anyplace. Forgers can efficiently create and spread forged images that don't imply that they are forged images produced by advanced image editing tools. Consequently, image forgery and forensic techniques to identify the effects of tampering with digital images become a serious problem and have been attracted considerable interest in research and industry [1] [2]. Among the techniques of tampering, copy-move (cloning), splicing, and removal methods are methods that considered as the most common manipulation. Copy-move is copied part of the image and pasted into the same one, while splicing involves cut a region from an image and pasted it into another, removal is removing part of an image in order to change the original. Sometimes post-processing is applied to the image such as Gaussian smoothing after the process of tampering. Figure 1 shows an example of this manipulation. It is apparent it's hard for humans to identify areas that have been tampered [3]. The rest of the paper is organized as follows: Section two presents the related work and section three is the proposed work details. The experimental results are devoted in Section 4, followed by a conclusion in Section 5.

We will focus in this paper on the domain of image splicing which is one of the most technique that used to alter or modify the digital image. Image splicing involves composing or combining of two images or more from a different source in order to create the tampered image. Image forgery detection approaches can be divided into active

and passive detection, for splicing detection the passive approaches will be used where there is no prior information known about the history of the forged image [4].

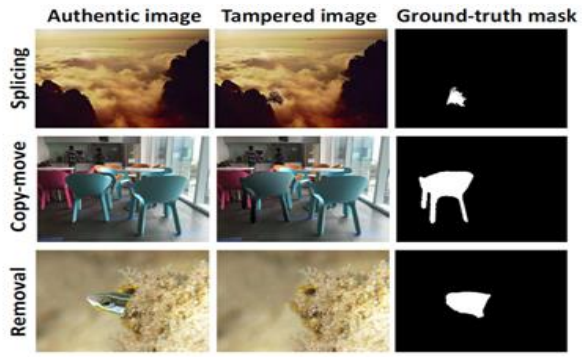

Figure 1. Examples of images that were tampered with and subjected to different manipulation techniques [3].

MATERIALS AND METHODS

Image splicing forgery

Image splicing is one of the most simple and popular types of image forgery. Image splicing involves the process of replace part of an image with part of another one [5]. Figure 2 illustrates an example of image splicing that is circulated in social media. The left image is the tampered while the right one is the original.

Figure 2. Example of image splicing [6].

Post-processing such as scaling and rotation are sometimes applied on splicing image in order to make it more realistic. In some cases, the spliced image can be identified by the experts just by looking at it. However, the experienced forger can make image forgery very elegant which make it almost impossible to say anything about the originality of the image by just looking at it [7].

Image splicing forgery detection methods

Due to the Vulnerability of digital image to malignant manipulation than the non-digital counterpart, the determining of image authenticity and detection of the manipulated part becomes an important domain for many researchers.

Splicing detection has various types such as illumination color estimation which depends on the light inconsistencies of the digital image where the spliced region and the original image will have different light conditions. Detection based on the inconsistency of noise level which relays on the fact that each image taking by digital Camera will contain a certain type of noise that different from other cameras. Also, the consistency of physical-based features between different parts of a single image such as related natural scene the properties of an imaging device such as the characteristics of the digital camera can be used as in detecting the spliced region of an image [5]. The main stages of the image splicing detection are pre-processing, feature extraction, classification, and post-processing. The general framework of image splicing forgery detection is shown in figure 3 below.

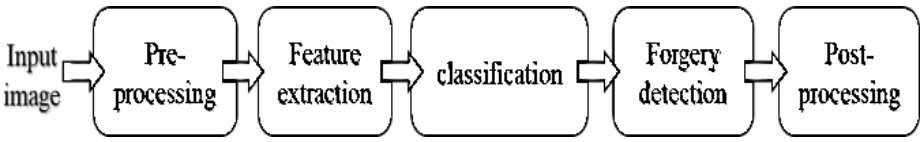

Figure 3. the general framework of image splicing detection [8].

Pre-processing: in the pre-processing, the image first converted from RGB to grayscale and divided into an overlapping or non-overlapping block.

Feature extraction: the process of feature extraction is the process of extracting the important features from the input image. Feature extraction aims to quantify specific representations of data to extract the odd information due to the image splicing detection aims to find the different features from within the image.

Classification: depending on the features extracted from the image, the classifier is selected or designed. Sometimes pre-processing is required for the extracted feature like reduce their dimension. The only purpose of the classifier is to classify the region of the image either as original or tampered. Such classifiers are the neural network, support vector machine (SVM), linear discriminant analysis (LDA), and K-mean [8].

Post-processing: the post-processing stage is helps to reduce the false detection of the tampered regions to improve the accuracy of the forgery detection.

RELATED WORK

In In the last decade, the increased use of the Internet and social media, it has become easy for users to exchange a forged image. The need for such studies and research has emerged as a result of widespread fraudulent images [8]. In the course of this paper, image splicing as one of the most technique used in tampering will be covered.

Zhang et.al. [10] proposed a method for image splicing detection try that uses Markov model in block discrete cosine transform (BDCT) and contourlet transform domain of gray channel of the colored image is used as feature extraction method which produces a large number of features that can be handled using Support Vector Machine Recursive Elimination (SVM-RFE). Finally, the Support Vector Machine (SVM) is used to determine the spliced and the authentic region.

Kumar et al. [11] presented an image splicing detection model. The features are extracted from Discrete Mayer Transform and Discrete Cosine Transform (DCT) to be used in Markov model. A threshold enhancement method is used to reduce the information as well as the computation cost. Finally, a support vector machine (SVM) classifier also used to classify the spliced region from the authentic region.

Cozzolino et al. [12] proposed a splicing detection method from the single image where they cast splicing localization as detection of the anomaly regions and the features extracted from the spliced regain are considered as anomalies. The extracted noise from the image used as a feature and introduced to an autoencoder that generates an implicit data model, this data model then labeled as pristine data while the spliced region is classified as anomalous by iterating discriminative feature labeling and autoencoder.

Kaur et al. [13] propose a blind technique for detecting using (DWT) to get the low-level coefficient and approximation coefficient, and the features extracted from this coefficient using Local Binary Pattern (LBP).

The method proposed by Pomari et al. [14] adopted a combination of high representative power of illuminant map and convolutional neural network (CNN) as a way of direct learning from available training data. The proposed method eliminates the laborious feature engineering process which improves forgery localization.

Moghaddasi et al. [15] proposed an approach based on the merging of the Singular Value Decomposition (SVD) features and (DCT) coefficient as a feature extraction method. The kernel PCA is adopted as a method for feature reduction, then the features introduced for the Support Vector Machine (SVM) as a classifier.

Finally, a method proposed by Yıldırım et al. [16] based on an expert system that depends on statistical and textural characteristics to detect image forgery. These characteristics extracted from the high-level sub-bands of the Stationary Wavelet Transform (SWT) domain. The statistical features are extracted from three sub-bands by the Markov model. The SVM is used as a classifier.

In this paper, a splicing detection method based on noise varieties is proposed and implemented using principal components analysis

PROPOSED METHOD

The basic of all image splicing forgery detection algorithm is to find the anomalies region in the suspicious image, for example, the difference in the noise level or light condition. The proposed method depends on the noise level to detect image forgery. Image noise is a disturbance that exists in every image captured using digital sensors. The noise level of an image normally has the same characteristics. These characteristics basically are depending on several factors such as the model of the camera and the exposure time during the acquisition time, therefore if there any variation observed in the characteristics of the noise in a specific area of an image it will be an indicator of manipulation. The proposed method of this paper depends on the noise characteristics of an image for splicing detection. Figure 4 depicts the general framework. It is composed of three stages: preprocessing, noise level estimation and K-means clustering.

Stage 1: includes converting a color image to be tested to grayscale (equation1) and then dividing the grayscale image into a non-overlapping block with a fixed size such as 64×64

$$Y=0.299R+0.587G+0.114B \quad (1)$$

Where R, G, B three-color and *Y* is the luminance component.

In Stage 2 (Noise level estimation), for each block, the noise information is estimated using Principal Component Analysis (PCA). While the K-means clustering stage is introduced to classify these blocks according to the level of noise into two clusters and the cluster with a fewer number of the block is regarded as the spliced region.

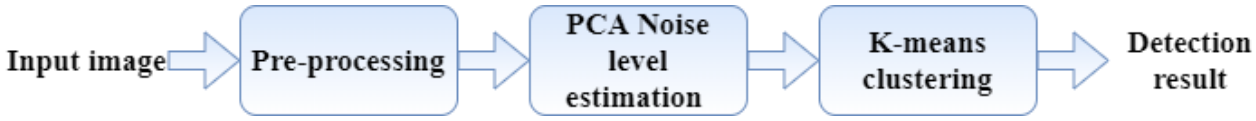

Figure 4. general framework of the proposed method.

Estimation of noise level

In this work PCA based method in [16] is used to get noise information for each block resulted from the preprocessing stage. Algorithm (1) is processed to calculate the estimation of noise variance for each block resulted from the preprocessing stage. It started with a specific estimation value (upper bound of the block). This upper bound is also used as a preliminary value for the repetitive procedure that refines the estimation variance which is performed in GetNextEstimate function in the algorithm (2). The process of the algorithm is iterated until the differences between the current estimation and the next estimation is negligible. Algorithm (2) is used the upper bound and the estimation noise variance as input to calculate the next estimation noise value. To clarify the algorithm, it is useful to offer the following notes:

1- The algorithm is based on *Assumption 1:* Let *m* be a predefined positive integer number. The information in noise-free image **x** is redundant in the sense that all $\mathbf{x}_i$ lie in subspace $V_M{-}m \subset \mathbb{R}^M$, whose dimension $M{-}m$ is smaller than the number of coordinates *M* mentioned in [17] and [18].

2- The algorithm divides each block *Y* (size S*S resulted from preprocessing stage) into overlapping patches of size M*M. The number of patches (N) is calculated according to equation 2.

$$\boldsymbol{N = (S - M1 + 1)(S - M2 + 1)} \quad (2)$$

3- A subset Y_p of the patches is selected by discarding the patches with the largest variance. This satisfied by equation 3, where Q(p) is p-quantile and P started from 1to 0.1 and decreasing 0.05 [16]

$$\boldsymbol{Y_p = (y_i | s^2(y_i) \le Q(P), i = 1, .., N)} \quad (3)$$

4- Principal component analysis (PCA) is performed on *Yp* to generate values $\lambda\mathbf{Y}$,1,... ., $\lambda\mathbf{Y}$, *M*.

5- Asumption1 is satisfied when the following condition is true:

$$\boldsymbol{\lambda_{Y,M-m+1} - \lambda_{Y,m} < T\sigma^2/\sqrt{N}} \quad (4)$$

6- the assumption 1 is true the author of [16] proved that equation 5 is true

$$\boldsymbol{lim_{N\to\infty} E\left(\left|\lambda_{Y,n} - \sigma^2\right|\right) = 0} \quad (5)$$

Where σ^2 is the estimation variance noise. The equation above refers that estimation accuracy is proportional to N.

7- The values of M_1, M_2, C_0, m, and T are identified with value equal 5,5,3.1,7, and 49 respectively as in [17].

Finally, $\sqrt{\lambda_{y_p min}}$ is regarded as the noise level of the current iteration. Algorithm 2 iterated until the convergence is achieved i.e. the difference between two consecutive estimations is less than *1e-5* as in [9].

Algorithm 1: PCA Noise estimation

Input: for each *y* resulted from preprocessing stage

Outputσ^2_{est}: the estimated noise variance

1. Start
2. i_{max}=*10*
3. compute the upper bound
$\sigma^2_{ub} \leftarrow \sigma^2 = 3.1Q(0.0005, y)$
4. set the upperbund to the estimated variance
$\sigma^2_{est} \leftarrow \sigma^2_{ub}$
5. for *i*=1 to i_{max} do
6. calculate the next estimation
$\sigma^2_{next} \leftarrow$ GetNextEstimate (y,σ^2_{ub}, σ^2_{est})
7. check if the estimated variance is equal to the

next estimation then return the estimated variance

if $\sigma_{est}^2 = \sigma_{next}^2$

8. return σ_{est}^2
9. Else return the value of the next estimate variance to the estimated variance

$$\sigma_{est}^2 \leftarrow \sigma_{next}^2$$

10. End for
11. Return σ_{est}^2
12. End.

Algorithm 2 Get Next Estimate

Input: for each *y* resulted from preprocessing stage

σ_{est}^2: the current value of the estimated noise variance

σ_{ub}^2: upper bound of the noise variance

Output: next estimate noise variance σ_{next}^2

Start

1. $p \leftarrow 1$ Set the value of p to 1
2. σ_{next}^2
3. while $p \geq p_{min}$
4. $Y_p = \{y_i \vee s^2(y_i) \leq Q(p), i = 1, \dots, N\}$
5. $\lambda_{yi} = ApplyPCA(Y_p)$ //compute the eigen value of the current block
6. set the eigenvalue to the next estimated variance

$\sigma_{next}^2 \leftarrow \lambda_{y,M}$

7. stop iterating if variance is already low

if $(\sigma_{next}^2 < 1e-5)$ then exit

8. else
9. if $\left(\lambda_{Y,M-m+1} - \lambda_{Y,M} < T\sigma_{est}^2\right)$ then
10. Return σ_{next}^2
11. End if
12. Decrease the value of p
13. $p \leftarrow p - 0.05$
14. End if
15. End while
16. Check the next estimation is greater than the value of the upper bound

if $\sigma_{next}^2 > \sigma_{ub}^2$ then

17. $\sigma_{next}^2 = \sigma_{ub}^2$
18. end if
19. return σ_{next}^2
20. end

EXPERIMENTAL RESULTS

Algorithms 1 and 2 have been implemented using MATLAB 2017. The Colombia image Splicing detection evaluation dataset [18] is used for evaluation. The dataset contains about 360 images taken with four different cameras: Canon G3, Nikon D70, Kodak DCS330 and Canon 350D Rebel XT. This dataset contain180 Spliced images that are created from combining two authentic images using Adobe Photoshop. The images with size from 757×568 to 1152×768.

Due to the spliced image created by combining two different images from two cameras and different settings they may have different levels of noise that can be used clue for tampering. Figure 5 shows a sample of eight spliced image and their detection result using the proposed method. The figure refers to accurate detection.

The experimental results show the ability to detect the true positive (TP) (the spliced image that detected correctly) forgery with accuracy about 87.66 % for Colombia image Splicing dataset while the true negative (TN) (the original image that detected as original) about 83.03% for the same dataset.

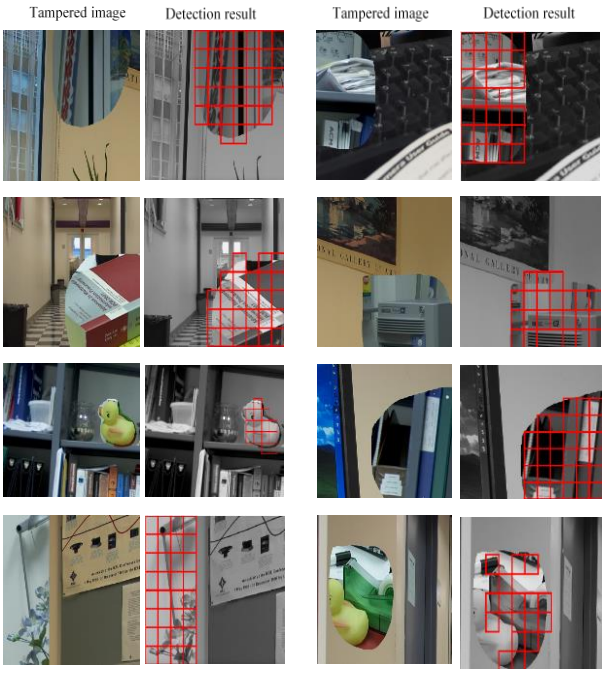

Figure 5. detection result for eight images splices from Colombia uncompressed image Splicing detection evaluation dataset [19].

The performance of noise-based methods is degrading significantly when the spliced image compressed heavily, so to overcome this limitation we suggest combining the noise-based method with the JPEG-based method this will help to increase the performance of detection. Also, such methods are affected by image texture which causes false detection in the result as shown in figure 6 that shows the result of high texture area. Generally, noise-based methods achieve satisfactory performance when the noise difference between the original and tampering areas is large enough.

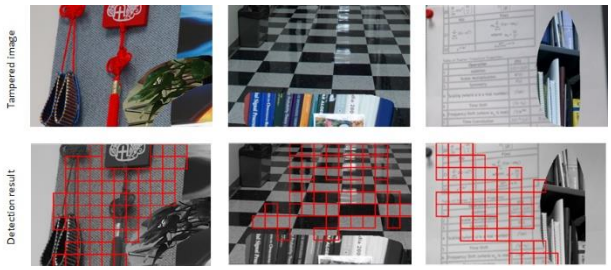

Figure 6. shows the image with high texture area**.**

CONCLUSIONS

Digital image forensic became a focus of attention to researchers. Image splicing forgery considered one of the common problems in the domain of digital image forensics. In this paper, we proposed a simple Splicing detection algorithm based on the fact that the spliced image will have different levels of noise. So, the spliced region can be detected depending on the noise level of the image. It is a PCA based noise level estimation. The experiment shows the ability of the proposed algorithm to detect forgery within the image even when the spliced part is scaled or rotated. This method indicates that the noise level can be used as a clue of image forgery. In general, the noise-based splicing detection method has a satisfactory performance when there are high differences between the original region and the spliced region is large enough.

ACKNOWLEDGEMENTS

I would like to thank Prof. Dr. Saad Najim AlSaad for his continued support and guidance during the management of this work. I would like also to express my appreciation to Mustansiriyah University, Faculty of Science, for their assistance and support in the study.

REFERENCES

[1] Wu, Y., Abd-Almageed, W., and Natarajan, P.: ‘Deep matching and validation network: An end-to-end solution to constrained image splicing localization and detection’, in Editor (Ed.)^(Eds.): ‘Book Deep matching and validation network: An end-to-end solution to constrained image splicing localization and detection’ (ACM, 2017, edn.), pp. 1480-1502

[2] Cozzolino, D., and Verdoliva, L.: ‘Noiseprint: a CNN-based camera model fingerprint’, IEEE Transactions on Information Forensics and Security, 2019.

[3] Zhou, P., Han, X., Morariu, V.I., and Davis, L.S.: ‘Learning rich features for image manipulation detection’, in Editor (Ed.)^(Eds.): ‘Book Learning rich features for image manipulation detection’ (2018, edn.), pp. 1053-1061K. Elissa, “Title of paper if known,” unpublished.

[4] Farid, H.: ‘Image forgery detection’, IEEE Signal processing magazine, 2009, 26, (2), pp. 16-25.

[5] Sekhar, C., and Sankar, T.: ‘Review on Image Splicing Forgery Detection’, International Journal of Computer Science and Information Security, 2016, 14, (11), pp. 471.

[6] https://gizmodo.com/that-viral-photo-of-putin-is-totally-fake-1796767457 [Accessed 21/07/2020].

[7] Meena, K.B., and Tyagi, V.: ‘Image Forgery Detection: Survey and Future Directions’: ‘Data, Engineering and Applications’ (Springer, 2019), pp. 163-194.

[8] Mushtaq, Saba, and Ajaz Hussain Mir. "Digital image forgeries and passive image authentication techniques: A survey." International Journal of Advanced Science and Technology 73 (2014): 15-32.

[9] Liu, Y., Zhu, X., Zhao, X., and Cao, Y.: ‘Adversarial Learning for Constrained Image Splicing Detection and Localization Based on Atrous Convolution’, IEEE Transactions on Information Forensics and Security, 2019, 14, (10), pp. 2551-2566.

[10] Zhang, Q., Lu, W., and Weng, J.: ‘Joint image splicing detection in DCT and Contourlet transform domain’, Journal of Visual Communication and Image Representation, 2016, 40, pp. 449-458.

[11] Kumar, A., Prakash, C.S., Maheshkar, S., and Maheshkar, V.: ‘Markov Feature Extraction Using Enhanced Threshold Method for Image Splicing Forgery Detection’: ‘Smart Innovations in Communication and Computational Sciences’ (Springer, 2019), pp. 17-27.

[12] Cozzolino, D., and Verdoliva, L.: ‘Single-image splicing localization through autoencoder-based anomaly detection’, in Editor (Ed.)^(Eds.): ‘Book

Single-image splicing localization through autoencoder-based anomaly detection' (IEEE, 2016, edn.), pp. 1-6.

[13] Kaur, M., and Gupta, S.: 'A passive blind approach for image splicing detection based on DWT and LBP histograms', in Editor (Ed.)^(Eds.): 'Book A passive blind approach for image splicing detection based on DWT and LBP histograms' (Springer, 2016, edn.), pp. 318-327.

[14] Pomari, T., Ruppert, G., Rezende, E., Rocha, A., and Carvalho, T.: 'Image splicing detection through illumination inconsistencies and deep learning', in Editor (Ed.)^(Eds.): 'Book Image splicing detection through illumination inconsistencies and deep learning' (IEEE, 2018, edn.), pp. 3788-3792.

[15] Moghaddasi, Z., Jalab, H.A., and Noor, R.M.: 'Image splicing forgery detection based on low-dimensional singular value decomposition of discrete cosine transform coefficients', Neural Computing and Applications, 2018, pp. 1-11.

[16] Yıldırım, E.O., and Ulutaş, G.: 'Augmented features to detect image splicing on SWT domain', Expert Systems with Applications, 2019, 131, pp. 81-93.

[17] Pyatykh, S., Hesser, J., and Zheng, L.: 'Image noise level estimation by principal component analysis', IEEE transactions on image processing, 2012, 22, (2), pp. 687-699.

[18] Zeng, H., Zhan, Y., Kang, X., and Lin, X.: 'Image splicing localization using PCA-based noise level estimation', Multimedia Tools and Applications, 2017, 76, (4), pp. 4783-4799.

[19] Hsu, Y.-F., and Chang, S.-F.: 'Detecting image splicing using geometry invariants and camera characteristics consistency', in Editor (Ed.)^(Eds.): 'Book Detecting image splicing using geometry invariants and camera characteristics consistency' (IEEE, 2006, edn.), pp. 549-552.