



Robust Image Forgery Detection Using Point Feature Analysis

Youssef William 
German University in Cairo
Cairo, Egypt
youssef.teryak@student.guc.edu.eg

Sherine Safwat 
German University in Cairo
Cairo, Egypt
sherine.safwat@guc.edu.eg

Mohammed A.-M. Salem 
German University in Cairo,
Ain Shams Univeristy
mohammed.salem@guc.edu.eg,
salem@cis.asu.edu.eg
Cairo, Egypt

Abstract—Day for day it becomes easier to temper digital images. Thus, people are in need of various forgery image detection. In this paper, we present forgery image detection techniques for two of the most common image tampering techniques; copy-move and splicing. We use match points technique after feature extraction process using SIFT and SURF. For splicing detection, we extracted the edges of the integral images of Y , C_b , and C_r image components. GLCM is applied for each edge integral image and the feature vector is formed. The feature vector is then fed to a SVM classifier. For the copy-move, the results show that SURF feature extraction can be more efficient than SIFT, where we achieved 80% accuracy of detecting tempered images. On the other hand, processing the image in YC_bC_r color model is found to give promising results in splicing image detection. We have achieved 99% true positive rate for detecting splicing images.

Index Terms—Image Forgery, Copy-Move Forgery Detection, Image Splicing, SIFT, SURF, Support Vector Machine (SVM), benchmark dataset, CASIA datasets, Gray Level Co-occurrence Matrix (GLCM)

I. INTRODUCTION

IN today's world, digital images are widely used in various domains such as; newspapers, scientific journals, magazines, and many other fields [25]. Unfortunately, today's digital technology made it easy for digital images to be forged due to the availability of the low cost photo editing software [17]. For example, during the incident of Hurricane Harvey, fake images were posted of sharks inside New York as shown in Figure 1. Another example, in Figure 2 as the cutout of the newspaper showed a forged photographs of Bill Clinton, and Saddam Hussein at the White House [9].

Of course, this can cause chaos and panic among the viewers of such digital images. In addition, it can cause erosion in people's trust towards images [20]. Thus, in order to recover people's trust towards digital images, it is important to develop new trustworthy techniques for digital images forgery detection.

Image forgery detection is such a complicated job. Nowadays, it became very difficult to detect whether an image is fake or not. According to Huynh, et al. image forgery detection is one type of the passive techniques that use blind algorithms

for tampering detection in the suspected image without using any prior information. Accordingly, they divided passive techniques into two types: copy-move and splicing [11].



Figure 1. Hurricane Harvey fake reports that were published in BBC in 2017

The copy-move is defined by copying region of an image and pasting it in another place in the *same* image, generally to hide unwanted parts of the image. On the other hand, image splicing is the process of copying a region of an image and pasting it in another place in *another* image. Thus, detection of tampered regions is done through searching for very similar regions in copy-move images and completely odd regions in spliced images [12].

In this paper, we are extracting the image features and analyzing it to detect the forged images and also determine the type of the forgery whether it is copy-move or splicing.



Figure 2. Example of realistic looking forgery

Our work is test on multiple datasets. The rest if the paper is organized as follows; in Section II, we present the literature review for the copy-move and image splicing forgery detection. Section III, introduces our Methodology for both copy-move and splicing along with the datasets used. Experimental results for both techniques are elaborated in Section IV. In Section V we discuss the results and the limitation of the proposed algorithms. Finally, in Section VI we drive the conclusions.

II. LITERATURE REVIEW

This section summarizes some of the work done in copy-move and splicing detection as follows.

A. Copy-Move Forgery Detection

The copy-move attack is one type of tampering in which a region of the image is copied and pasted in another area in the same image to cover an important image feature. In [25] a technique for detecting copy-move forgery is presented based on SURF and KD-Tree for multidimensional data matching. Shivakumar et al. designed a system to identify the duplicated areas, then extracted key points in the forged areas and matched them among the SURF features, thus determined the possibility of forgery.

Alberry et al. introduced a fast technique optimizing SIFT and fuzzy c-means clustering for copy-move forgery detection. First, the algorithm detected and matched the key points in the image and clustered the points based on their descriptors using c-means algorithm. Their algorithm could successfully come over the computational complexity in the matching stage after using the clustering algorithm [5].

Pasquini et al. designed an empirical system to verify online news by analyzing images from news article. The system identified the set of meta-data visuals related to the same topic and presented some common visual elements. After that, the data set was compared with many websites with the same topic. Thus, the system the could differentiate between the images and output the fake one [20].

In [9] Fridrich et al. succeeded in detecting the forged parts even when the copied areas were skillfully enhanced and merged with the background and saved in the lossy JPEG format. They introduces a novel correlation between the original image segment and the pasted part to be used as a basis for a successful detection for the copy-move.

The paper [7] examined several block-based methods to detect the copy-move forgery. Bayram et al. showed their time complexity and robustness in the results. They discussed Discrete Cosine Transform (DCT), Fourier Mellin Transform (FMT) and Principal Component Analysis (PCA). The results were good on any JPEG image, but the algorithm is limited to non-rotated or scaled objects. However, they could improve the efficiency of copy-move forgery techniques by counting

bloom filters, especially when the image quality is high.

Ryu et al. [22] proposed a forensic technique to localize duplicated image regions based on Zernike moments of small image blocks. They utilized the characteristics of rotation in variance to reliably unveil duplicated areas after random rotations. By examining the image, they designed a new block matching operation centered on locality-sensitive hashing and decrease fake positives. Their experiments indicated high robustness for JPEG compression, blurring, additive white Gaussian noise, and moderate scaling.

The work done [15] by Kakar et al. proposed a novel technique based on transform-invariant features for copy-move detection. The results provided efficacy of this technique in detecting copy-move forgeries with translation, scaling, rotation, flipping, lossy compression, noise addition and blurring.

Lin et al. [18] introduced an image forgery detection using both copy-move and splicing forgeries detector. They first used a forgery picture identification strategy through periodicity assessment with the double mixing impact in the temporal and DCT domain. Then the function obtained by SURF descriptors is implemented to resist the variety of rotating and/or scaling of tampered objects in an image. Experimental results showed that their suggested methods were well conducted in the identification of forgery location. The suggested methods were prepared to identify the forged areas and acknowledge the non-original areas, especially for the copy-move forgery pictures.

Finally, We built our work of copy-move detection on [8]. Christlein et al. examined the 15 most prominent feature sets and created a challenging real-world copy-move dataset "Benchmark", that we used as part of our dataset. The paper showed many algorithms in detecting copy-move forgery using both key-point and block-based methods. The results showed that key-point methods have a clear advantage in terms of computational complexity, while the most accurate detection was achieved through the block-based method Zernike.

B. Image Splicing Forgery Detection

The splicing attack is one type of tampering in which different regions of the same or separate sources are combined to create a new fake image. In [21], Riess et al. introduced a method for detecting image splicing through the change of illumination environment of the spliced object. They could overcome one of the biggest challenges which is computing the lighting environment from homogeneous materials. Their approach could successfully improve the mean error by almost 30%. Yet, hair, structurally unsmooth regions, and highly textured clothes were from the model limitations.

Ke et al. proposed forged image detection technique based on shadow consistency, assuming that the shadow and the main body were copied from one image and pasted to another. The algorithm worked as follows; the suspicious region including shadow and non-shadow were first selected and the texture features were then extracted. Next, the similarity of the two texture characteristics were measured using the correlation function. Finally, by comparing the similarity, the decision would be made whether the image was tampered or not [16].

Similarly, an algorithm for digital image forgery detection based on shadow detection of the spliced object was presented in [26] by Tuba et al. They based their algorithm on the fact that a shadow wouldn't change the surface texture, thus if two adjacent areas (with and without shadow) had different texture, then the image could very likely be forged. The algorithm used Local Binary Pattern (LBP) from shadow areas and adjacent non-shadow areas. The energy and entropy extracted from the features histograms proved to be the most discriminating.

On the other hand, Hakimi et al. used different approach for detecting image splicing based on LBP and Discrete Wavelet Transform (DWT). The images were first converted from RGB into $YCbCr$ color channel. Next, the chrominance component were divided into non-overlapping blocks. After that, LBP operator was performed and the wavelet transform applied to all blocks. The output was then fed to the Support Vector Machine (SVM) classifier as features. Haar wavelet was used to reduce the image dimension. The results showed that the algorithm was effective in detecting spliced photos with acceptable accuracy [10].

Regarding LBP, and DCT, Bebis et al. [4] proposed a method to detect image splicing forgeries using these two techniques. They divided the chrominance component of the input image into overlapping blocks, then once used 2D DCT and once used the LBP for each block. Standard deviation is then estimated along with the DCT or LBP to extract the feature vectors from each block and fed it to SVM. Their experiments were on Benchmark dataset with detection accuracy of 97%.

In [13] Huynh-Kha et al. focused on developing a system to detect copy-move and the splicing forgeries together in one image. By applying one-level Discrete Wavelet Transform, the sharpened edges with high frequencies were detected from LH, HL and HH sub-bands. The suspicious region was extracted the feature using Run Difference Method (RDM).

Wang et al. [28] worked on splicing detection through using the GLCM and detecting edges from the integral image and then passing the resulted features to a SVM classifier. They used all images component $YCbCr$ in extracting the feature vectors of an image. They used a certain algorithm to detect

the edges of the image horizontally, vertically and diagonally. We built our work in splicing detection on this paper, we used integral image in detecting the edges of the image.

III. METHODOLOGY

This section is divided into two subsections; copy-move detection technique, and the splicing detection technique. We will explain how our algorithm in both techniques, the workflow, and our datasets are represented in the block diagram, Figure 3.

A. Proposed Method of Copy-Move Forgery Detection

1) *Working Plan*: In copy-move detection, based on [8]. Given an image, the detected regions are computed through the following steps:

- Step 1: Convert the image from RGB to gray-scale color model.
- Step 2: Divide the image into 4 equal blocks and calculate their integral features.
- Step 3: Divide each of the 4 blocks into another four blocks of same size and execute their features.
- Step 4: Extract key-points of all blocks using SIFT and SURF.
- Step 5: Calculate a feature vector for each key-point.
- Step 6: Match each feature vector by comparing each block's features executed with another block.
- Step 7: The forgery is then detected according to a certain threshold among all blocks.
- Step 8: The detected blocks are then displayed with the common object plotted.

2) *Datasets of Copy-Move Images*: We used multiple datasets for copy-move detection; **MICC-F8multi** consisting of 8 forged PNG images, **MICC-F220** consisting of 220 images, 210 original images and 10 fake images [14]. Images were either scaled or rotated or duplicated in different parts of the image. The last dataset was the **Benchmark** datasets that consisted of 4 datasets [8]. Examples of Benchmark datasets are shown in Figure 9.

3) *Pre-processing*: In the beginning, our system was designed using MATLAB, where it requests an RGB image of any format, then the system converts it into a gray-scale. Then the image now is ready for the blocking process. A simple two stages algorithm is then used to divide an image into blocks. In the first stage, the image is divided to 4 equal blocks of the same size and angle. Similarly in the second stage, the system divides each individual block into another 4 equal smaller blocks. This approach is called "*Multi Staged blocking*". We will result in having 20 blocks (4 large blocks + 4*4 small blocks) as shown in Figure 6. The blocking technique eases the features extraction and matching processes that will be discussed later.

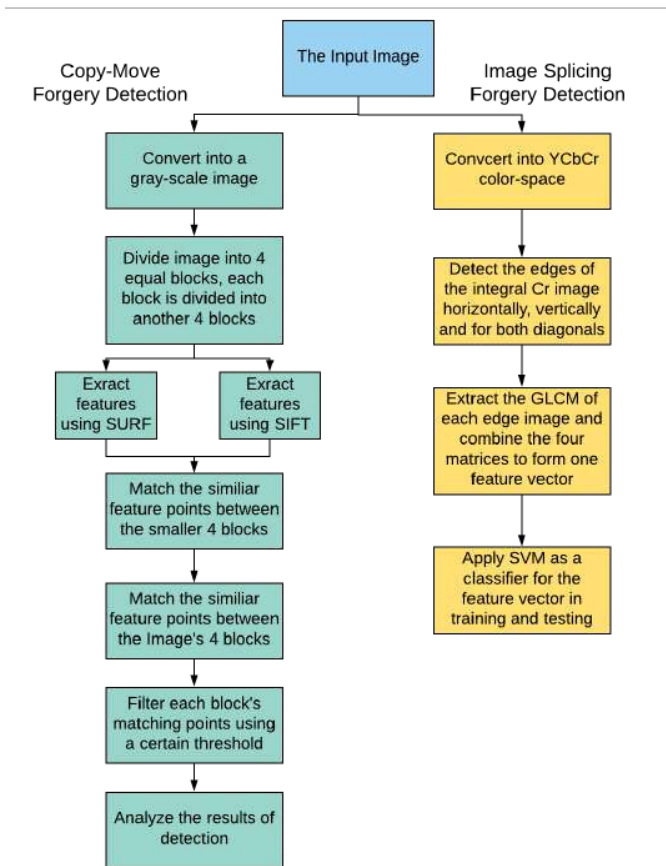


Figure 3. Image Detection Block Diagram

4) *Features Extraction*: For the features extraction, both key-point based methods were used; SIFT & SURF approaches for each block.

SIFT Key-points based method: SIFT (Scale-Invariant Feature Transform) is an algorithm to detect and describe local features in an image. The SIFT algorithm converts an image into a local feature vector called SIFT descriptors and these descriptors have powerful geometric transformations that are constant to scaling and rotation [5], [19].

In addition to extracting the features using SIFT, Harris features on the gray image is used to find the corner points. This process is applied to each block of the image. As a result, we obtain the valid points for the neighboring features.

SURF Key-points based method: similar to SIFT, SURF (Speed Up Robust Feature) is a descriptor used to recognize and locate objects. The values of Hessian determination for each pixel in the image are used to find the points of interest. Next, functions are constructed to be used to select extreme points [6].

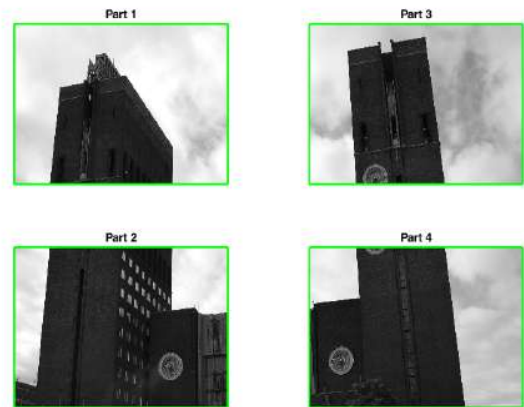


Figure 4. represents the first stage in multi-blocking

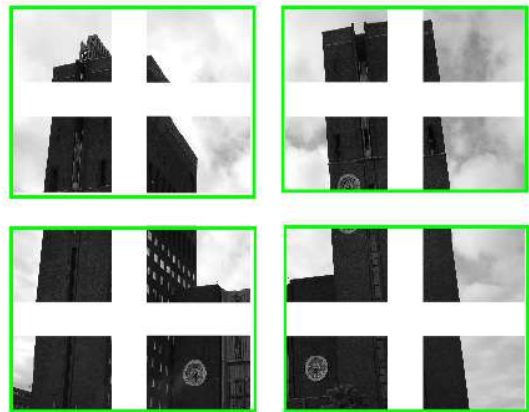


Figure 5. represents the second stage in multi-blocking

Figure 6. An example for the multi-stage blocking of a gray-scale image.

Alternatively, we replace the SIFT step with the SURF. Then, we find the corner points using the Harris detection on the gray image. This process is performed on each block of the image. Lastly, we obtain the valid points for the neighboring features.

5) *Matching Points*: After extracting the neighboring features of each block, the neighboring features are compared to features of another blocks as to find the matched features. Successfully, the locations of the corresponding points for each block will be determined. Ultimately, the system allows the user to view the corresponding points. The system shows the two suspicious blocks where they exceeded the threshold of detected matched points as shown in Figure 7.

6) *Filtering & Analyzing*: The blocks are filtered according to a threshold for the number of matching points detected between two blocks. The threshold is calculated from the

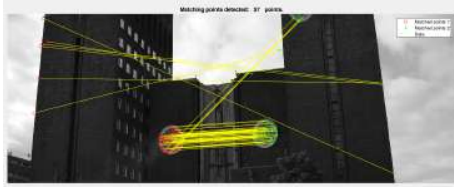


Figure 7. Some of the detected blocks of the image

average number of matched points detected in our datasets.

The system calculates a percentage of the forgery in the image based on the number of suspicious blocks. Accordingly, the percentage of forgery decides which key-point-based method works better on our datasets.

B. Proposed Method of Image Splicing Forgery Detection

Regarding the image splicing forgery detection our algorithm is based on the Gray Level Co-occurrence Matrix (GLCM) for feature extraction similar to [28] and the Support Vector Machine (SVM) for classification [23].

1) *Working Plan*: Given an RGB image as an input, our system runs as follows:

- Step 1: Convert the RGB image to the YC_bC_r image component.
- Step 2: Extract each color channel.
- Step 3: Edge detection is performed on each individual color channel image resulting in edge images. The edges are detected horizontally, vertically and both combined.
- Step 3: Gray Level Co-occurrence Matrix (GLCM) is calculated for each edge, holding the features of the edge image.
- Step 4: These features are given to the Support Vector Machine (SVM) to decide whether a forgery is detected or not.

2) *Review on the System Algorithm*: Our algorithm assumes that the images are colored as colors encode relevant information and sensitive to lighting condition at the moment of image acquisition. Therefore, it is expected to have homogeneous color distribution in case of image splicing. Unlike the copy-move forgery detection, we use YC_bC_r color model instead of gray-scale images. Y is the component of luminance that contains most of the image content. C_b and C_r are the component of chroma blue-difference and red-difference [28].

Our algorithm for image splicing detection works as follows:

Image Edge detection: There are multiple edge detector techniques such as Sobel, LoG or Canny. In this paper we adopted similar technique to [27]. We used the edge detection on the equivalent integral image of the input image. We used four edge images which are: vertical, horizontal, diagonal



Figure 8. An example of spliced image and the Diagonal Edge detection of RGB, Y , C_b and C_r images from top to down and from left to right respectively

and the opposite diagonal which we call the co-diagonal. After obtaining the C_r , we built Haar-like wavelet filters to find vertical and horizontal edges in the C_r image. Next, we calculated the integral image, and built a Haar-like wavelet filter, thus, we could construct the vertical and horizontal edges of the image. For the diagonal and the co-diagonal images, we applied the same method, however, a rotated version of the integral image was used instead of the original one.

Gray Level Co-occurrence Matrix (GLCM): After constructing the C_r edge images, Gray Level Co-occurrence Matrix (GLCM) was applied for texture extraction for each horizontal, vertical, diagonal and co-diagonal edge image. Texture extraction is the equivalent process to the image extraction feature in the copy-move forgery detection. Thus, Texture features are needed to decide the forgery. The Gray Level Co-occurrence Matrix (GLCM) is calculated by creating 8x8 matrix that contains all the features needed for the four edge images. The combination of these matrices generates a feature vector of length 256. This vector will be fed to the classifier for the forgery detection.

3) *SVM Classifier*: Support Vector Machine (SVM) is an efficient and optimal classifier commonly used with machine learning systems, and neural networks [28], [2]. In our system we only have two classes original and fake. So, our model predicts the labels or the classes of our tested features.

4) *Datasets used*: We used CASIA datasets [1] for image splicing, which was divided into two versions; **CASIA I** that consists of 1,737 images (816 authenticated images and 921 spliced images). **CASIA II** consists of 12,625 images (7,492 authenticated images and 5,133 spliced images). We randomly

selected 500 authenticated images and 448 spliced images from both datasets to train and test model. We divided the chosen images into 2 classes; training class (790 images; 417 original images and 373 spliced images), and the testing class (158 images; 83 original images and 75 fake images). An examples for this dataset is shown in Figure 10. Finally, we were limited to colored images as our algorithm works on the YC_bC_r image components.



Figure 9. An example from Benchmark dataset. The original image is on the left and its fake copy is on the right

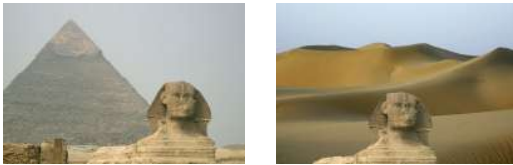


Figure 10. An example from CASIA dataset. The original image on the left and its spliced image on the right

IV. EXPERIMENTS & RESULTS

In this section, our results are presented for the copy-move and compared with [8], and the same for image splicing compared with [28]

A. Copy-Move Results

We examined two different versions of key-points based feature vectors; SIFT and SURF. methods in our system to extract the features from each block to detect identical features and thus, the type of forgery. We compared the SIFT with the SURF to find out which one is better for feature extraction. We ran our algorithm on 3 datasets MICC-F8multi, MICC-F220 [14], and Benchmark datasets [8] as shown in Tables I. From the table it appears that SURF produced more robust results as the number of matched feature points in all test datasets are relatively high when compared to that points matched and were extracted by SIFT.

Table I
AVERAGE NUMBER OF MATCHING POINTS PER IMAGE

	Datasets		
	Average Matching Points		
	MICC-F8Multi	MICC-F220	Benchmark
SIFT	58	40	1774
SURF	113	120	2023

In Table II the confusion matrix is presented for the Benchmark datasets [8] and MICC datasets [14] with 163 tampered images and 110 original images as shown in Table II.

Table II
CONFUSION MATRIX FOR COPY-MOVE DATASET

		Predicted	
		Original	Fake
Actual	Original	100	10
	Fake	10	153

Regarding the F-Measurements the achieved True-Positive (TP) rate is 56%, and the False-Negative(FN) rate is 3.8%. The other two metrics: the True-Negative (TN) rate is 36.6% and the False-Positive(FP) rate were 3.6%. The accuracy is 92.67%.

We compared our Benchmark dataset results with [8] as our work on is based on. The results showed that our execution time is less for each mentioned step leading to a decrease in the average execution time for image tampering detection.

According to [8] the average execution time for copy-move detection per image using SIFT is 610.96 seconds, while using SURF is 1052.12 seconds. For our proposed approach, the average execution time using SIFT is 150.8449648 seconds, and for SURF is 89.4841087 seconds. Our Results shows that "Multi-blocking" can enhance the execution time. In addition, it shows that SURF as a feature extractor is more reliable than using SIFT.

B. Image Splicing Results

We collected 158 images to test our system, 83 original images, and 75 spliced images. The system converts the input images to YC_bC_r to detect image splicing. In the following subsection, our results for each image component are presented including the accuracy and performance, beside highlighting the component that gave the best result.

1) *Y Image Component*: We created GLCM on the Y image component for all images in the dataset. Then we created a training model and added the test feature vectors for all 158 images in the Y image component. There was 40% fake images detected, which means 30 images out of the 75 fake images were correctly detected. On the other hand, 60% of fake images were falsely detected as original. Also, 80 images of 83 original images were correctly defined as original images. So, the percentage of original images falsely detected as fake images was 3%.

2) *C_b Image Component*: Again we developed the feature vector for C_b image component. The results were much better than the Y image component. The system showed 47% of fake images, which means that 35 images out of 75 spliced images were correctly found. While, the rest of the spliced images 53% were falsely considered as original images which is equivalent to 40 images of 74 spliced images. Regarding the original images 71 images were positively detected from 83 original images. However, there was 14% of original

images falsely detected as fake.

3) C_r Image Component: Our system gave the best result for C_r image component in image splicing detection. In Table III we present the confusion matrix of C_r image component based on 158 images from CASIA dataset [1]

Table III
CONFUSION MATRIX FOR SPLICING DATASET

		Predicted	
		Original	Fake
Actual	Original	59	24
	Fake	1	74

The results of the C_r component show that we achieved True-Positive (TP) rate about 99%, and True-Negative (TN) rate greater than 71%. The False-Positive (FP) rate is 29%, and the False-Negative (FN) rate is just 1%. According to [28] C_r component showed accuracy up to 90.5% which is less than our result by 8.5%.

V. DISCUSSION

In this section, the results will be discussed and compared to [8] for the copy-move, and [28] for the image splicing. Also, some limitations of the system are discussed.

Our algorithm showed that SURF in extracting features is more reliable than SIFT. According to our results, SURF managed to extract more reasonable matching points from the image blocks, which in return increased the accuracy of detecting the forgery in more than SIFT. Beside, SURF can detect the scaled and rotated forged objects.

In image splicing, we worked with the Y , C_b , and C_r components individually. C_r proved its reliability in detecting the splicing higher than C_b and Y components.

There are some limitations in our system. First, There were few features extracted in the copy-move algorithm from some of the images in the dataset using our 2 feature extraction methods; SIFT and SURF. One proposed solution can be using another feature extraction as block-based methods such as DCT [24] or DWT [3]. Also, our algorithm depends on dividing the images into blocks in the copy-move detection, however some objects can be divided between multiple blocks which can cause negatively affects the matching point step that compares the features of the blocks to one another.

Concerning the splicing forgery detection, some of edges in integral images were not clear enough to be detected and added to the feature vector of the image. Thus, we propose using combined features instead. Also using a different kernel in the SVM model could be used instead Gaussian or Radial Basis Function (RBF) such as Linear, Polynomial or Sigmoid.

VI. CONCLUSION

In this work, we presented a general framework for detecting two challenging forgery techniques, the copy-move and splicing. In particular, our system can detect the manipulated regions in the image. Our results show that a key-point based method based on the SURF features, can be more efficient for copy-move forgery detection than SIFT. Its main advantage is the remarkably low computational load, combined with good performance and detection of scaled or rotated objects. We also quantified the performance of splicing forgery detection using SVM model with RBF kernel, which give outstanding results when applied on the C_r component of the image. We hope our work can serve as an initial building block to improve the security of images on the web. We also believe that our insights would help the forensics professionals with a more concrete decisions.

REFERENCES

- [1] CASIA V1,II, author=Jing Dong,Wei Wang,Tieniu Tan, howpublished = <https://www.kaggle.com/sophatvathana/casia-dataset>.
- [2] Tim Adams, Jens Dörpinghaus, Marc Jacobs, and Volker Steinhage. Automated lung tumor detection and diagnosis in ct scans using texture feature analysis and svm. In *FedCSIS Communication Papers*, 2018. doi: 10.15439/2018F176.
- [3] Maryam Nabil Al-Berry, Mohammed A.-M. Salem, Hala Mousher Ebeid, Ashraf S Hussein, and Mohammed F Tolba. Fusing directional wavelet local binary pattern and moments for human action recognition. *IET Computer Vision*, 10(2):153–162, 2016.
- [4] Amani A Alahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, and George Bebis. Splicing image forgery detection based on dct and local binary pattern. In *2013 IEEE Global Conference on Signal and Information Processing*, pages 253–256. IEEE, 2013. doi: 10.1109/GlobalSIP.2013.6736863.
- [5] Hesham A Alberry, Abdelfatah A Hegazy, and Gouda I Salama. A fast sift based method for copy move forgery detection. *Future Computing and Informatics Journal*, 3(2):159–165, 2018. doi:10.1016/j.fcij.2018.03.001.
- [6] Herbert Bay, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool. Speeded-up robust features (surf). *Computer vision and image understanding*, 110(3):346–359, 2008.
- [7] Sevinc Bayram, Husrev Taha Sencar, and Nasir Memon. A survey of copy-move forgery detection techniques. pages 538–542, 2008. doi: 10.1109/ICISC.2017.8068703.
- [8] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou. An evaluation of popular copy-move forgery detection approaches. *IEEE Transactions on information forensics and security*, 7(6):1841–1854, 2012. doi:10.1109/TIFS.2012.2218597.
- [9] A Jessica Fridrich, B David Soukal, and A Jan Lukáš. Detection of copy-move forgery in digital images. In *in Proceedings of Digital Forensic Research Workshop*. Citeseer, 2003. doi:10.1016/j.forsciint.2013.05.027.
- [10] Fahime Hakimi, Mahdi Hariri, and Farhad GharehBaghi. Image splicing forgery detection using local binary pattern and discrete wavelet transform. In *2015 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI)*, pages 1074–1077. IEEE, 2015. doi:10.1109/KBEI.2015.7436195.
- [11] Tu K Huynh, Khoa V Huynh, Thuong Le-Tien, and Sy C Nguyen. A survey on image forgery detection techniques. In *The 2015 IEEE RIVF International Conference on Computing & Communication Technologies-Research, Innovation, and Vision for Future (RIVF)*, pages 71–76. IEEE, 2015. doi: 10.1109/RIVF.2015.7049877.
- [12] Tu Huynh-Kha, Thuong Le-Tien, Synh Ha-Viet-Uyen, Khoa Huynh-Van, and Marie Luong. A robust algorithm of forgery detection in copy-move and spliced images. *IJACSA International Journal of Advanced Computer Science and Applications*, 7(3), 2016. doi: 10.14569/IJACSA.2016.070301.

- [13] Tu Huynh-Kha, Thuong Le-Tien, Synh Ha-Viet-Uyen, Khoa Huynh-Van, and Marie Luong. A robust algorithm of forgery detection in copy-move and spliced images. *IJACSA International Journal of Advanced Computer Science and Applications*, 7(3), 2016.
- [14] R. Caldelli A. Del Bimbo G. Serra. I. Amerini, L. Ballan. A sift-based forensic method for copy-move attack detection and transformation recovery. pages pp. 1099–1110. *IEEE Transactions on Information Forensics and Security*, vol. 6, issue 3, 2011. doi: 10.1109/TIFS.2011.2129512.
- [15] Pravin Kakar and N Sudha. Exposing postprocessed copy–paste forgeries through transform-invariant features. *IEEE Transactions on Information Forensics and Security*, 7(3):1018–1028, 2012.
- [16] Yongzhen Ke, Fan Qin, Weidong Min, and Guiling Zhang. Exposing image forgery by detecting consistency of shadow. *The Scientific World Journal*, 2014, 2014. doi:10.1155/2014/364501.
- [17] Shinfeng D Lin and Tszan Wu. An integrated technique for splicing and copy-move forgery image detection. In 2011 4th International Congress on Image and Signal Processing, volume 2, pages 1086–1090. IEEE, 2011. doi: 10.1109/CISP.2011.6100366.
- [18] Shinfeng D Lin and Tszan Wu. An integrated technique for splicing and copy-move forgery image detection. In 2011 4th International Congress on Image and Signal Processing, volume 2, pages 1086–1090. IEEE, 2011.
- [19] Tony Lindeberg. Scale invariant feature transform. 2012.
- [20] Cecilia Pasquini, Carlo Brunetta, Andrea F Vinci, Valentina Conotter, and Giulia Boato. Towards the verification of image integrity in online news. pages 1–6, 2015. doi: 10.1109/ICMEW.2015.7169801.
- [21] Christian Riess, Mathias Unberath, Farzad Naderi, Sven Pfäller, Marc Stamminger, and Elli Angelopoulou. Handling multiple materials for exposure of digital forgeries using 2-d lighting environments. *Multimedia Tools and Applications*, 76(4):4747–4764, 2017. doi: 10.1007/s11042-016-3655-0.
- [22] Seung-Jin Ryu, Matthias Kirchner, Min-Jeong Lee, and Heung-Kyu Lee. Rotation invariant localization of duplicated image regions based on zernike moments. *IEEE Transactions on Information Forensics and Security*, 8(8):1355–1370, 2013.
- [23] M.A.-M. Salem. Multi-stage localization given topological map for autonomous robots. In *International Conference on Computer Engineering and Systems, ICCES 2012*, pages 55–60, 2012.
- [24] Mohammed A.-M. Salem, Markus Appel, Frank Winkler, and Beate Meffert. Fpga-based smart camera for 3d wavelet-based image segmentation. In *2008 Second ACM/IEEE International Conference on Distributed Smart Cameras*, pages 1–8. IEEE, 2008.
- [25] BL Shivakumar and S Santhosh Baboo. Detection of region duplication forgery in digital images using surf. *International Journal of Computer Science Issues (IJCSI)*, 8(4):199, 2011.
- [26] Ira Tuba, Eva Tuba, and Marko Beko. Digital image forgery detection based on shadow texture features. In *2016 24th Telecommunications Forum (TELFOR)*, pages 1–4. IEEE, 2016. doi: 10.1109/TELFOR.2016.7818875.
- [27] Paul Viola and Michael J. Jones. Rapid object detection using a boosted cascade of simple features. In *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001. Volume: 1*, pp.511–518., pages 1257–1260. IEEE, 2009. doi: 10.1109/CVPR.2001.990517.
- [28] Wei Wang, Jing Dong, and Tieniu Tan. Effective image splicing detection based on image chroma. In *2009 16th IEEE International Conference on Image Processing (ICIP)*, pages 1257–1260. IEEE, 2009. doi: 10.1109/ICIP.2009.5413549.