Malaya Journal of Matematik, Vol. S, No. 1, 23-30, 2021

https://doi.org/10.26637/MJMS2101/0005

A robust image copy detection method using machine learning

Arunkumar Lourembam[1] and K. M. V Madan Kumar[2] and Thounaojam Rupachandra Singh[3]

Abstract

In this present time, it is very easy to get a digital image through our smartphone we use everyday. Thus easily our digital image can be processed and used by other people without our knowledge. The original image gets manipulated and processed for various reasons without the authentication of those who belong to it. Due to this reason image copy detection plays a significant role. This research paper tries to present the image copy detection model for the 2 most common image tampering method which includes copy-image forgery detection and Image Splicing. Also Feature extraction process is done through the Speeded up robust features(SURF), and Scale Invariant Feature Transform(SIFT) Descriptor method for identifying the matching point. In the case of Image Splicing Detection, it is used for extracting the image edges of Y(brightness in luma), Cb(blue minus luma), and C_r (Red minus luma) of the image components. Gray Level Co-Occurrence Matrix (GLCM) is utilized for each and every edge internal image through which the feature vector is created. The created feature vector is fed into a Support Vector Machine (SVM Classifier). In the research, the proposed method for image copy detection represents an outcome showing that the Speeded up robust feature is superior to the Scale Invariant Feature Transform. The proposed method simulates 80 percent accuracy for the detection of tampered images. The image processing technique using the YC_b C_r color model showed a significant result in image splicing detection. The outcome from this method simulates 98 percent positivity for the detection of image splicing.

Keywords

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

[1,2] *Department of Computer Science, CMJ University, Shillong, India.*

[3] *Department of Computer Science, Manipur University, India.*

Article History: Received **12** December **2020**; Accepted **10** February **2021**

Contents

1. Introduction

Image coping has become one of the easiest jobs to do since images are very easily available on the web. There is much software which easily available for image manipulation through an original image that can be rechanged so that it appears as a brand new image. A recent report states that there are almost a billion similar digital images available on the web. And the usage of low-cost manipulated images and the dataset of these manipulated photos and videos easily makes the web an easy process for getting those images. For these kinds of image manipulation on the web, the "A ROBUST IMAGE COPY DETECTION METHOD USING MACHINE LEARNING" approach has been proposed in this research article. Managing digital images of an individual is always a daring thing in the presence of cyberspace society. Present generation due to the availability of smart devices they share their personal life day to day activity on social media websites such as Insta-

gram, Twitter, Facebook either as photos or videos. So there is a chance for any random individual to access those photos and manipulated them. Image manipulation is present long back but in this scenario, it has gained more attention among IT (information technology), intelligence service, forensic investigation, movies, social media sites, etc. Image Copy

Figure 1. Copied images Vs Original image

Detection Method has now become an important research topic in various fields which includes computer technology, criminal investigation, biomedical, forensic, etc. this method has sought more attention and is considered as one of the challenging processes with the utilization of the latest software system.

Social media is one of the places where the more digital image gets shared and viewed by many and thus security issue arises if someone manipulates the original image. The transistionfrom non-digital to digital life allows data to be stored in digital format and it is a daring task to maintain authentication of those data.

The digitally stored files, videos, images, and data can be easily manipulated and forged without the knowledge of the user. The original image will be altered slightly which is termed as near-duplicate image detection. Feature extraction must be used to over image manipulation. Because it is an accurate step to detect a near-duplicate image.

It is more critical because the features extracted directly influence the efficiency in the detection/retrieval. The motivation to propose efficient copy-move forgery detection methods with the use of optimization techniques and a classifier is discussed.In this paper, extracting the image features and analyzingthem to detect the copied images and also determine the type of the forgery/copy whether it is copy-move or splicing.

2. Review of Literature

In this paper, the extracted 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. The present work is to test multiple datasets.

In today's world, digital images are widely used in various domains such as; newspapers, scientific journals, magazines, and many other fields (Huynh-Kha et al., 2016). Unfortunately, today's digital technology made it easy for digital images to be forged due to the availability of low-cost photo editing software(Al-Berry et al., 2017).

Due to the huge development of technology, the usage of the digital image has been expanding day by day in our daily lives. Because of this forgery of the digital image has turned out to be increasingly straightforward and indiscoverable. At present technology where anything can be controlled or changed with the assistance of modern technology had started to disintegrate the authenticity of images (George, et al 2013) counterfeiting and forgeries with the move to the Megapixels, which gives a new way for forgery.

Imitation is not new to humankind but rather it is past generation issues. In the past it was limited to craftsmanship and composing yet did not impact the overall population. The ability to create image forgery is nearly as old as photography itself (Alberry, et al 2018).

Over a two-decade, photography is a normal and fascinating art which turned out for creating portraits and by that portrait photographers can earn money by making forgery possible by enhancing deals by retouching their photographs (Herbert Bay, et al 2008).

Image forgery detection had gained more attention and incredible investigation in various fields such as computer visualization, image processing, biomedical tools, immoral analysis, image forensics, etc. It gained further attention and demanding due to advanced software's that become difficult to verify whether an image is influenced by naked eyes (Nasir, et al 2008).

(Jessica Friedrich, et al 2013) However, now because of the advanced software and development of numerous gadgets, a photo can be changed and altered. It prompts to exceedingly worrying for people to distinguish the picture is authenticate or forged. The accessibility of digital image processing software includes Photo Shop, Adobe Photoshop makes it moderately simple to generate the forged image from several images. In any case, the image contains many sources of data, and the dependability of digital images is therefore turning into an imperative issue. A photo may worth a thousand words however, nearby, it might have scores of analysis. Images are used to elucidate extreme ideas and move us easily in each field. Images are noticeable techniques for communication and various individuals rely on them, so it is significant that their genuineness should be illustrated.

The work in this chapter reveals the importance of image forgery detection in real-world applications. It is a difficult task to identify the forgery image. This can be possible by adopting image processing techniques for efficient detection. Due to the availability of image processing techniques, editing tools, the conversion of images has become so easy and accessible. Nowadays image processing techniques are widely used in all fields due to easy manipulation, low expensive, less computation time, and efficient result. In this research detection of image forgery by image processing techniques to differentiate the forgery and authenticate image.

Image forensics is a well-developed field that analyzes the images of specific conditions to build up trust and genuineness. It is a quick and better-known domain due to several

executions of real-time applications in numerous areas that incorporate intelligence, sports, legitimate administrations, news reporting, medical imaging, and protection assert investigations. An image can be faked by modifying the image features characteristics such as brightness, darkness, or image parameters or concealing data (Serra, et al 2011, Amreni, et al 2011).

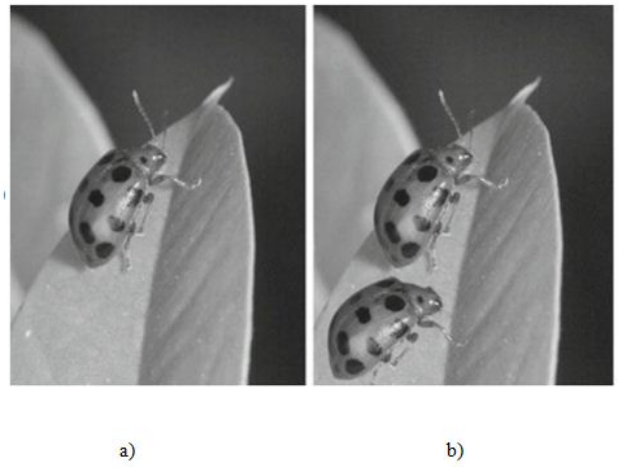
(Guiling Zhang, et al 2014) Image copy implies altering the digital image to some meaningful or valuable data. Simply it can define as the process of inserting or eliminating the specific features from an image without any proof of altering and to evade for malicious purposes. In some cases, it is complicated to recognize the altered image part from the authenticate image. The identification of a forged image is essential for originality and to preserve the truthfulness of the image. A forgery detection that endeavors the unobtrusive irregularities in the color shade of the illumination changes in images. To accomplish this by consolidating data from material science and statistical-based illuminate estimators on image regions to separate texture and edge-based features.

The copy-move is defined by copying a 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 (Volker, et al 2018).

3. Peoposed methodology

This section is divided into two subsections; the copy-move detection technique, and the splicing detection technique. The explanation on the algorithm in both techniques, the workflow, and the datasets are represented in the block diagram.

A. Proposed Method of Copy-Move Forgery Detection



a) b)

Figure 2. Example of Copy-Move Forgery a) original image b) tampered image

1. Working Plan:In copy-move detection, based on (Vincent, et al 2011). Given an image, the detected regions are computed through the following steps:

   - ✓ **Step 1:** Convert the image from RGB to the 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 the 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:** in this research the 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 (Serra, et al 2011). 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 (Vincent, et al 2011). Examples of Benchmark datasets are shown in this research.

3. **Pre-processing:** In the beginning, the 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 into 4 equal blocks of the same size and angle. Similarly in the second stage, the system divides each block into another 4 equal smaller blocks. This approach is called Multi Staged blocking. The blocking technique eases the feature extraction and matching processes that will be discussed later.

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

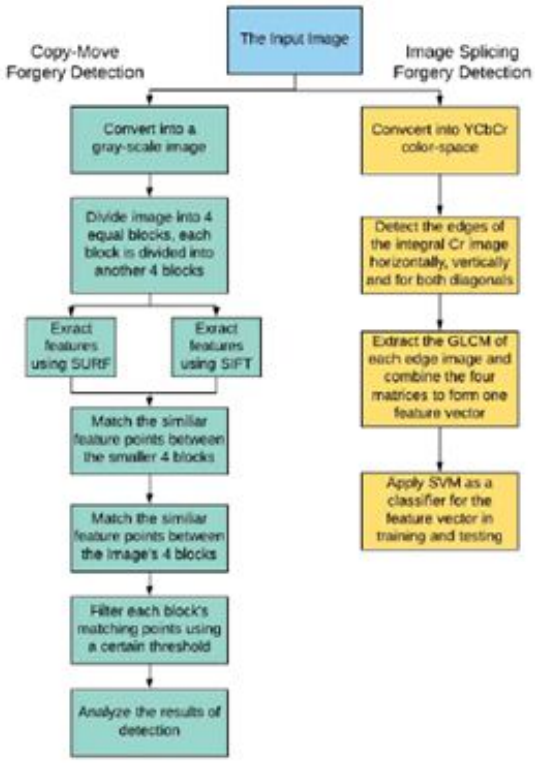


Figure 3. Image Detection Method

geometric transformations that are constant to scaling and rotation (Alberry, et al 2018, Tony, et al 2012).

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, it is to 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 (Helbery bay, et al 2011).

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 block 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.

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 average number of matched points detected in the 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 the datasets.

B. Proposed Method of Image Splicing Forgery Detection
Regarding the image splicing forgery detection the algorithm is based on the Gray Level Co-occurrence Matrix (GLCM) for feature extraction similar to (Wang, et al 2009) and the Support Vector Machine (SVM) for classification (Salem, et al 2012).

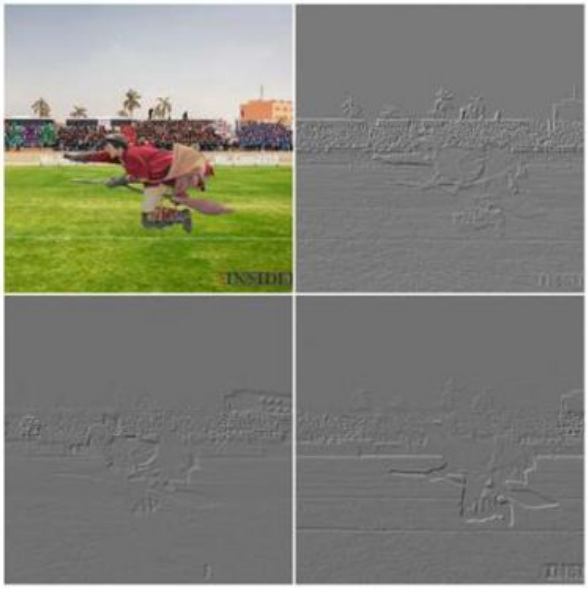


Figure 4. An example of spliced image and the Diagonal Edge detection of RGB

1. **Working Plan:** Given an RGB image as an input, the presented system runs as follows:

   - **Step 1:** Convert the RGB image to the YCbCrimage component.
   - **Step 2:** Extract each color channel.
   - **Step 3:** Edge detection is preformed on each individual color channel image resulting in edge images. The edges are detected horizontally, vertically and both combined.
   - **Step 4:** Gray Level Co-occurrence Matrix (GLCM) is calculated for each edge, holding the features of the edge image.

- **Step 5:** 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:** The present 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, the usedYCbCrcolor model instead of gray-scale images. Y is the component of luminescence that contains most of the image content. Cband Cr are the component of chroma blue-difference and red-difference (Wang, et al 2009).

The present algorithm for image splicing detection works as follows:

3.1 Image Edge detection

There are multiple edge detector techniques such as Sobel,LoG or Canny. In this paper the adopted similar technique to (Paul, et al 2009).The used edge detection on the equivalent integral image of the input image. We used four edge images which are: vertical, horizontal, diagonaland the opposite diagonal which it is called the co-diagonal. After obtaining the Cr, is built Haar-like wavelet filters to find vertical and horizontal edges in the Cr image. Next, it is to calculate the integral image, and built a Haar-like wavelet filter, thus, it is possible to construct the vertical and horizontal edges of the image. For the diagonal and the co-diagonal images, applied the same method, however, a rotated version of the integral image was used instead of the original one.

3.2 Gray Level Co-occurrence Matrix (GLCM)

After constructing the Cr 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.

3.3 SVM Classifier

Support Vector Machine (SVM) is an efficient and optimal classifier commonly used with machine learning systems, and neural networks (Wang, et al 2009, Volker, et al 2018). In this system it is the only have two classes original and fake. So, the model predicts the labels or the classes of the tested features.

3.4 Datasets used

Theused CASIA datasets (Casia, et al) 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). The randomly

Figure 5. An example from Benchmark dataset. The original image is on the left and its fake copy is on the right

Figure 6. An example from CASIA dataset. The original image on the left and its spliced image on the right

selected 500 authenticated images and 448 spliced images from both datasets to train and test model. 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). Finally, they were limited to colored images as the present algorithm works on the YCbCrimage components.

4. Results and Discussion

In this section, the results are presented for the copy-move and compared with (Vincent, et al 2018), and the same for image splicing compared with (Wang, et al 2009).

4.1 Copy-Move Results

Examined two different versions of key-points based feature vectors; SIFT and SURF. methods in the system to extract the features from each block to detect identical features and thus, the type of forgery. The comparison between the SIFT with the SURF to find out which one is better for feature extraction. The algorithm ran on 3 datasets MICC-F8multi, MICCF220 (Serra, et al 2011), and Benchmark datasets (Vincent, et al 2018)as shown in Tables 1. 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 1. Average Number of Matching Points for an image

Dataset		
Average Matching Points		
MICC-F8 Multi BenchMark		
MICC-F220		
SIFT	58 40	1774
SURF	113 120	2023

In Table II the confusion matrix is presented for the Benchmark datasets (Vincent, et al 2012) and MICC datasets (Serra, et al 2011) with 163 tampered images and 110 original images as shown in Table 2.

Table 2. Confusion Matrix for Image Copy-Move Dataset

	Predicted	
	Original	Fake
Original	98	12
Fake	12	154

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%. The comparison between the Benchmark dataset results with (Vincent, et al 2012) as the work on is based on. The results showed that the execution time is less for each mentioned step leading to a decrease in the average execution time for image tampering detection.

According to (Vincent, et al 2012) the average execution time for copy-move detection per image using SIFT is 610.96 seconds, while using SURF is 1052.12 seconds. For the proposed approach, the average execution time using SIFT is 150.8449648 seconds, and for SURF is 89.4841087 seconds. the Results shows that Multi-blocking can enhance the execution time. In addition, it shows that SURF as an feature extractor is more reliable than using SIFT.

4.2 Image Splicing Results

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

Y Image Component:

The created GLCM on the Y image component for all images in the dataset. 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%.

C_b Image Component:

Again the developed the feature vector for Cbimage 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 are 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 were falsely detected as fake.

C_r Image Component:

The system gave the best result for Cr image component in image splicing detection. Table 3presents the confusion matrix of Cr image component based on 158 images from CASIA dataset (Casia, et al)

Table 3. Confusion Matrix for Image Splicing Dataset

	Predicted	
	Original	Fake
Original	58	23
Fake	2	75

The results of the Cr component show that the achieved True-Positive (TP) rate about 99%, and True-Negative (TN) rate greater than 70%. The False-Positive (FP) rate is 23%, and the False-Negative (FN) rate is just 2%.According to [28] Cr component showed accuracy up to 91.5% which is less than the present result by 8.5%.In this section, the results will be discussed and compared to (Vincent, et al 2012) for the copy-move, and (Wang, et al 2009) for the image splicing. Also, some limitations of the system are discussed.

The algorithm showed that SURF in extracting features is more reliable than SIFT. According to the 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, 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 the system. First, There were few f eatures extracted in the copy-move algorithm from some of the images in the dataset using the 2 feature extraction methods; SIFT and SURF. One proposed solution can be using another feature extraction as block-based methods such as DCT (Winkler, et al 2008) or DWT (Maryam, et al 2016). Also, the 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, the 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.

5. Conclusion

In this work, it presents a general framework for detecting two challenging forgery techniques, the copy-move and splicing. In particular, the system can detect the manipulated regions in the image. The 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. The quantified the performance of splicing forgery detection using SVM model with the RBF kernel, which gives outstanding results when applied on the Cr component of the image. The further must serve as an initial building block to improve the security of images on the web. It is believed that insights would help forensics professionals with more concrete decisions.

References

[1] William, Youssef, SherineSafwat, and Mohammed A-M. Salem. *Robust Image Forgery Detection Using Point Feature Analysis.* 2019 Federated Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2019.

[2] Malík, Peter, Štefan Krištofík, and Kristína Knapová. *Instance Segmentation Model Created from Three Semantic Segmentations of Mask,* Boundary and Centroid Pixels Verified on GlaS Dataset. 2020 15th Conference on Computer Science and Information Systems (FedCSIS). IEEE, 2020.

[3] Al-Berry, M. N., et al. Directional Multi-Scale Stationary Wavelet-Based Representation for Human Action Classification. *Handbook of Research on Machine Learning Innovations and Trends.* IGI Global, 2017. 295-319.

[4] Muhammad, Ghulam, et al. Image forgery detection using steerable pyramid transform and local binary pattern. *Machine Vision and Applications.* 25(4)(2014), 985-995.

[5] Kuznetsov, Andrey, and Vladislav Myasnikov. A new copy-move forgery detection algorithm using image preprocessing procedure. *Procedia engineering.* 201(2017), 436-444.

[6] Bay, Herbert, et al. Speeded-up robust features (SURF). *Computer vision and image understanding.* 110(3)(2008), 346-359.

[7] Kanagavalli, N., and L. Latha. *A survey of copy-move image forgery detection techniques.* 2017 International Conference on Inventive Systems and Control (ICISC). IEEE, 2017.

[8] Amerini, Irene, et al. A sift-based forensic method for copy–move attack detection and transformation recovery. *IEEE transactions on information forensics and security,* 6(3)(2011), 1099-1110.

[9] Huynh, Tu K., et al. *A survey on image forgery detection techniques*. The 2015 IEEE RIVF International Conference on Computing & Communication Technologies-Research, Innovation, and Vision for Future (RIVF). IEEE, 2015.

[10] Huynh-Kha, Tu, et al. A robust algorithm of forgery detection in copy-move and spliced images. *International Journal of Advanced Computer Science and Applications,* 7(3)(2016).

[11] Zhang, Daniel Yue, et al. *Towards reliable missing truth discovery in online social media sensing applications.* 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). IEEE, 2018.

[12] Amerini, Irene, et al. A sift-based forensic method for copy–move attack detection and transformation recovery. *IEEE transactions on information forensics and security.* 6(3)(2011), 1099-1110.

[13] Sudha, N., and PravinKakar. *Exposing postprocessed copy–paste forgeries through transform-invariant features*. (2012).

[14] Ke, Yongzhen, et al. Exposing image forgery by detecting consistency of shadow. *The Scientific World Journal.* 2014(2014).

[15] Lin, Shinfeng D., and Tszan Wu. *An integrated technique for splicing and copy-move forgery image detection*. 2011 4th International Congress on Image and Signal Processing. IEEE, 2011.

[16] Lindeberg, Tony. *Scale invariant feature transform.* (2012): 10491.

[17] Pasquini, Cecilia, et al. *Towards the verification of image integrity in online news.* 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW). IEEE, 2015.

[18] Riess, Christian, et al. Handling multiple materials for exposure of digital forgeries using 2-D lighting environments. *Multimedia Tools and Applications,* 76(4)(2017), 4747-4764.

[19] Ryu, Seung-Jin, et al. Rotation invariant localization of duplicated image regions based on Zernike moments. *IEEE Transactions on Information Forensics and Security.* 8(8)(2013), 1355-1370.

[20] Mohammed, A., and Megeed Salem. *Multi-stage localization given topological map for autonomous robots*. 2012 Seventh International Conference on Computer Engineering & Systems (ICCES). IEEE, 2012.

[21] Mohammed, A., et al. *FPGA-based smart camera for 3D wavelet-based image segmentation*. 2008 Second ACM/IEEE International Conference on Distributed Smart Cameras. IEEE, 2008.

[22] Shivakumar, B. L., and S. Santhosh Baboo. Detection of region duplication forgery in digital images using SURF. *International Journal of Computer Science Issues,* 8(4)(2011), 199.

[23] Tuba, Ira, Eva Tuba, and Marko Beko. *Digital im-*

age forgery detection based on shadow texture features. 2016 24th Telecommunications Forum (TELFOR). IEEE, 2016.

[24] Viola, Paul, and Michael Jones. *Rapid object detection using a boosted cascade of simple features.* Proceedings of the 2001 IEEE computer society conference on computer vision and pattern recognition. CVPR 2001. IEEE, 2001.

[25] Dong, Jing, et al. *Run-length and edge statistics based approach for image splicing detection*. International workshop on digital watermarking. Springer, Berlin, Heidelberg, 2008.

[26] Armas Vega, Esteban Alejandro, et al. Digital images authentication technique based on DWT, DCT and local binary patterns. *Sensors.* 18(10)(2018), 3372.

[27] Vialatte, Jean-Charles, Vincent Gripon, and Gilles Coppin. *Learning local receptive fields and their weight sharing scheme on graphs.* 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP). IEEE, 2017.

[28] Alhussein, Musaed. *Image tampering detection based on local texture descriptor and extreme learning machine*. 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation (UKSim). IEEE, 2016.

[29] Ojeniyi, Joseph A., et al. Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques. *International Journal of Image, Graphics and Signal Processing.* 10(4)(2018), 22.

[30] Ardizzone, Edoardo, Alessandro Bruno, and Giuseppe Mazzola. Copy–move forgery detection by matching triangles of keypoints. *IEEE Transactions on Information Forensics and Security.* 10(10)(2015), 2084-2094.

[31] Gomes, Juliana C., et al. Electrical impedance tomography image reconstruction based on back projection and extreme learning machines. *Research on Biomedical Engineering,* (2020), 1-12.

[32] Apollonio, F. I., et al. *Evaluation of feature-based methods for automated network orientation*. International Archives of the Photogrammetry, Remote Sensing & Spatial Information Sciences. 45(2014).

[33] Wang, Zhaoyang, et al. Digital image correlation in experimental mechanics and image registration in computer vision: similarities, differences and complements. *Optics and Lasers in Engineering.* 65(2015), 18-27.

[34] Bayram, Sevinc, HusrevTahaSencar, and Nasir Memon. *An efficient and robust method for detecting copy-move forgery.* 2009 IEEE International Conference on Acoustics, Speech and Signal Processing. IEEE, 2009.

[35] Birajdar, Gajanan K., and Vijay H. Mankar. Digital image forgery detection using passive techniques: A survey. *Digital investigation.* 10(3)(2013), 226-245.

[36] Marra, Francesco, Diego Gragnaniello, and Luisa Verdoliva. On the vulnerability of deep learning to adversarial attacks for camera model identification. *Signal Processing: Image Communication.* 65(2018), 240-248.

[37] Abdalla, Younis, M. Tariq Iqbal, and Mohamed Shehata. Copy-Move Forgery Detection and Localization Using a Generative Adversarial Network and Convolutional Neural-Network. *Information.* 10(9)(2019), 286.

[38] Bappy, Jawadul, et al. *Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning*. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. 2017.

[39] Camps-Valls, Gustavo, et al. Fuzzy sigmoid kernel for support vector classifiers. *Neurocomputing.* 62(2004), 501-506.

[40] Chauhan, Devanshi, et al. Survey on keypoint based copy-move forgery detection methods on image. *Procedia Computer Science.* 85(2016), 206-212.

⋆⋆⋆⋆⋆⋆⋆⋆⋆

ISSN(P):2319 – 3786
Malaya Journal of Matematik
ISSN(O):2321 – 5666

⋆⋆⋆⋆⋆⋆⋆⋆⋆