Copy-Move Forgery Detection using Integrated DWT and SURF

Loai Alamro, Nooraini Yusoff
School of Computing, UUM College of Arts and Sciences, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah.
loaialamro@gmail.com

***Abstract*—In this study, we propose a combination of two feature extraction methods namely Discrete Wavelet Transform (DWT) and Speeded Up Robust Features (SURF) to detect a copy-move forgery in digital media. Copy-move is one of the most popular kinds of digital image tempering, in which one or more parts of a digital image are copied and pasted into different locations. DWT is used to reduce image dimension and SURF is superior in extracting the key features from the image. The method has been tested with BMP and JPG images consisting of genuine and counterfeited images. Furthermore, the method has also been tested with copied-moved images applied with a number of various geometric transformation attacks including rotation, translation, scaling or set of them. The experiments results prove that the proposed method is superior with overall accuracy 95% when compared with the existing method. The copy-move attacks in the digital image have been successfully detected.**

***Index Terms*—Image Tampering; Digital Image Forgery; Copy-Move Forgery; Dimensionality Reduction; Discrete Wavelet Transform; Speeded Up Robust Features.**

I. INTRODUCTION

Digital images are widely used in media both in printed or electronic. As a result of the digital revolution, dealing with images has become easier in the last few years. The existence of digital imaging devices has made the accessing, editing and sharing of digital images to be an easy process. Digital images have been used extensively in various applications that include medical imaging, banking, journalism, and education [1]. Despite the proliferation of digital images and the rapid development of image editing tools, this have also offered some major security challenges.

Digital images can be fraud by manipulating some important information of the image [2]. Generally, digital image forgery can be classified into four main types namely image retouching, re-sampling, image splicing and copy-move image, depending on the method used to rig the images.

Image retouching method is used to enhance the quality of the image to have a more attractive look. This method is normally used by most publishers and magazines to design high quality covers. The method manipulates the image properties (e.g., changing color, brightness, contrast, hue, saturation, white balance or/and background) using an editing software to get the desired results as shown in Figure 1.

Image resampling is a method used to resemble images or parts of it. The method is done by applying some common geometric transform (e.g., scaling, rotation, translation and resize) [3]. Figure 2 shows some examples of images as a result of applying this method.

Figure 1: An example of image retouching. A) The genuine image B) The forged image.

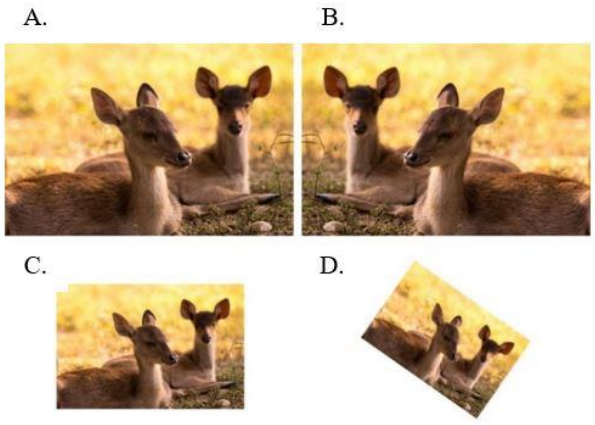

Figure 2: An example of the image resampling. A) The genuine image B) Image resampling through flipping. C) Image resampling using scaling. D) Image resampling using rotation and scaling.

The image splicing is a method that uses parts of two or more images to create a fraud image. This method uses the cut and paste techniques to implement the fraud process [4]. Figure 3 shows an example of image splicing.

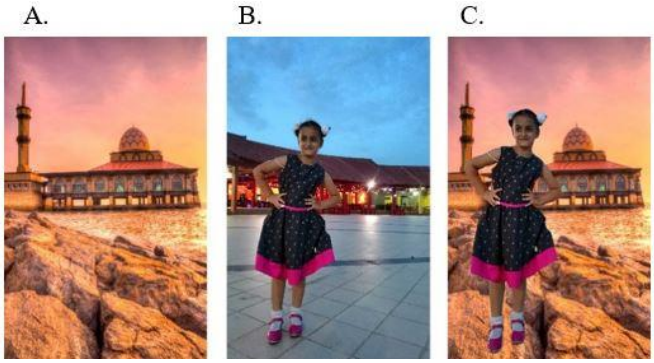

Figure 3: An example of image splicing (A) and (B) The genuine images (C) The resulted image.

Copy-move is a method of image forgery which is done by copying a part of an image, and applying one or more image transformations, e.g. rotation and scaling, to increase the

difficulty of detection. Then the copied and transformed part is pasted once or several times into the same image [5] as shown in Figure 4.

The advancement of digital image forgery methods has created an urgent need to verify an image authenticity and credibility. Therefore, there is a need to find robust techniques to determine fraud issues in a digital image. Digital image forensic approaches are categorized into two categories, active approach, and passive approach. The former approach uses a digital signature or digital watermark and embedded in the genuine image which can be used to reject or prove the image originality. The process of adding digital signature or digital watermark to the digital image can be implemented by the camera during the process of saving the image information from the camera sensor to its memory to create the digital image, or during processing the image in editing tools by the authorized person. These techniques depend on prior information (i.e., digital signature or digital watermark) to prove the authenticity of the image [6, 7] as shown in Figure 5.

Conversely, the latter approach does not depend on the previous information of an image. This approach relies on the statistical changes resulted from the forgery process that is applied to the digital image. The passive approach also depends on the changes in the properties of the image (e.g., discrepancy in lighting) that left by the camera during the capture of the image to detect the forgery. The most common image forgery detection method can be categorized into six categories: source camera identification-based, camera-based, physics-based, format-based, geometric-based and pixel-based [8, 9].

This study focuses on pixel-level forgery detection technique. Practically most common techniques used to fraud digital images are based on pixel-level [4]. Pixel-based techniques investigate the statistical distortion that resulted from the fraud process at the pixel-level [10]. Pixel-based detection method can be categorized into four detection categories: statistical, splicing, resampling and copy-move [2]. Copy-move is one of the most commonly used methods among counterfeiters [11]. The copy-move forgery detection methods are divided into two parts namely block based and keypoint. We focus on the integration of the two methods to detect copy-move region exposed to rotation and scaling. The advantage of using the block-based is to reduce image dimensions (less computational complexity), and the advantage in using the keypoint is to extract more robust features.

Figure 4: An example of copying and moving parts of image. (A) The genuine image. (B) The fraud image.

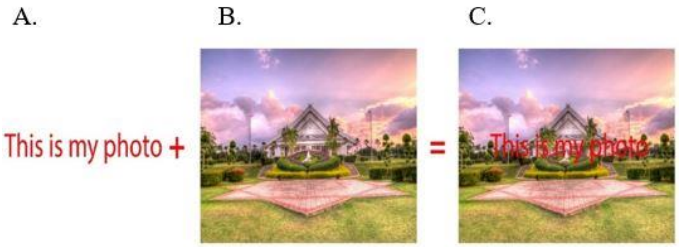

Figure 5: An example of digital watermark. (A) The text used to prove the authenticity, (B) The genuine image. (C) The resulted image after adding the watermark.

II. Related Work

For detecting a copy-move image, Lin, et al. [12] proposed a method based on the principal component analysis (PCA). The method begins by dividing an image into overlapping blocks of identical size. Features extracted for each block are used as vectors, and these vectors are then sorted by using radix-sort. The differences in positions (shift-vector) are calculated for each adjacent pair of feature vectors, and then the cumulative numbers of each vector are calculated. In the case of a large value of the accumulated, there is a potential to have a duplicate region. The feature vectors are indicated and the corresponding shift-vectors that have large cumulative are considered as tentative result. Finally, a medium filter was used to get the final result. This method is effective in detecting counterfeit regions even though the image is added with Gaussian noise or/and compressed by JPEG-compression. However, the method has a limitation in detracting a small region and it is limited to high rotation angles.

In another application, Kumar, et al. [13] suggest a method to improve the discrete cosine transform (DCT) algorithm. In particular, they focused on optimizing the speed of the algorithm. Inputting a grayscale image to the algorithm was the first step. The image was then divided into several overlapping-blocks. DCT was applied on each block to represent the block-features. Row vectors were sorted after representing the block features. Matching was executed and the blocks that do not belong to the group were canceled. In the final step, the duplicate regions were highlighted. Other scholars stated that this method is faster than other existing methods. It is also compatible with JPEG compression and Gaussian noise. Nevertheless, it can only deal with a small degree of rotation and scaling. Amerini, et al. [14] proposed a method based on Scale-invariant feature transform (SIFT) to get the features of the blocks and used those features to detect a counterfeit region in a picture exposed to geometric transforms. SIFT algorithm uses the similarity between original zones and cloned zones to detect forgery while the keypoints are extracted from the forged parts that are identical to the keypoints of the original zones. The author stated that the method has limitations in detecting high-texture and false positive ratio was not used to measure it performance. Moreover, Pan and Lyu [15] proposed a method based on SIFT to detect duplicated zones. It begins with estimating the transform matching without considering the lighting and geometric transformations. Then, the pixels for the counterfeit zones are determined by subtracting the estimated transformation. This method cannot find the credible keypoints in zones with little visual-structures and is limited to detecting small zones that have slight keypoint.

Conversely, there are several proposed methods that integrate more than one method to detect copy-move. The integration of these techniques enhances the performance of the copy-move detection methods to make them more accurate and give better results. In this manner, Ghorbani, et al. [16] proposed a method to detect copy-move forgery based on DWT and DCT-QCD. The steps involved in this method are as follows: Firstly, DWT is applied to a grayscale image to extract only low frequency sub band (Ir×c). Then, DCT-QCD is applied to reduce row vector length. In order to compute shift-vector for each row-vector in the matrix, each row-vector must be sorted lexicographically, in the third step. Finally, the row vector compared with the shift vector to find the similar region. However, this method cannot detect a duplicate region that has been rotated and scaled.

Additionally, Shabanifard, et al. [17] proposed a method based on Zernike moments and pixel-pair histogram. This method involves the following steps: Firstly, calculating the pixel-pair histogram and its binary from the absolute value of the first 36 Zernike-moments of the image. Secondly, selecting the features that produce the maximum of class secession. Some other features that acquired from Fourier transform are also used for more secession. Finally, classifying the input image into four categories by using the support vector machine-classifier. According to the authors, this method does not support detection of geometric transforms such as rotation and rescaling. On the other hand, Sunil, et al. [18] proposed a method based on DCT and PCA. The input image was grayscaled and if the image was colorful it would be converted to grayscale. The further step was to divide the input image into blocks. Then, DCT was applied on each block. The resulting row vector was saved with zigzag order and stored in the matrix. Then, DC was used to get samples and PCA was applied on a matrix of the row vector to minimize the matrix dimensions. To produce (A) matrix, the row vectors in (A) matrix was sorted by their similarity. They were finally matched to find the duplicate region. The author stated that this method has limited to detect scale and rotation.

III. Integrated Copy-Move Forgery using Block-Based and Keypoint Methods

In this study, we combine two features extraction methods to get the ideal solution to detect copy-move image forgery. The first method namely, the Discrete Wavelet Transform (DWT) is chosen from the block-based group to reduce image dimension (i.e., less features and fewer calculations). On the other hand, the second method, namely the Speed up Robust Features (SURF) is selected from the keypoint group is due to the main advantage of SURF that is to extract robust features from the image. Figure 5 explains the steps flow of the method, starting from features extraction methods, followed by the matching process and finally Identifying the copy-move regions.

Firstly, the input image (I) of BMP format and size 512×512 is decomposed into RGB components. Next, the DWT is calculated for each RGB channel of the input image. As a result of applying DWT, each channel gets divided into 4 sub-bands (Red channel [LLr, LHr, HLr and HHr], Green channel [LLg, LHg, HLg and HHg] and Blue channel [LLb, LHb, HLb and HHb]. Then, we compose the RGB channels component of LLr, LLg and LLb sub-band only from each channel to represent the input image with less features (IL). Next, we convert the new resulting image (IL) into grayscale using Equation (1):

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

where, R refers to the red color, G refers to the green color, and B refers to the blue color.

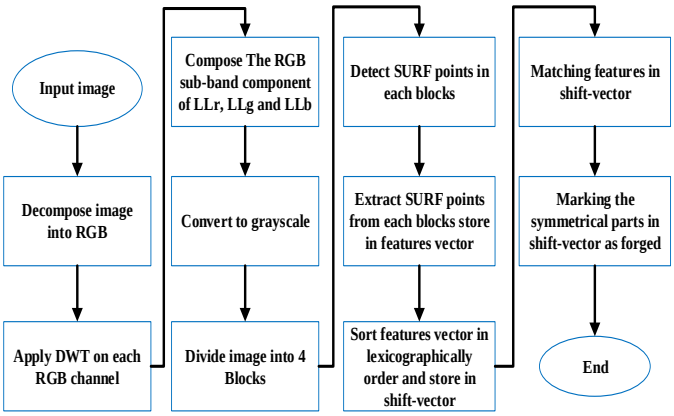

Figure 5: Proposed method framework

After that, we divide the image into four blocks, detect the SURF points on each block and extract the key features of each block and represent as features vector. Next, we sort the features vector in lexicographically and represent as shift-vector and then, match the shift-vector to determinate the symmetrical nearest neighbor of SURF points. The matching method results the distance between two nearest neighbors of SURF points. This distance is usually known as a threshold. If the distance between two SURF points is less than the specified threshold, then the matched points are acceptable. On the other hand, if the distance between the two SURF points is greater than the specified threshold, the points are rejected. Based on the experiments the threshold in this study has been set to 0.65. Finally, all the identical SURF marked as forged points as shown in Figure 6.

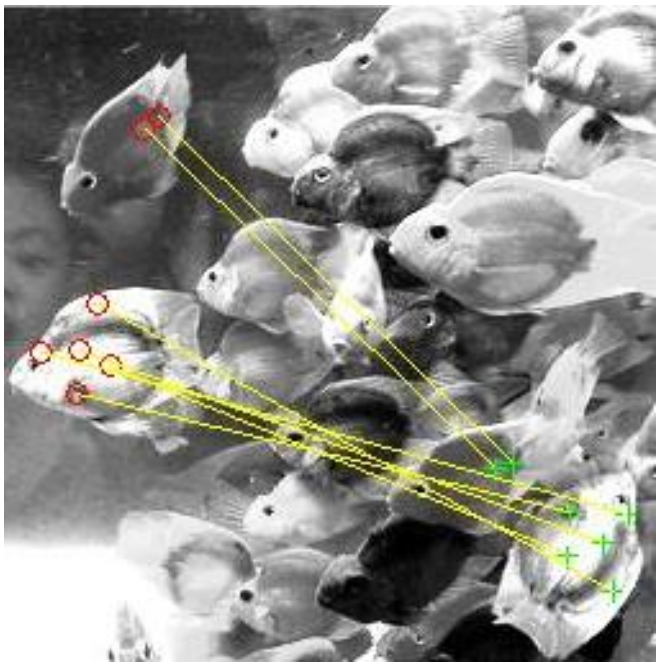

Figure 6: Marks of the identical SURF points in forged image

IV. EXPERIMENTS RESULTS

The study used two main datasets to evaluate the performance of the proposed method. The first dataset is a collection of 50 BMP images with 512 × 512 pixels. From the 50 images, 25 images are forged images, and the rest are genuine images. The second dataset is MICC-F2000 it was presented by Amerini, et al. 14, which comprises several JPG images with 2,048 × 1,536 pixels. From these images, 50 were acquired for the evaluation of the proposed method; 25 of the images are forged while the rest are genuine images. The forged images in both datasets are created by selecting an image region and copy–moving it on an image after applying a number of various attacks, such as rotation, translation, scaling or set of them.

Table 1 presents the geometric transformations for the type of attacks applied to the forged area in the MICC-F2000 dataset. In particular, this table provides the degrees of the rotation angle and scaling factors S_x ,S_y for all the attacks added to the x and y axes of the copied region (e.g., x and y axes are rotated by 35° and scaled by 20%).

Table 1
Geometric transformations (i.e., a…z) added to the cloned parts for the experimental dataset.

Attack	θº	S_x	S_y	Attack	θº	S_x	S_y
a	0	1	1	n	30	0.7	0.9
b	0	0.5	0.5	o	180	1	1
c	0	0.7	0.7	p	180	0.5	0.5
d	0	1.2	1.2	q	180	0.7	0.7
e	0	1.6	1.6	r	180	1.2	1.2
f	0	2	2	s	180	1.6	1.6
g	0	1.6	1.2	t	270	1.1	1.6
h	0	1.2	1.6	u	180	0.7	0.9
i	5	1	1	v	270	1.6	1.2
j	30	1	1	w	180	1.2	1.6
k	70	1	1	x	270	1	1
l	90	1	1	Y	270	0.5	0.5
m	40	1.1	1.6	Z	270	0.7	0.7

The method has been implemented in MATLAB 2014b on a machine equipped with Intel Core i5 2.20 GHz processor and 8 GB DDR3RAM. Some photos of the first dataset were captured using a SONY A77 camera.

The performance of the proposed method on all 100 images from both datasets are evaluated based on sensitivity, specificity, and accuracy. The evaluation is defined as follows:

The sensitivity refers to the capability of the method to detect a counterfeited image properly as counterfeited [14]. The sensitivity of a method measured by following equation:

$$Sensitivity = \frac{TP}{TP + FN} \quad (2)$$

The specificity refers to the capability of the method to identify a genuine image properly as genuine [19]. The specificity of an method is measured by the following equation:

$$Specificity = \frac{TN}{TN + FP} \quad (3)$$

Consequently, a good value of specificity and sensitivity reveal best performance (accuracy) of the method [20]. The accuracy of the method is measured by the following equation:

$$Accuracy = \frac{TP + TN}{TN + FP + TP + FN} \quad (4)$$

where:
TP = number of fraud images correctly identified as fraud.
FN = number of fraud images identified as genuine.
TN = number of genuine images identified as genuine.
FP = number of genuine images identified as fraud.

The proposed method performance for its sensitivity, specificity and accuracy is summarized in Table 2.

Table 2
Evaluation result of the proposed method

Number of genuine images	Number of forged images	TP	TN	FP	FN
50	50	47	48	2	3

From Table 2, it has been shown that the proposed method is superior in detecting copy-move images. The overall accuracy of the proposed method is 95% on the 100 image dataset (50 genuine and 50 forged images). The proposed approach gave sensible values of specificity and sensitivity achieved at 96% and 94%, respectively.

The accuracy of the proposed method was then compared with Pan and Lyu [15] and Amerini, et al. [14]. Pan and Lyu [15] achieved an accuracy of 83% on images of (800 x 600) pixel with forged region of small rotation angle. While, Amerini, et al. [14] attained an accuracy around 93% on JPG image of (2048 x 1536) pixel. On the other hand, the proposed method attained an accuracy of 95% over 100 images as shown in Figure 7.

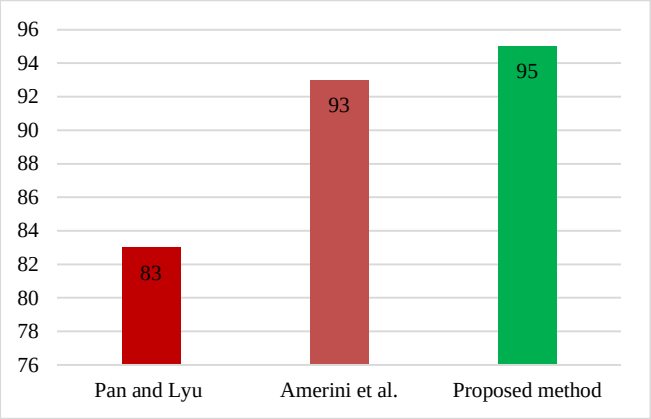

Figure 7: The performance comparison indicated by the percentage of accuracy between the proposed method and Pan & Lyu's [15] and Amerini et al.'s [14]

V. CONCLUSION

This study integrates two methods namely DWT and SURF to detect copy-move attacks. DWT decreases the image information to analyze the relevant data and reduces the computational complexity. SURF introduces the effectiveness in dealing with geometric transformation with various attacks including rotation, translation, scaling or set of them. The method has been tested with a dataset of 100 images with 50 genuine and 50 fraud images. The experiments results demonstrate that the proposed method has achieved significant performance shown by the accuracy value achieved at 95%, with a specificity of 96% and 94% of sensitivity. The future work of this study is to investigate the

proposed method with datasets consisting of different images format and larger image sizes.

REFERENCES

[1] S. Bravo-Solorio, A. K. Nandi, P. S. Burvin, and J. M. Esther, "Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling.," Paper presented at Conference on the Acoustics Speech and Signal Processing ICASSP Analysis of Digital Image Splicing Detection of Computer Engineering , vol. 16, (2014) 10-13.

[2] H. Farid, "Image forgery detection," Signal Processing Magazine, IEEE, vol. 26, (2009) 16-25.

[3] J. Fridrich and H. T. In, "Four and Six ." vol. 2014 SRC (2013) 179-218.

[4] M. D. Ansari, S. Ghrera, and V. Tyagi, "Pixel-Based Image Forgery Detection: of Education, , ." vol. 55, (2014) 40-46.

[5] W. N. Nathalie Diane, S. Xingming, and F. K. Moise, "A Survey of Partition-Based Techniques for Copy-Move Forgery Detection," The Scientific World Journal, vol. 2014, (2014).

[6] I. J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, Digital watermarking vol. 1558607145: Springer, (2002).

[7] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, (1996) Handbook of applied cryptography: CRC press.

[8] G. K. Birajdar and V. H. Mankar, "Digital Image Forgery Detection Using Passive Techniques: Digital Investigation, , ." vol. 10, (2013) 226-245.

[9] S. A. Chatzichristofis, K. Zagoris, Y. S. Boutalis, and N. Papamarkos, "Accurate Image Retrieval Based on Compact Composite Descriptors and Relevance Feedback Information.," International Journal of Pattern Recognition and Artificial Intelligence, vol. 24, (2010) 207-244.

[10] N. Thakur and H. Kundra, "on the Digital Image Copy Move Forgery Detection Techniques.," International Journal of Advances in Science and Technology IJAST Special Issue, (2015) 0-66.

[11] P. Kakar and N. Sudha, "Exposing Postprocessed Copy-Paste Forgeries through Transform-Invariant Features.," on Information Forensics and Security, vol. 7, (2012) 1018-1028.

[12] H. Lin, C. W. Wang, and Y. T. Kao, "Fast Copy-Move Forgery Detection.," on Signal Processing, vol. 5, (2009) 188-197.

[13] S. Kumar, J. Desai, and S. Mukherjee, "A fast DCT based method for copy move forgery detection," in Image Information Processing (ICIIP), 2013 IEEE Second International Conference on, 2013, (2013) 649-654.

[14] I. Amerini, L. Ballan, R. Caldelli, A. Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," on Information Forensics and Security, vol. 6, (2011) 1099-1110.

[15] X. Pan and S. Lyu, "Detecting image region duplication using SIFT features," in ICASSP, (2010) 1706-1709.

[16] M. Ghorbani, M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in Systems, Signals and Image Processing (IWSSIP), 2011 18th International Conference on, (2011) 1-4.

[17] M. Shabanifard, M. G. Shayesteh, and M. A. Akhaee, "Forensic Detection of Image Manipulation Using the Zernike Moments and Pixel-Pair Histogram.," Processing, vol. 7, (2013) 817-828.

[18] K. Sunil, D. Jagan, and M. Shaktidev, "DCT-PCA based method for copy-move forgery detection," in ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol II, (2014) 577-583.

[19] K. Li, C. Xiao-ping, L. Li, S. Li, H. Zhu, S. C. Chu, et al., "Copy-Move Forgery Detection in Digital Image.," Paper presented at the 3rd International Congress on Image and Signal Processing CISP An Efficient Scheme for Detecting CopyMove Forged Images by Local Binary Patterns Journal of Information Hiding and Multimedia Signal Processing, vol. 4, (2013) 46-56.

[20] J. Qiao, Z. Du, Y. Zhang, H. Du, L. Guo, M. Zhong, et al., "Proteomic identification of the related immune-enhancing proteins in shrimp Litopenaeus vannamei stimulated with vitamin C and Chinese herbs.," Fish & shellfish immunology, vol. 31, (2011) 736-745.