Applied Information Technology And Computer Science Vol. 2 No. 2 (2021) 021-036
© Universiti Tun Hussein Onn Malaysia Publisher's Office

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

A comparison between Speeded Up Robust Features (SURF) and Discrete Wavelet Transform (DWT) as feature extraction in Copy-Move Forgery Detection

Balqis Bohari, Nordiana Rahim*

Fakulti Sains Komputer dan Teknologi Maklumat,
Universiti Tun Hussein Onn Malaysia, Parit Raja, 86400, Malaysia

DOI: https://doi.org/10.30880/aitcs.2021.02.02.002
Received 15 June 2021; Accepted 09 September 2021; Available online 30 November 2021

Abstract: The development that these day era has results in numerous new technological revolutions inclusive of photo enhancing software program. Modern and easy-to-use enhancing software program has allowed the content of the digital images less difficult being tampered with. Therefore, the validity, credibility, and authenticity of such digital images have come to be an important concern. There are many varieties of forgeries, however, copy-pass forgery is the maximum hard to detect as it has the consistency of noise variables, colour palette, dynamic range, and maximum different basic properties with the rest of the photo, so it will now no longer be observed. Look for anomalies in special parts of the statistical measurement. There are classes for copy-move forgery detection (CMFD) which are (a) Keypoint based and (b) Block based. The block-based techniques are beneficial for the precise identification of forged regions, however, are surprisingly complicated in computer technology. That is why the alternate ways to solve the problem by the usage of keypoint based that is concerning different function vectors to lessen the computational complexity. This thesis reviewed the differences in keypoint methods the usage of the SURF (speeded up robust features) method and the block-based method the usage of the DWT (discrete wavelet transform) method using the MATLAB platform. The overall performance of those techniques is applying using dataset MICC-F220.

Keywords: digital image, copy-move forgery detection, SURF, DWT

1. Introduction

The issue of image forgery is nothing new. Moreover, with the availability of various social media makes people more likely to edit pictures and improve the quality of pictures to be more beautiful and attractive.

Various types of forging are used in the context of digital image forgery. Image tampered is targeted at acquiring fraudulent gains or misconceptions. Today, information in the form of a digital image

*Corresponding author: nordiana@uthm.edu.my cannot be genuine and should not be acknowledged readily without verification. Like mention before, the photos forged have a negative effect on those who see them and they can lead to misunderstandings of events and individuals. Manipulated photographs are most also used in courts of law as evidence [1]. For example, dashboard camera images are sometimes used by a court of law to provide solid evidence either by the defense or the prosecution. If trust in these images is called into question and the jury is unable to place the greatest possible trust in them, then the trial will be called into question. Therefore, the identification of fraud and forgery within these images is of the utmost importance.

There are two types of approaches can be used for digital image forgery detection which are active approach and passive approach. Active approach is largely focused on digital watermarking and signatures. In comparison to active approach, passive approach does not focus on pre-registration or pre-embedded knowledge and have not been extensively researched [2].

In passive approach, there are many types of image forgery such as copy-move, image splicing, image retouching and image morphing [3]. This paper discussed about copy-move forgery detection that obviously will be detecting copy-move forgery. In copy-move forgery, part of the image is copied to some other part of the same image and transferred to it. The origin of the forgery is however in the picture itself [4]. It is difficult to detect this forgery since the distorted fragments have the same characteristics as the rest of the original image. [5] stated in their research paper that in many of the image forgery techniques, copy-move forgery and copy-move forgery detection is being used widely for study case. The objectives of this research are:

- To study about Speeded Up Robust Features (SURF) algorithm and Discrete Wavelet Transform (DWT) algorithm.
- To analyse about Speeded Up Robust Features (SURF) algorithm and Discrete Wavelet Transform (DWT) algorithm.
- To compare about Speeded Up Robust Features (SURF) and Discrete Wavelet Transform (DWT) in their accuracy rate.

This research focusing mainly on the copy-move forgery that are found in digital images. The study covers common features of copy-move forgery. Besides that, the study only limited to study the algorithms using Speeded Up Robust Features (SURF) as feature extraction and another algorithm using Discrete Wavelet Transform (DWT) as feature extraction to detect copy-move forgery in an image.

2. Literature Review

2.1 Mechanisms in Image Forgery Detection

There are two types of approaches available for detecting digital image forgery. First, active approach and the other is passive approach as shown in Figure 1. The whole explanations for Figure 1 below will be at the next section.

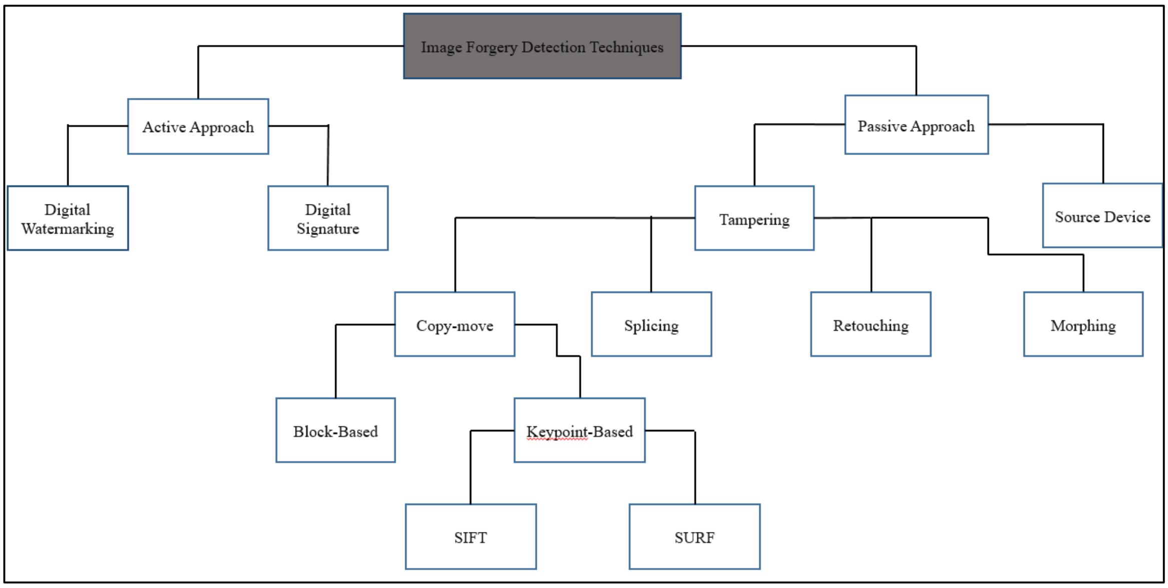


Figure 1: Image Forgery Detection Techniques

As shown in the Figure 1 above, the first approach which is the active approach also known as image authentication techniques is typically focused on digital signatures or digital watermarking (data hiding). In these approaches, a watermark or digital signature is inserted in an image to verify the validity of an image at the moment of capture or immediately after the image is taken. This is the biggest downside of the technique of active authentication. Firstly, since any captured image cannot be embedded with watermarks / signatures, and secondly, the deterioration of image quality caused by this embedding cannot be reasonable to users.

For the second approach which is passive approach uses the received image only to verify its validity or credibility, without the original image being signed or watermarked by the sender. It is focused on the assumption that while digital forgeries which leave no visual clues of being tampered with, the underlying statistical property or image continuity of a natural scene image that incorporates new objects resulting in different types of inconsistencies may be highly likely to be disrupted. To check its genuineness, passive use image statistics or image content.

Figure 1 also shown the types of Image Forgery. There are different classes of image forgery, such as:

- Copy-move

Copy-move forgery is the hardest type of forgery to detect. Copy-move distorted an image by replicating a part of the picture in a different position within the same picture.

Figure 2 below shows the example of the copy-move forgery happened in an image where you can see there are the original image and forged image which is the part of the image being copied and pasted at the other part of the same image as shown in yellow circles. Copy move forgery is nevertheless a major challenge because the copy move region forms part of the same picture. It is also more difficult to classify the manipulated zone in the same image compared to the field of many other image statistical approaches, like image splicing[1]. The origin of the falsification is therefore in the frame itself. Thus the feature matching-based technique is useful for detecting such falsifications[2].

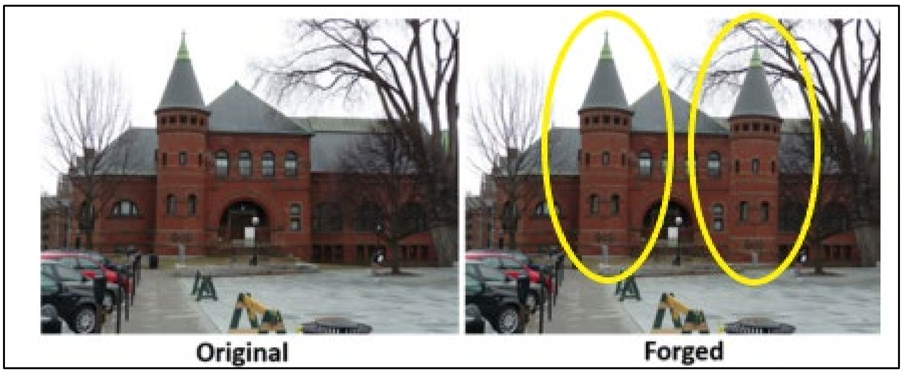


Figure 2: Example copy-move forgery[2]

- Image Splicing

The splicing of images is one of the basic and typical image processing schemes. The splicing of images is a crucial task in the detection of image forgery[3]. Image Splicing is a technique consisting of a combination of two or more images merged to create a false image[4]. Forgery for image splicing is used to copy and paste a different image on the image to create the forgery. It refers to a paste-up created using digital software, for instance Photoshop, to the relation of images. The main difference between this kind of forgery and copy-move falsification is that the origin of the forgery does not lie within the picture itself [2].

- Image Retouching

Retouching images can be seen as the less damaging kind of digital image falsification. Retouching images does not alter an image substantially, but improves or diminishes the characteristics of the image. It is popular with photo editors of magazines. It can be said that almost every cover of the magazine uses this technique to add some of the characteristics to an image, which is more appealing[4].

- Image Morphing

Image morphing is a combination of generalized image warping with a cross-dissolve between pixels. It is a special effect in movies and animations that transforms one picture or type into another by a smooth transition. It is used most frequently to represent someone who becomes another through technology or a dream or a surreal series.

2.2 Classification of Copy-Move Forgery Detection methods

Two different classes can be categorized as the copy-move forgery detection method which are block-based method and keypoint-based method. The images are divided into fixed dimensions in block-based methods, which overlap or not overlap blocks. Whereas in keypoint-based techniques certain interest points or keypoints are identified on the basis of which forged regions are identified. A significant number of investigators have worked separately to identify region of copy-move forgery based either on the block method or the keyboard method[5].

For the keypoint-based method, there are two techniques being discussed which are Scale Invariant Feature Transform (SIFT) and Speeded Up Robust Features (SURF).

- Scale Invariant Feature Transform (SIFT)

David Lowe released SIFT in 1999 [6]. The content of the imaging is translated into coordinates for local features, which are different in terms of rotation, scale, rotation and other parameters for imagery. Using the local features in a SIFT image descriptor, the matching process is performed to fetch the copy-move region into the image[6]. SIFT Algorithm comprises of four major steps which are Scale –Space extrema detection, Key point localization, Orientation assignment, Key point Descriptors. SIFT can transform pictures into local features vectors that then act as a key-point to identify objects. The detector SIFT is based on a Laplacian-of-Gaussian (LoG) approximation for Gaussian differences (DoG)[7].

- Speeded Up Robust Features (SURF)

SURF was first developed by Bay and Ess in 2008 [8]. SURF came from improvement of SIFT. These keypoint approaches can effectively detect duplicate areas and do well for geometric distortions such as transitions, scaling and translations[9]. SURF is more robust than SIFT which is can handle noise, detection displacements, and geometric and illuminated deformations other than can maintain the scaling and rotation invariance in a digital image. Because of the robustness that SURF has, the method for detecting forgeries in digital images can quickly be changed to detect forgeries. The SURF algorithm has been shown to be less complex in data processing which is means computationally faster than the commonly known Scale Invariant Feature Transform (SIFT) algorithm used in keypoint-based copy moving forgery detection techniques[8].

In block-based, contrast with keypoint-based, it is actually more time consuming and higher in computational complexity. In many techniques used for block-based method the differences of them are in the feature used to match the blocks. The popular techniques used in block-based method are Discrete Cosine Transform (DCT), Fourier Mellin Transform (FMT) and Discrete Wavelet Transform (DWT). These three techniques are based on transform domain. Below is the explanation of the techniques:

- Discrete Cosine Transform (DCT)

CMFD method using DCT based first being proposed by [10]. DCT applied to all small image blocks and quantified DCT coefficient in this process. Then mark the block as tempered part of the image after this similar DCT coefficient. When the tempered image is first separated into certain overlapping blocks of specified sizes and DCT is computed for each of those blocks. The quantified image information-containing coefficients are useful in the identification of duplicate image blocks.

- Fourier-Mellin Transform (FMT)

Bayram et al. in 2009 has proposed this method for CMFD [11]. Counting bloom filter method is used to improve detecting process of this method. This method is invariant with rotation (up to 10) and scaling (up to 10)

- Discrete Wavelet Transform (DWT)

DWT is known for its multi-resolution capabilities in time and frequency for image processing proposed by [12]. In DWT, the forged image is decomposed by wavelet transform into frequency sub-bands. The image is normally divided by four sub-bands, like approximation, horizontal, vertical and diagonal, integrating the information in its entirety. Low-frequency approach sub bands play a crucial role in the detection of duplicate picture regions, as they contain full image detail. Similarly, provided that diagonal sub-band has minimal details, the number of wrong matches can be regulated during duplication detection [13]. According to [13], DWT transforms the wavelet (down-sampling), where the image size is halved by any scale. DWT can be very useful for data compression application, but in applications such as filtering, detections, patterns, texture analysis it does not produce many successful results. This is because DWT is not shifting invariant.

3. Methodology/Framework

Here, will describe about the Speeded Up Robust Features (SURF) feature extraction and Discrete Wavelet Transform (DWT) feature extraction in forgery detection algorithm.

3.1 Speeded Up Robust Features (SURF)

The SURF algorithm has been shown to be less complex in data processing which is means computationally faster than the commonly known Scale Invariant Feature Transform (SIFT) algorithm used in keypoint-based copy moving forgery detection techniques [8]. SURF being developed to ensure the very high speed in the three of the feature detection steps which are detection step, description step and matching step.

According to [7], SURF algorithm can has four main steps: Hessian Matrix, based on a point detector in the size field, the direction of the interest point, orientation segmentation and the number of Haar wavelet responses. A keypoint detector and descriptor are defined in this SURF approach which is function as object recognition, registration, classification or 3D reconstruction[14]. The detector detects the points of interest in the picture and the descriptor illustrates the properties of the points of interest and generates the vectors of the points of interest.

Keypoints are found using a so-called quick-hessian detector which is based on the Hessian matrix approximation for a certain image point. The keypoints extract process from the test image and from the suspect area starts when the hessian matrices are obtained. For selecting region and size, SURF relies on the Hessian Matrix determinant. This is the first main step. The determinant would then calculate the local changes around points and then pick features where the determinant is the limit. According to [15], Hessian Matrix can be computed as;

$$H(p, \sigma) = \frac{Lxx\ (p, \sigma)\ \ Lxy\ (p, \sigma)}{Lyx\ (p, \sigma)\ \ Lyy\ (p, \sigma)} \qquad Eq. 1$$

From the Eq.1 above, H(p, σ) is Hessian matrix with point p with coordinates (x,y)for the image and scale, σ. L_{xx} (p, σ), L_{xy} (p, σ), L_{yx} (p, σ) are Gaussian second-order derivative convolution given by d/dx2(g(r)). The SURF generates a circular region in all x-and-y directions denoted by dx and dy in a bike neighbourhood of the 6s radius, in a particular orientation, which is determined by Haar Wavelet responses, where the point at which the point was defined[15]. The second step is the direction of the points of interest by defining the maximal value for the extreme point and the hessian matrix. Then, the extreme points were generated in the 3x3x3 neighbourhood. Feature points are only chosen for points of values higher than 26 other neighbourhoods[7].

To improve the strength of detection in pre- and/or post-processing attacks, SURF descriptors built square region around the keypoints by identifying square areas and directed to the dominant direction. Each of these square regions is divided into 4 by 4 sub-sections. With each sub-region, dx wavelet is weighed in a horizontal and dy wavelet in the vertical direction using a Gaussian μ = 3.3s based in an interstitial stage. The number of absolute wavelet responses |dx| and |dy| have been determined as the initial collection of entries on the functional vector to also endorse improvements in the polarity of images strength. For all 4 x 4 sub-regions, a descriptor vector with 4-dimensional vector V is thus generated, as is defined in Eq.2 [16];

$$V\ =\ (\sum dx\ , \sum dy\ , \sum |dx|, \sum |dy|) \qquad Eq. 2$$

3.2 Discrete Wavelet Transform (DWT)

DWT can be used in two ways. First, one dimensional. Second, two dimensional. This paper chose two dimensional to be discussed. DWT uses images to decompose by reducing the image size or by eliminating image compression.

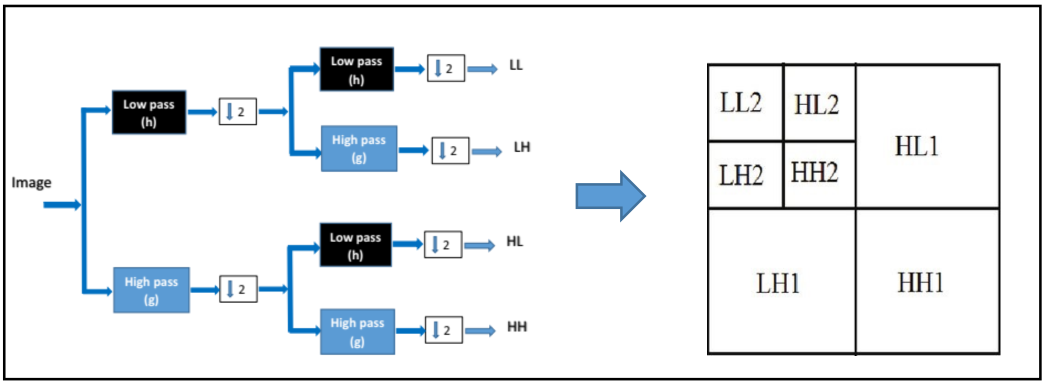


Figure 3: First level decomposition of two dimensional DWT [17]

Figure 3 above shown the first level decomposition of two dimensional DWT. The forged picture is decomposed into frequency sub-bands using wavelet transform. The image is generally divided into four sub-bands, such as approximation, horizontal, vertical and diagonal, of which the whole picture information can be given. A low frequency sub-band approximation plays a key role in finding duplicated picture regions since it provides the maximum picture detail. Likewise, as a diagonal sub-band contains minimal information, the number of false matches during duplication detection can be regulated. L refers to low-pass filtering and H refers to high-pass filtering. The image is separated into four parts after the first step of decomposition. The parts contain LL, HL, LH and HH. Where LL is the top left, HL and LH are the top right and bottom left, and the last block is HH, the lowest right quadrant. To perform second level disintegration, the DWT is connected to the LL1 band which deteriorates the LL1 band into the four sub-groups LL2, LH2, HL2, and HH2. With the use of discrete wavelet transformation, the method of feature extraction is faster and accurately. Then image will undergo feature matching to get the detection result.

Haar wavelet is being used [17], to applies ψHaar(x) and ΦHaar(x) as high-pass filter and low-pass filters, respectively as shown in Eq.3 and Eq.4 below.

$$\psi\text{Haar}(x) = \begin{cases} 1 & 0 < x > 0.5 \\ -1 & 0.5 < x < 1 \\ 0 & otherwise \end{cases} \qquad Eq.3$$

$$\Phi\text{Haar}(x) = \begin{cases} 1 & 0 < x < 1 \\ 0 & otherwise \end{cases} \qquad Eq.4$$

This algorithm depends upon the transformation of the Haar wavelet to remove the four bands (LL, LH, HL, HH) and to form a new block for every block. This block has the same size as the original block, but has Haar wavelet elements [17].

3.3 Research Framework

The framework for this research study explains about the process detection of copy-move forgery using the MICC-F220 dataset. Through this development of copy-move forgery detection framework the objective of the research study will be accomplished successfully. The figure 4 below shows the steps to conduct the study. The framework simplifies the process flow of this research classification into an understandable form. The whole explanation about the flow of the framework is explaining in the next section.

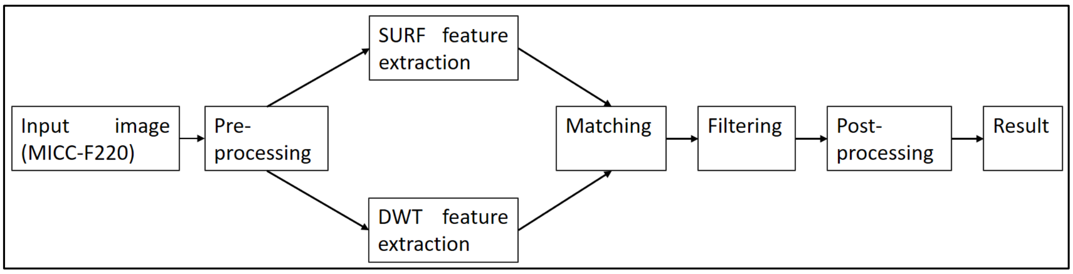


Figure 4: Framework to detect copy-move forgery

3.3.1 Pre-processing

Image preprocessing is done to reduce the redundancy of image information and increase the computing performance in the next stages of CMFD. The tasks consists of image RGB transforming to grey, image resizing and area recognition being altered [18]. So in phase, the image being divide into four sub-blocks, which do not overlap, to minimize the high and complicated measurement needed for block comparisons. There are three steps involved for this phase[18]:

- Grayscale conversion

The grayscale image pixel value varies between 0 and 255. By transforming a red image into a gray image, the RGB value (24 bit) is transformed into a graying image (8 bit). Various image recognition and programming methods transform the color image to the grayscale image. Gray is a collection of black-and-white monochromatic shades here. A grayscale picture thus includes no hue or gray tones. Three photographs (a red image size, a green scale and a blue scale) stacked over each other can be interpreted as RGB images. MATLAB is an RGB image that consists of a color pixel MxNx3 array where each color pixel is a three-fold color that fits the color red, blue and green at the space you mark. The algorithm for conversions are as stated below:

- Read RGB color image into a MATLAB environment
- Extract Red, blue, and green color components from RGB image into three different 2D matrices.
- Create another matrix with a similar number of rows and columns as RGB picture, containing all zeros.
- Convert each RGB pixel values at a location (i, j) to grayscale values by shaping a weighted sum of the Red, Green, and Blue color components and assign it to a corresponding location (i, j) in a new matrix.

- Contrast stretched images

The upper and lower pixel values over which the image is to be normalized need to be specified. These restrictions are also the minimum and maximum pixel values permitted for the type of image involved. For instance, the lower and the upper limits of 8-bit gray levels may be 0 and 255. Taking into consideration the higher and lower ranges as a and b. The goal is to decide the lowest and highest pixel values in the image. As c and d, name them. At that time, the following function is used to scale per pixel P[14].

- Binary image conversion based on thresholding

The threshold image shows a real numerical spectrum of some dimension that is incomplete. The multi-level threshold technique is to locate the thresholds dependent on the whole array's aggregate histogram. Thus the RGB picture is known to be the 3D number sequence and the thresholds for all three color planes are determined. The multilevel threshold processes the image A that restricts the histogram to be computed. Some + α and – α are used respectively in the first and last cases of the histogram. No feasible solution using Otsu technology can be found for degenerated sources where the number of unique values is not exactly or equal to N in A. The return threshold value for this input contains all specific values from A, and some extra values are imaginably picked discretionarily. The default value of the feature with a threshold level is 0.5[14].

3.3.2 Feature Extractions

For this researches study, the study comprises of two methods of features extraction for detecting copy-move forgery which are Speeded Up (SURF) and Discrete Wavelet Transform (DWT). These two methods are implemented in the chosen software MATLAB R2020b and it is classified based on its performance and accuracy rate in detecting the copy-move forgery.

3.3.3 Feature Matching

Feature matching is the phase designed where the images undergo to find the similarities between two images which is original image and tampered image. High similarity between two feature descriptors is interpreted as a cue for a duplicated region. Matching using unique technique can reduce the false matching. Unique matching return unique matches between feature vectors, the function performs forward-backward matches to select a unique match and keeps the closest.

3.3.4 Filtering

In the filtering process, based on the number of points in the statistical image block, false matching points are removed. The filter converts the image data into invariant coordinates in relation to local characteristics [19]. Filtering the image in an attempt to gain high detection accuracy. Filtering also functioned to remove false negative match in matching process.

3.3.5 Post-processing

This is the last stage of certain forgery procedures of copy-moves. Some filter operations are used to eliminate some false matches during this process. In the post-processing process to delete or minimize isolated regions, moral operations may also be used [13]. This step filters all the detected blocks and remove false positive to improve the detection accuracy [11]. Various post-processing operations may be carried out to mask the deceptive traces of images. The most frequently used post-processing operations include scale, adding noise, JPEG compression, blurring image, and rotation [5].

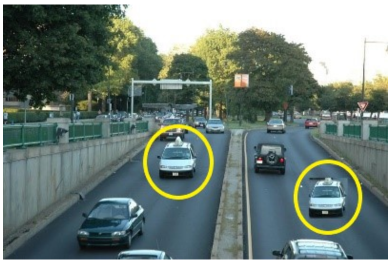
The purpose of this final phase is to maintain matches with a common behavior only. When a number of matches belong to a copied area, both source and target blocks are supposed to be spatially close together (or key points). Moreover, similar amount of translation, scaling and rotation are needed to matches derived from the same copy-shifting action [20].

4. Results and Discussion

4.1 Dataset and Performance Measure

To run the experiments study, the algorithms were tested and verified using the dataset of MICC-F220 with MATLAB R2020 software. A sample of tampering images of the dataset is shown in Figure 5 below where you can see in (a) is the original image and image (b) is forged image which is the part of the image being copied and pasted at the other part of the same image as shown in yellow circles. The tampered images are generated by, randomly copy-move image region(s), the copy image region(s) can be processed with the resizing, rotation, or other distortion and then be pasted to generate a spliced image. The post-processing (such as blurring) is considered after copy and paste operation to finish the tampered image generation.

(a)Original image



(b)Forged image

In experiment study, the original images are used just to generate the ground truth. Which is means, the original images in this dataset are not included in the experiment.

Performance of the algorithms be measured using Precision-Recall (PR). In this experiment, Precision-Recall (PR) are used to show the explaines algorithms perfomances. Precision shows that the probability that a detected forgey is truly a forgery while Recall shows the probability that a forged image is detected. The equation used to calculate the precision and recall are presented in Eq.5 and Eq.6 listed below. Also, to combine both precision and recall in a single value, it is computed as in equation Eq.7 below.

$$Recall = \frac{TP}{TP+FN} \qquad Eq.5$$

$$Precision = \frac{TP}{TP+FP} \qquad Eq.6$$

$$F1\,score = 2\,x\,(\frac{(P\,x\,R)}{(P+R)}) \qquad Eq.7$$

Here defined the terms;

TP (True Positive): Forged image identified as forged

FP (False Positive): Authentic image identifies as forged

TN (True Negative): Authentic image identified as authentic

FN (False Negative): Forged image identified as authentic

Table 1: Tabulation for confusion matrix for threshold of 0.5

Threshold = 0.5	Actual positives	Actual negatives
Predicted positives	(TP) 82	(FP) 40
Predicted negatives	(FN) 61	(TN) 21

Table 1 describes about the positive and negative points calculated at threshold 0.5. By which the true positive (TP), false positive (FP), true negatives (TN) and false negatives (FN) values are obtained. A sample calculation with threshold 0.5 is shown below:

Precision = TP/TP + FP = 0.67 = 67%

Recall = TP/TP + FN = 0.79 = 79%

F1 score = 2 x (Recall x precision) / (Recall x Precision) = 0.72 = 72%

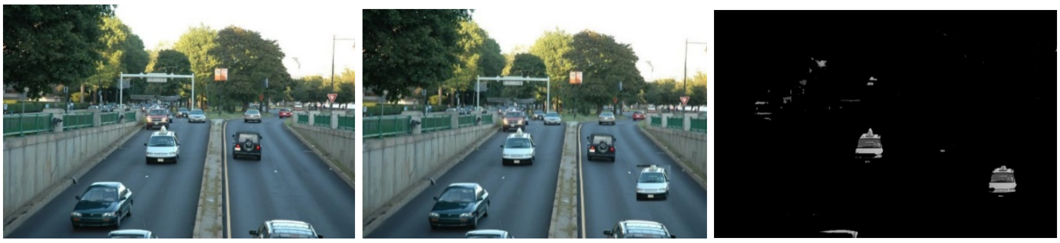
4.2 Copy-Move Forgery using SURF as feature extraction

Figure 6 shows the first three examples result of the experiment based on SURF feature extraction. In this algorithm, in order to locate the detected forgeries in the image, the image being detected by non-overlapping in irregular block compared to regular blocks to reduce the high and complex computation required in block comparisons. It also helps in extracting the size of the super pixels, S of the image before applying the SURF feature extraction to easier detecting the same region in the image.

Then, image undergo SURF feature extraction, which to extract the features points after finding the super pixels size. SURF designed with four steps which (1) scale space extrema detection (2) key-point localization (3) orientation assignment (4) descriptor generation. Initially using different values of sigma, in the Difference of- Gaussian (DoG) function as shown below in Eq.8, it is required to identify the location and scaling points, this is done by Scale space extrema.

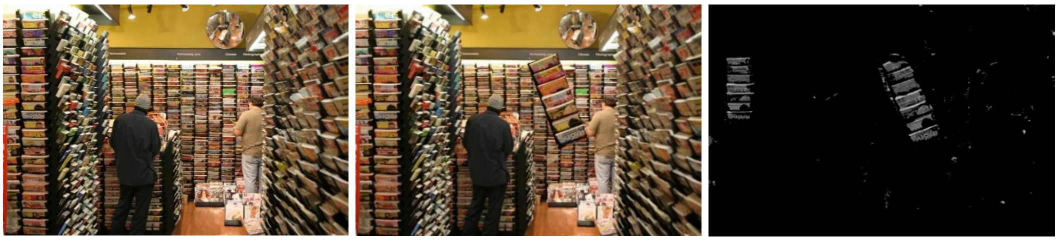
$$D(X,Y)\sigma = ((G(x,y,k\sigma)G(x,y,\sigma)I(x,y)) \quad Eq.8$$

Example 1:



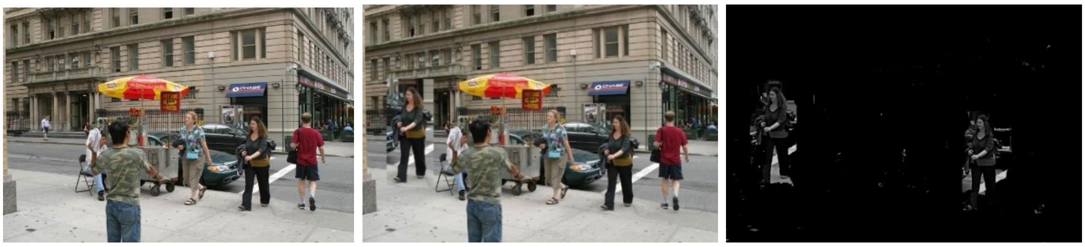
(a) Original image (b) Forged image (c) Locate the forged region

Example 2:



(a) Original image (b) Forged image (c) Locate the forged region

Example 3



(a) Original image (b) Forged image c) Locate the forged region

Figure 6: The examples of the result using SURF feature extraction

Figure 6 above shows the examples of the result using SURF feature extraction which is all respectively shows the (a) original image, (b) forged image and (c) locate forged region. The (b) forged image is the one being used in algorithms and (c) is the results of the algorithms in detection the region of being tampered which is shown there are two regions being detected which one region is original region and another region is tampered region.

4.2 Copy-move forgery using DWT as feature extraction

For the second algorithm which using DWT as feature extraction for finding the wavelet coefficients of the images. The wavelet transform is used to breakdown the forged image into frequency sub-bands. The image is typically divided into four sub-bands, such as approximation, horizontal, vertical, and diagonal, which when combined can provide all of the image's information. Because it carries the most image information, the approximation sub-band with low frequency is crucial for locating duplicate image regions. The diagonal sub-band can also be used to control the frequency of false matches during duplicate detection because it includes minimum information.

Figure 7 below shows the 2-level DWT decomposition of an image. With only a few coefficients, the discrete wavelet transform (DWT) can provide unique and discriminatory representations that can quantify vital and interesting structures (edges, details) with good resolution. These coefficients can be used as features immediately. The wavelet domain can be used to extract these characteristics, which describe the data anomalies. It basically reduces wavelet coefficient correlation and offers energy compression in a small number of wavelet coefficients. Approximations and detail coefficients are provided using wavelet analysis. The signal's high-scale, low-frequency components are the approximations. The details are the low-scale, high-frequency component. The wavelet transformation of an image helps in its analysis at various scales and orientations.

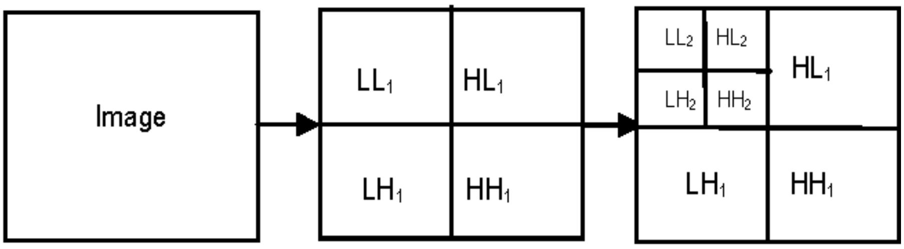
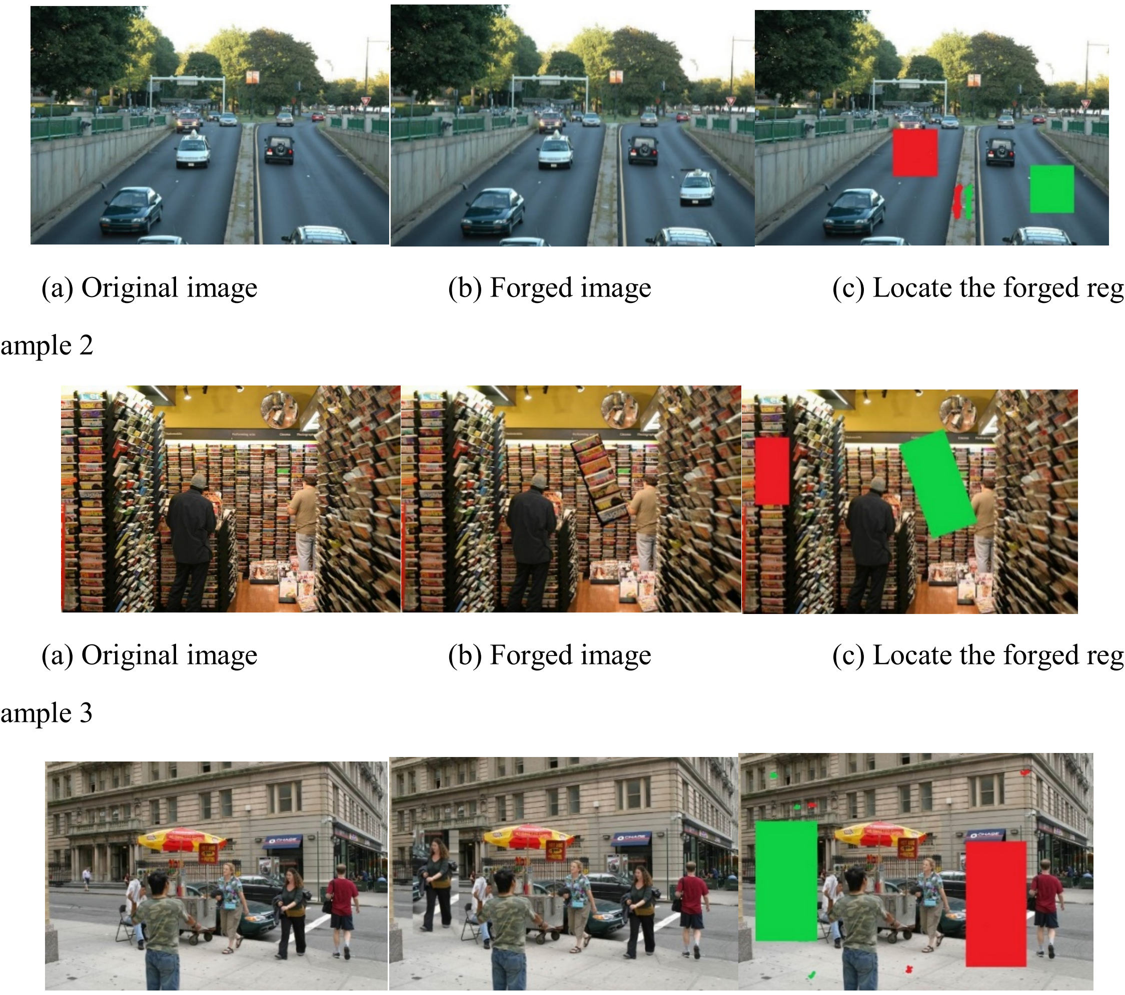


Figure 7: 2-level DWT decomposition of an image

Figure 8 below shows the first three examples result of the experiment based on DWT feature extraction. Which the red region shows the original region and the green region shows the forged region of the image.

Example 1



(a) Original image (b) Forged image (c) Locate the forged region

Example 2

(a) Original image (b) Forged image (c) Locate the forged region

Example 3

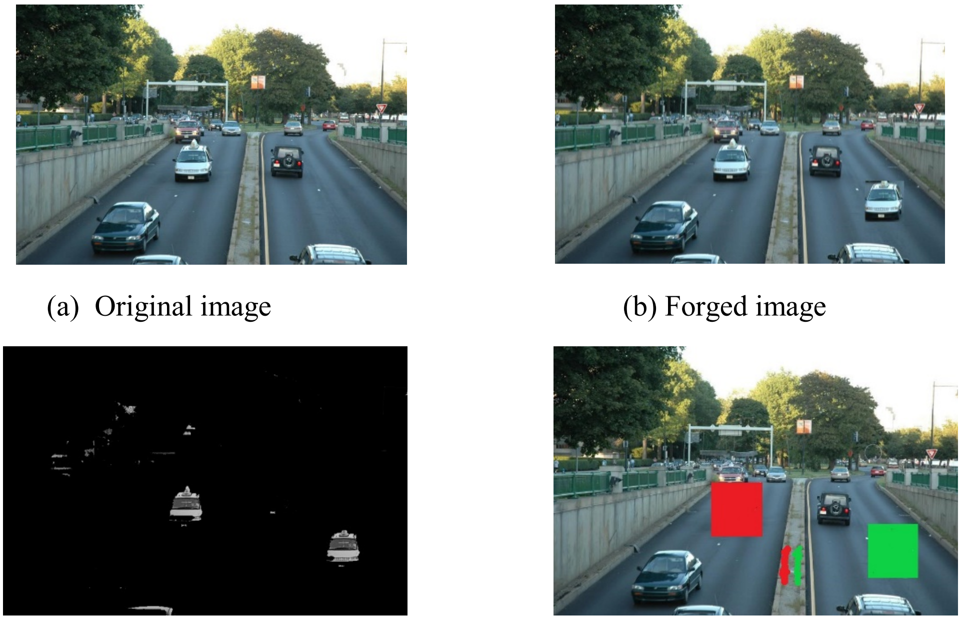
(a) Original image (b) Forged image (c) Locate the forged region

Figure 8: The first three examples of the result using DWT feature extraction

Figure 8 above shows the examples of the result using DWT feature extraction which is all respectively shows the (a) original image, (b) forged image and (c) locate forged region. The (b) forged image is the one being used in algorithms and (c) is the results of the algorithms in detection the region of being tampered which is shown there are two regions being detected which the red one is original region and green region is tampered region.

4.3 Comparison result between SURF and DWT as feature extraction

Here, the accuracy of algorithm in detecting forgeries and locating the duplicated region is examined and being compared. The following results belong to the experiments within two different algorithms with different type of feature extraction.



(a) Original image

(b) Forged image

(c) Locate the forged region using SURF

(d) Locate the forged region using DWT

Figure 9: Comparison result of the locate forged region using SURF and DWT

As shown in Figure 9, the result in (c) which applying SURF as feature extraction, the forged region detecting considerable well but there are many false positive points along the images. While in (d) shows the better result using DWT as feature extraction because the forged region detected better compared to in (c) and the false positive points lesser than in (c). Based on the displayed result, copy-move forgery detection using DWT as feature extraction shown the better accuracy which is more efficient to detect and localize the copy-move image forgery.

4.4 Performance detection result

Table 2 presenting the result of the performance detection from Figure 6 using algorithm with SURF as feature extraction.

Table 2 Performance detection result using SURF as feature extraction

	Precision %	Recall %	F1 Score %
Example 1	55.55	52.63	53.45
Example 2	74.00	59.00	65.00
Example 3	67.00	79.00	72.00

The result of the performance detection from Figure 8 using algorithm with DWT as feature extraction is presented as in Table 3.

Table 3 Performance detection result using DWT as feature extraction

	Precision %	Recall %	F1 Score %
Example 1	90.00	64.28	74.00
Example 2	89.00	76.00	81.00
Example 3	92.00	86.00	89.47

In this section, the performance of the forgery detection for both of the algorithms is evaluated and compared as above. Based on the displayed results, the algorithm using DWT as feature extraction was more efficient to detect and localize the copy-move image forgery as can see F1 score percentage for DWT shows the better value than SURF. But during experiments study, I found out there is a drawback using DWT as feature extraction which is because of the complexity of the algorithm, so there is very time consuming than using SURF as feature extraction.

5. Conclusion

In this thesis, two methods for detecting and verifying copy-move forgery on which two different and well-known feature extraction methods are used and compared in this problem. These two method are used feature extraction methods to select correspondences along in image by using different algorithms. This thesis was able to locate the duplication region and detect the forgeries with various combinations of operations and locate the portion of the image involved in the altering. By comparing both of the result, the final result of the approaches shows that, the algorithm using DWT as feature extraction can detect the forgery better and can locate it in the image more accurately but very time consuming compared to using SURF as feature extraction.

In future work, researchers can extend the comparison using different advance feature extraction by including different types of local descriptors such as LBP, HOG, WLD, etc. as well as make the method more accurate in the reviewed altering type.

6. Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support and encouragement throughout the process of conducting this study.

References

[1] M. H. Alkawaz, G. Sulong, T. Saba, and A. Rehman, “Detection of copy-move image forgery based on discrete cosine transform,” Neural Comput. Appl., vol. 30, no. 1, pp. 183–192, 2018, doi: 10.1007/s00521-016-2663-3.

[2] A. Roy, R. Dixit, R. N. Rajat, and S. Chakraborty, Studies in Computational Intelligence 755 Digital Image Forensics Theory and Implementation. 2020.

[3] G. K. Birajdar and V. H. Mankar, “Digital image forgery detection using passive techniques: A survey,” Digit. Investig., vol. 10, no. 3, pp. 226–245, 2013, doi: 10.1016/j.diin.2013.04.007.

[4] A. Kaur and J. Rani, “Digital Image Forgery and Techniques of Forgery Detection,” Int. J. Tech. Res. Sci., vol. 1, no. 4, pp. 18–24, 2016, [Online]. Available: www.ijtrs.com.

[5] S. P. Jaiprakash, M. B. Desai, C. S. Prakash, V. H. Mistry, and K. L. Radadiya, “Low dimensional DCT and DWT feature based model for detection of image splicing and copy-move forgery,” Multimed. Tools Appl., vol. 79, no. 39–40, pp. 29977–30005, 2020, doi: 10.1007/s11042-020-09415-2.

[6] R. Singh and R. P. Chaturvedi, “SWT-SIFT based copy-move forgery detection of digital images,” Int. Conf. Innov. Control. Commun. Inf. Syst. ICICCI 2017, pp. 1–4, 2019, doi: 10.1109/ICICCIS.2017.8660907.

[7] R. Nuari, E. Utami, and S. Raharjo, “Comparison of scale invariant feature transform and speed up robust feature for image forgery detection copy move,” 2019 4th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2019, pp. 107–112, 2019, doi: 10.1109/ICITISEE48480.2019.9003761.

[8] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-Up Robust Features (SURF)," Comput. Vis. Image Underst., vol. 110, no. 3, pp. 346–359, 2008, doi: 10.1016/j.cviu.2007.09.014.

[9] J. Ouyang, Y. Liu, and M. Liao, "Robust copy-move forgery detection method using pyramid model and Zernike moments," Multimed. Tools Appl., vol. 78, no. 8, pp. 10207–10225, 2019, doi: 10.1007/s11042-018-6605-1.

[10] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of Copy-Move Forgery in Digital Images," Int. J., vol. 3, no. 2, pp. 652–663, 2003, [Online]. Available: http://www.ws.binghamton.edu/fridrich/Research/copymove.pdf.

[11] T. Mahmood, T. Nawaz, M. Shah, Z. Khan, R. Ashraf, and H. A. Habib, "Copy-move forgery detection technique based on DWT and Hu Moments," vol. 14, no. 5, pp. 156–161, 2016.

[12] H. T. Hu, L. Y. Hsu, and J. Garcia-Alfaro, "Exploring DWT-SVD-DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression," Comput. Electr. Eng., vol. 41, no. C, pp. 52–63, 2015, doi: 10.1016/j.compeleceng.2014.08.001.

[13] B. Soni and D. Biswas, "Image Forensic using Block-based Copy-move Forgery Detection," 2018 5th Int. Conf. Signal Process. Integr. Networks, SPIN 2018, pp. 888–893, 2018, doi: 10.1109/SPIN.2018.8474287.

[14] S. Dhivya, J. Sangeetha, and B. Sudhakar, "Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique," Soft Comput., vol. 24, no. 19, pp. 14429–14440, 2020, doi: 10.1007/s00500-020-04795-x.

[15] A. Badr, A. Youssif, and M. Wafi, "A Robust Copy-Move Forgery Detection in Digital Image Forensics Using SURF," 8th Int. Symp. Digit. Forensics Secur. ISDFS 2020, 2020, doi: 10.1109/ISDFS49300.2020.9116433.

[16] K. H. Paul, K. R. Akshatha, A. K. Karunakar, and S. Seshadri, "SURF Based Copy Move Forgery Detection Using kNN Mapping," in Advances in Intelligent Systems and Computing, 2020, vol. 944, pp. 234–245, doi: 10.1007/978-3-030-17798-0_20.

[17] F. M. Al_azrak, Z. F. Elsharkawy, A. S. Elkorany, G. M. El Banby, M. I. Dessowky, and F. E. Abd El-Samie, "Copy-Move Forgery Detection Based on Discrete and SURF Transforms," Wirel. Pers. Commun., vol. 110, no. 1, pp. 503–530, 2020, doi: 10.1007/s11277-019-06739-7.

[18] Y. Y. Yeap, U. Sheikh, and A. A. H. A. Rahman, "Image forensic for digital image copy move forgery detection," Proc. - 2018 IEEE 14th Int. Colloq. Signal Process. its Appl. CSPA 2018, no. March, pp. 239–244, 2018, doi: 10.1109/CSPA.2018.8368719.

[19] W. C. N. Kaura and S. Dhavale, "Analysis of SIFT and SURF features for copy-move image forgery detection," Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017, vol. 2018-Janua, pp. 1–4, 2018, doi: 10.1109/ICIIECS.2017.8276160.

[20] F. O. Haimour, M. A. Khraiwesh, and D. M. A. Khraiwesh, "An Improved Method for Detecting Copy-Move Forgery in Digital Images," 2015.