

An Effective Blind Detection Technique for Medical Images Forgery

Dr. Sahab Dheyaa Mohammed

University of Information Technology and Communications, Baghdad, Iraq.

E-mail: sahab7dia@gmail.com

Taha Mohammed Hasan

Department of Computer Science, College of Science University of Diyala, Iraq.

Jumana Waleed

Department of Computer Science, College of Science University of Diyala, Iraq.

Received August 07, 2020; Accepted October 10, 2020

ISSN: 1735-188X

DOI: 10.14704/WEB/V17I2/WEB17072

Abstract

The progress in the technologies of communication has produced different methods of transferring and accessing medical images. The prevalent utilization of communication and information methods enables anyone to tamper the contents of the original images. Consequently, for protecting the privacy of the patients and for ensuring the accuracy of diagnostics, a technique for detecting medical images forgery is needed. In that respect, in this paper, an effective block based detection technique for medical images has been proposed. In this proposed technique the copy and move tampering in the medical images can be detected in the discrete wavelet transform (DWT) and the matching process of blocks can be speeded up by utilizing the automatic clustering. The experimental results explain that the proposed forgery detection technique of medical images is capable of successfully detecting copy and move tampering with low processing time and high accuracy.

Keywords

Medical Images, Blind Detection Technique, Copy and Move Tampering, Discrete Wavelet Transform (DWT).

Introduction

In the medical sciences, the usage of digital images has expanded extremely, consequently, the authenticity of these images should be provided. The medical images' authenticity is highly significant in the fields of government documents, scientific researches, forensic investigations, etcetera. The existence of user-friendly and powerful software of editing images like Photoshop makes tampering of digital images very easy.

Recently, this issue has been faced in medical imaging for the intention of fake insurance demands [1].

In recent, the techniques of image forensics have caught the attention to validate the authenticity of the medical images. These techniques give affirmations about the integrity of the images and provide evidence about the manipulations nature. In general, techniques of image forensics are evaluated under two main headings as active forensic techniques, and passive "blind" forensic techniques [2]. The techniques of medical image forensics are explained in figure (1).

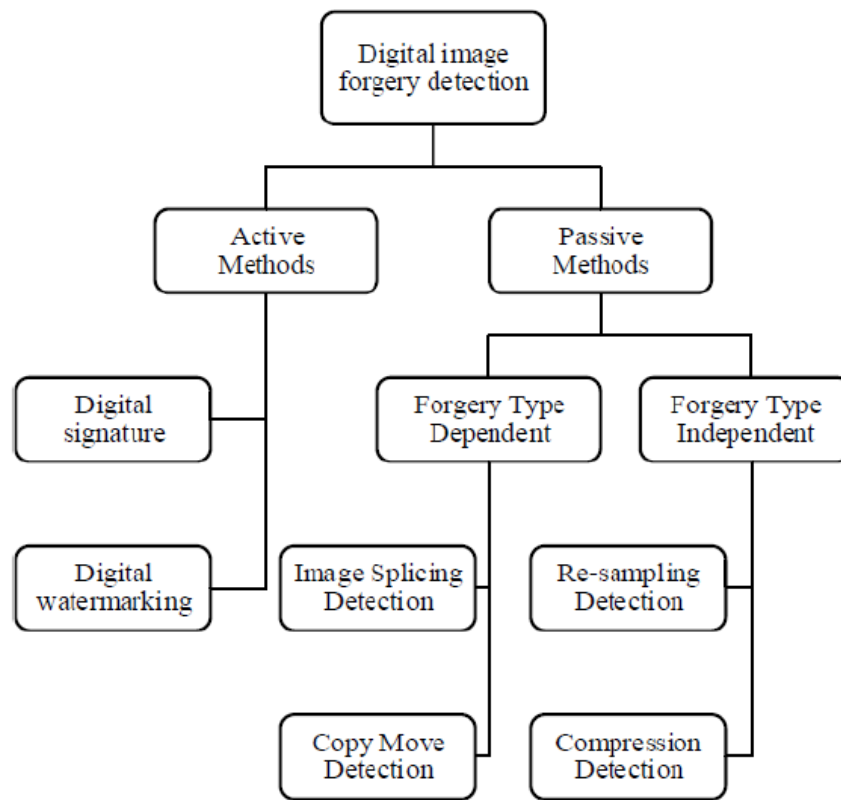


Figure 1 The techniques of medical image forensics

As active techniques, digital watermarking is utilized to hide an authentic watermark inside the image, and the digital signature is utilized to add signatures or digests. Although watermarking is an effective technique to verify the origins and integrity of images, its implementation needs that a watermark is hidden over the process of images generation, thus, its utilization is limited with the applications that capable of generating digital objects with built-in watermarking. Today, the most captured images are not watermarked. So, there is an intensive requirement for passive forensic techniques. These techniques are utilized to identify evidence left after tampering the image [3]. Among the

passive techniques, copy and move forgery is a common form of forgery, which is performed by affixing one or more regions in the image to the same image. Sometimes, diverse post-processes such as scaling, blurring, JPEG compression, and rotation are implemented before pasting the copied regions. Figure (2) shows an example of copy and move forgery [4].

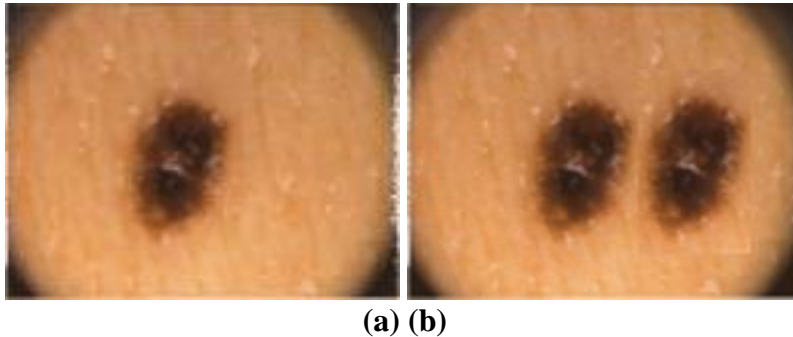


Figure 2 (a) Original medical image; (b) Fake medical image.

In the literature, several techniques for detecting copy and move forgeries are divided into block based techniques and key point based techniques according to the study structure [5]. In block-based techniques, first, the image is divided into square or circular blocks. Property descriptive vectors representing blocks are obtained using various property descriptor algorithms, and repeating blocks are found by matching the most similar vectors. In key point techniques, property identifiers of key points obtained from the image are matched [6]. This paper is aimed to achieve higher performance by supporting copy and move forgery detection (even if the copied regions were rotated) in a discrete wavelet transform (DWT) domain using the strategy of blocks matching.

In the rest of this paper, related works are explained in the next section, the details of the proposed technique and the algorithms used will be given in the third section and the experimental results will be given in the fourth section. General conclusion will be given in the last section.

Related Works

Various medical images forensic techniques were presented in the literature for verifying the authenticity and integrity of medical images. The most commonly used techniques are watermarking, and blind forensic techniques. The watermarking of medical images represents highly challenge, hence, several fundamental restrictions should be regarded through the process of watermarking. Hiding information in the cover image leads to distortions, which can be completely unsuitable for medical applications, as in the medical

image forensic technique based watermarking proposed in [7]. These distortions in the medical images make the using of watermarking not practicable to the physicians. So, there is a demand for developing the techniques of watermarking to be capable of restoring the content of the original medical images after extracting the watermark, as in the technique of reversible watermarking proposed in [8]. But the utilization of the watermarking technique is still required in a particular situation. While, blind forensic techniques are utilized to detect evidence left after tampering the medical images. H. Huang et. al [9] proposed a blind forensic technique to detect the medical images alterations such as compression, filtering, scaling and etc. This technique is depending on a set of (Histogram statistics of Reorganized Block-based Tchebichef moments) for building image features, and that are utilized as input to the classifiers to identify the integrity and authenticity of medical images. Also, S. Govarthini and M. Vadivel [10] proposed a blind forensic technique for medical images for detecting if the images have been altered via some processes. This technique works on comparing two sets of features: the first set is the histogram statistics of reorganized block-based Tchebichef moments, and the second set is the histogram statistics of reorganized block-based discrete cosine transform, and these sets are utilized as input to the support vector machine classifiers to identify the authenticity and integrity of medical images. T. D. Gadhiya et. al [1] presented a forensic technique for detecting and localizing medical images tampering. This technique is depending on the representation of hash-based for medical image and the DWT is utilized for detecting and localizing the tampering. This technique shows robustness against harmless modifications and very sensitive to a minute tampering. Most of these proposed blind forensic techniques are focused on the medical images alterations such as compression, filtering, scaling, and neglected the rotation.

The Proposed Medical Images Tampering Detection Technique

In the proposed tampering detection technique, firstly, the input medical image is converted into grayscale image, then decomposed using DWT, after that the LL sub-band is selected and separated into overlapping blocks. For every block, the features are extracted via separating it into nested frames and calculating the average to every frame. The extracted features are utilized in the step of clustering to group identical blocks into several classes. The feature vectors in every class are lexicographically sorted. A comparison is calculated between every close pair of blocks, when it is minimal than a specified threshold, two blocks are regarded as identical. And, for reducing false detection, the distance between these blocks is computed. Figure (3) illustrates the construction of the presented tampering detection processes.

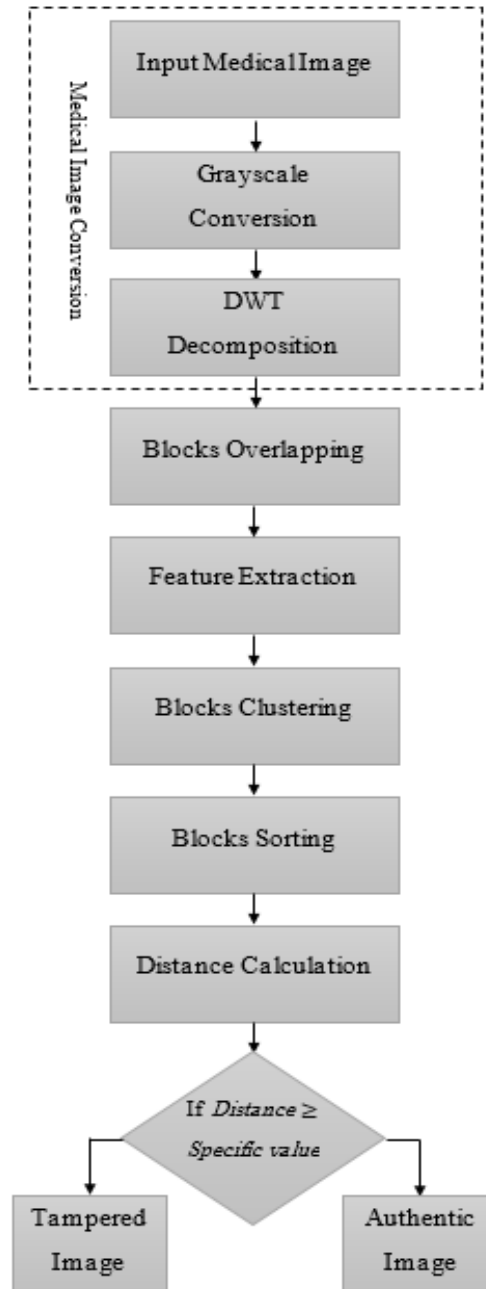


Figure 3 The construction of presented tampering detection processes

The steps of the proposed tampering detection technique are as follows;

Step 1: The conversion process: If the input medical image is RGB color image, it will be converted to grayscale image, else, when the input medical image is grayscale, it will be used directly.

Step 2: Applying One-level of DWT: Decompose the grayscale medical image, into four sub-bands LL, HL, LH, and HH.

Step 3: Overlapping blocks: The LL sub-band with the size of $(M \times N)$ can be separated into overlapping blocks of $(t \times t)$ pixels, where t is an even number, to result in T of blocks, as explained in the next equation:

$$T = (M - t + 1) \times (N - t + 1) \quad (1)$$

Step 4: Features extraction process: Each block is separated into four frames as illustrated in figure (4), supposing t is equal to eight. For all blocks, the features are extracted by computing the averages of these frames. Feature vector includes $(\text{Number} = t/2)$ coefficients, in addition to two indices to the block location, as explained in the next equation:

$$FV_i = \text{Average}(F_i), 1 \leq i \leq \text{Number} \quad (2)$$

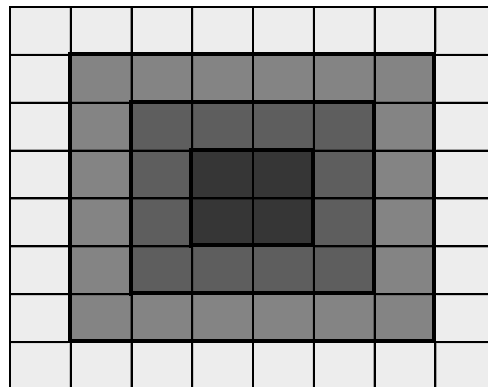


Figure 4 The division of block

If the block is rotated via the fundamental angles (90, 180 and 270), then the block values are unchanged along the block frame. Lastly, the whole blocks are stored in an array with size " $T \times (\text{Number} + 2)$ ".

Step 5: The blocks clustering process: K-Means algorithm is utilized for the purpose of clustering. This algorithm represents a fast clustering which works on grouping similar objects depending on features into the "K" number of groups, where "K" refers to an integer "positive" number. The process of grouping is accomplished via reducing the sum of squares of distances between data and the corresponding cluster centroid. The values of features in every vector are stored in a matrix to implement the K-Means algorithm.

Step 6: The blocks sorting process: The algorithm of radix sorting (based on the most significant digit) has been utilized for ascendingly sorting the vectors of clustered blocks.

In order to obtain new vectors, similar values are lexicographically sorted (from left to right) to permit a comparison between every neighbour vectors.

Step 7: The distance calculation process: The equation of Correlation (Co) is used between every two similar blocks, as follows:

$$Co = \frac{\sum_{i=1}^j (k_i - k') \cdot (l_i - l')}{\sqrt{\sum_{i=1}^j (k_i - k')^2 \cdot \sum_{i=1}^j (l_i - l')^2}} \quad (3)$$

Where k , and l represents the LL sub-band block coefficients, and k' , l' represents mean values, j denotes the no. of coefficients in a block. If Co is greater than the Threshold, then, two blocks are supposed to be similar, after that, the distance between these similar blocks should be found to eliminate the false positives, else, this block is exceeded The distance were calculatated using the next equation:

$$Distance = \sqrt{(D_b^k - D_{b+1}^k) + (D_b^l - D_{b+1}^l)} \quad (4)$$


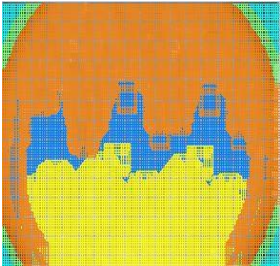
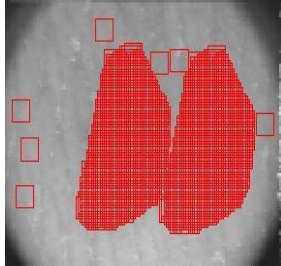

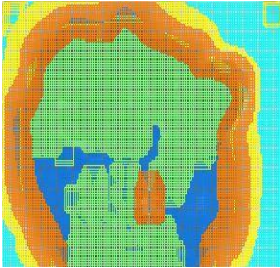
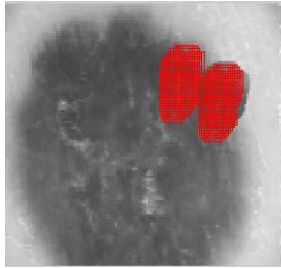
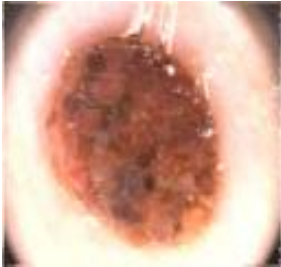
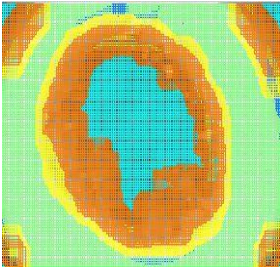
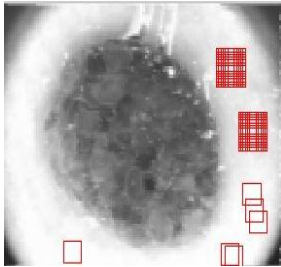

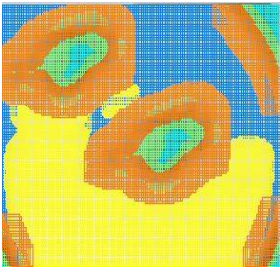
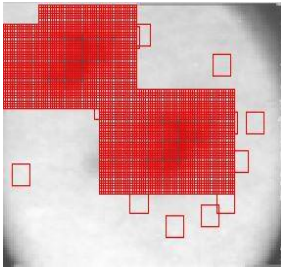
Where (D_b^k, D_b^l) is the " b " block location, and (D_{b+1}^k, D_{b+1}^l) is the " $b+1$ " block location.

The distance between similar blocks are compared; If $Distance \geq Specific\ value$, (The *Specific value* is equal to *Sixteen* found by experiments), then a decision is taken about the existence of tampering.

The Experimental Results

The dataset which has been used in this proposed tampering detection technique has some specifications like "512×512" dimension, "BMP" file type, "24" bit depth, and "120" number of samples for skin cancer medical images. This dataset is tempered by using the Microsoft Paint program to forge the skin cancer images. The implementation of the proposed technique is done using Matlab 2017 programming language. The experiments were performed on an Intel Core i7, 64-bit OS, 6 GB RAM, and 2.50 GHz processor. Some samples of tampered skin cancer images are tested and evaluated as illustrated in table (1). Figure (5) shows the time required to detect the tampering when Feature=4, and K=5, 10, and 20.

Table 1 Medical images tampering detection using some samples of skin cancer images

Image No.	Samples of tampered medical images	Clustering process	Localization process of duplicated regions
1 st Image			
2 nd Image			
3 rd Image			
4 th Image			

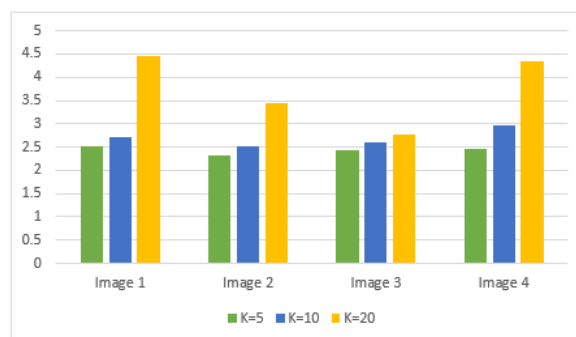


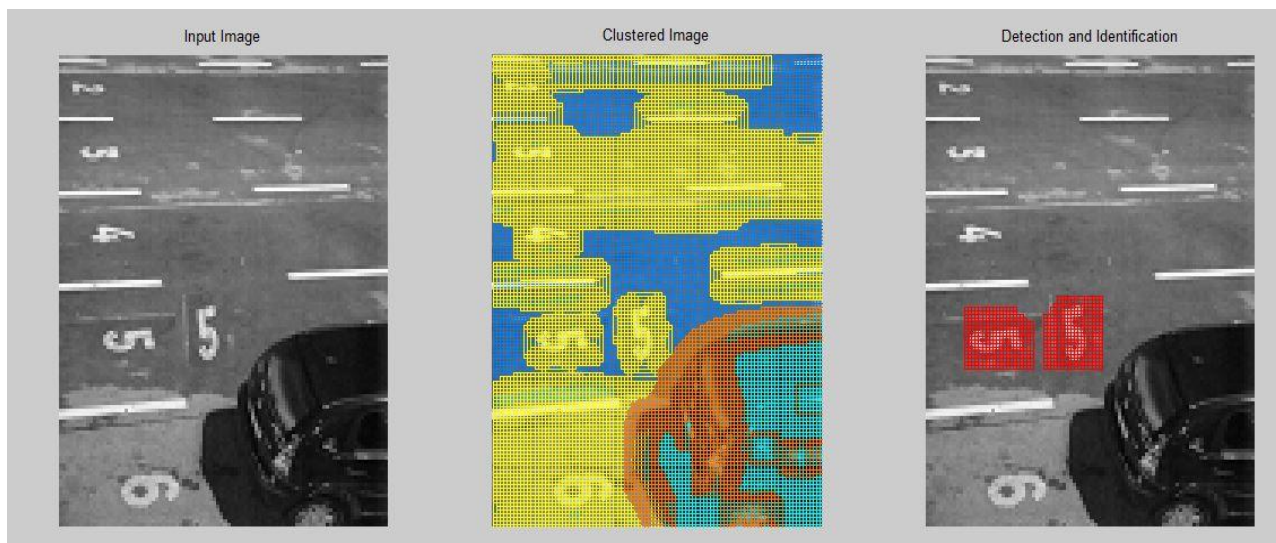
Figure 5 The time required (in seconds) for the detection technique of medical skin cancer images samples tampering, when Feature=4, and K=5, 10, and 20.

Table (2) shows the True Positive (TP) and False Positive (FP) for detecting the Copy-Move in the first medical image with several Thresholds (0.1, 0.2, 0.3, 0.4, and 0.5). The detected medical images represent the capability of the proposed technique to be effective in detecting multi-duplicated regions over various distortions, especially, rotation. From the results, we found that the obtained accuracy is high and the time to find tampering is low.

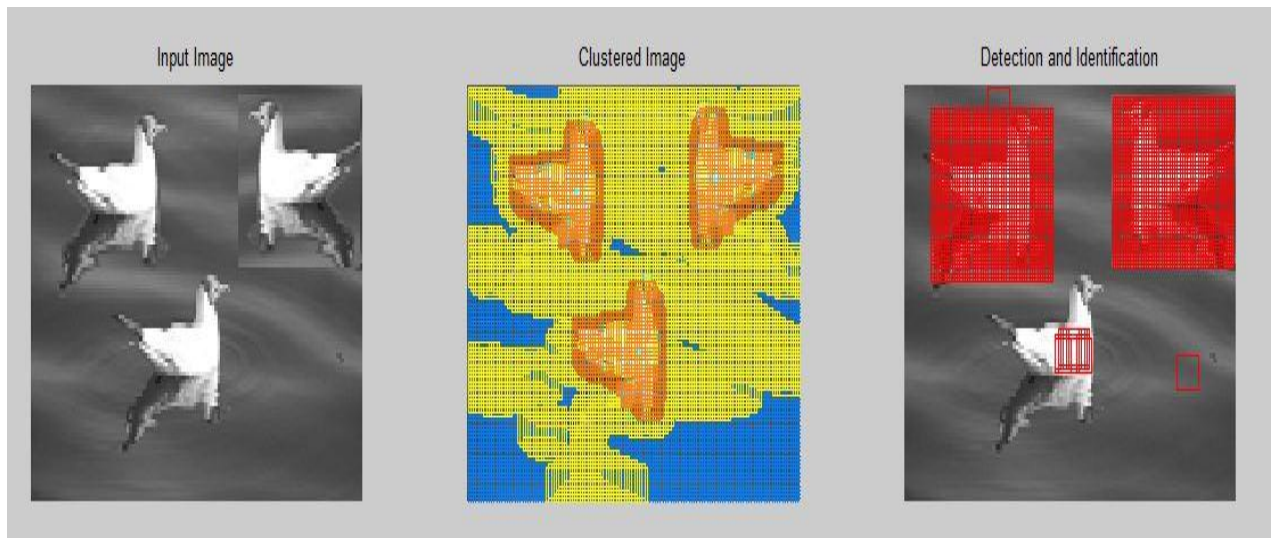
Table 2 True positive and false positive for the 1st medical image

Threshold	Number of Blocks		
	Detection	TP	FP
0.1	1802	1802(100%)	0 (0%)
0.2	1083	1802(99.9%)	1(0.1%)
0.3	1827	1802(98.63%)	25(1.37%)
0.4	1832	1802(97.99%)	37(2.01%)
0.5	1852	1802(97.3%)	50(2.7%)

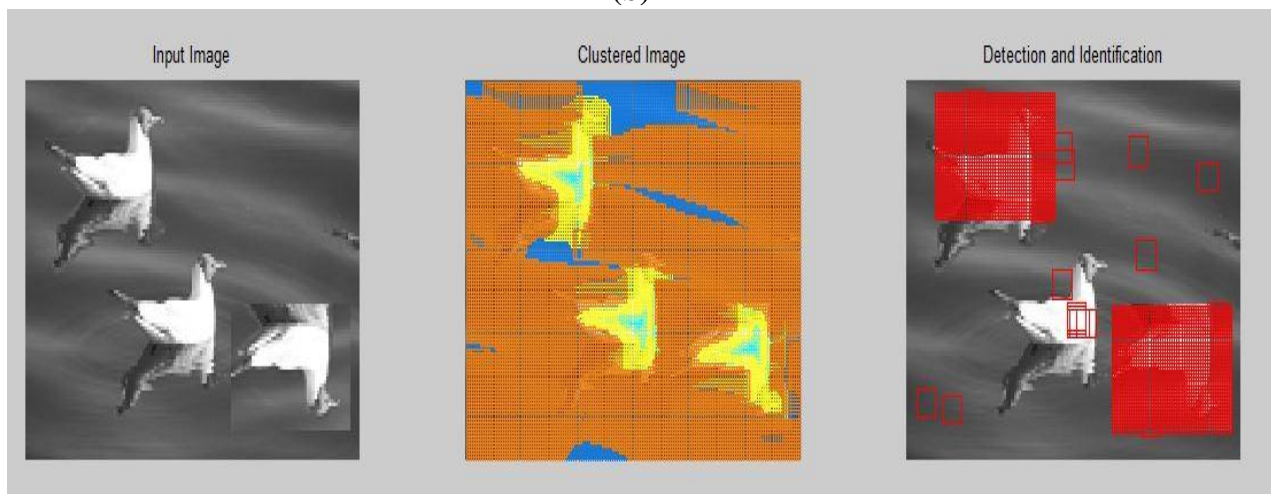
This proposed technique can be also implemented in the ordinary images for detecting tampering with different types of rotations 90°, 180°, and 270° degrees (clockwise and anti-clockwise), flip /reflection vertical and horizontal, as shown in Figure 6; (a) segment rotates by 90 degree left, (b) horizontal rotation, (c) vertical rotation and (d) segment rotates by 90 ° degree left, additionally, it could detect the tampering after different scaling conditions; (e) scaling segment size +10%, (f) multiple copy move forgery detection with scaling.



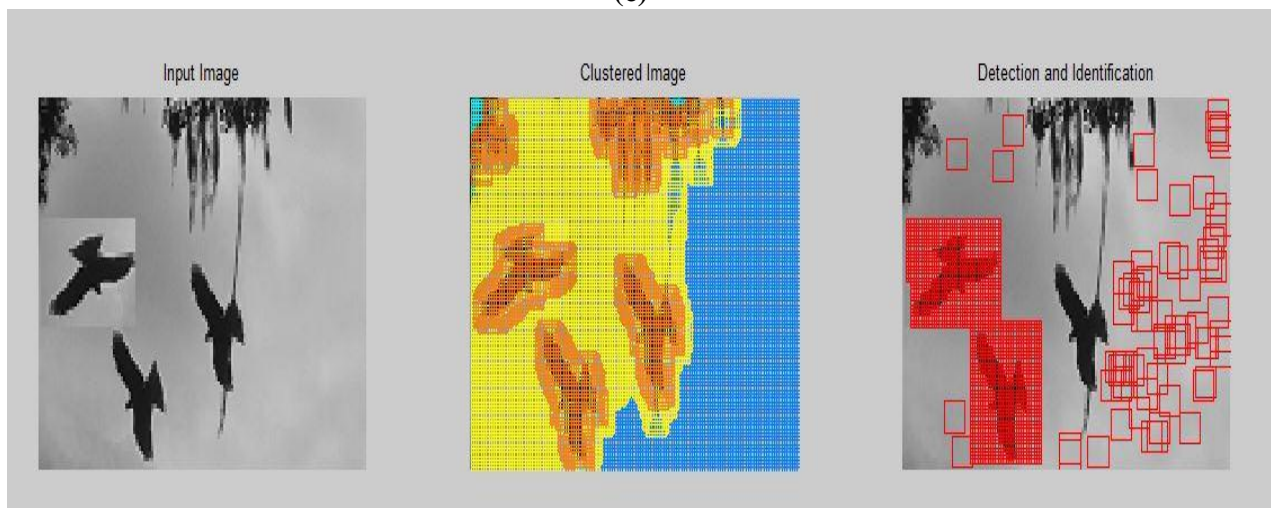
(a)



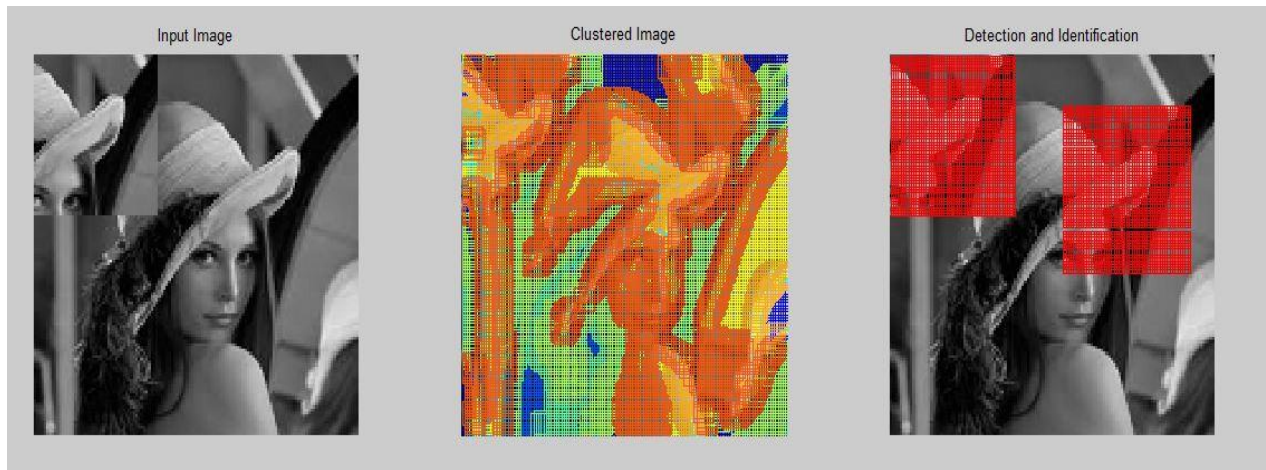
(b)



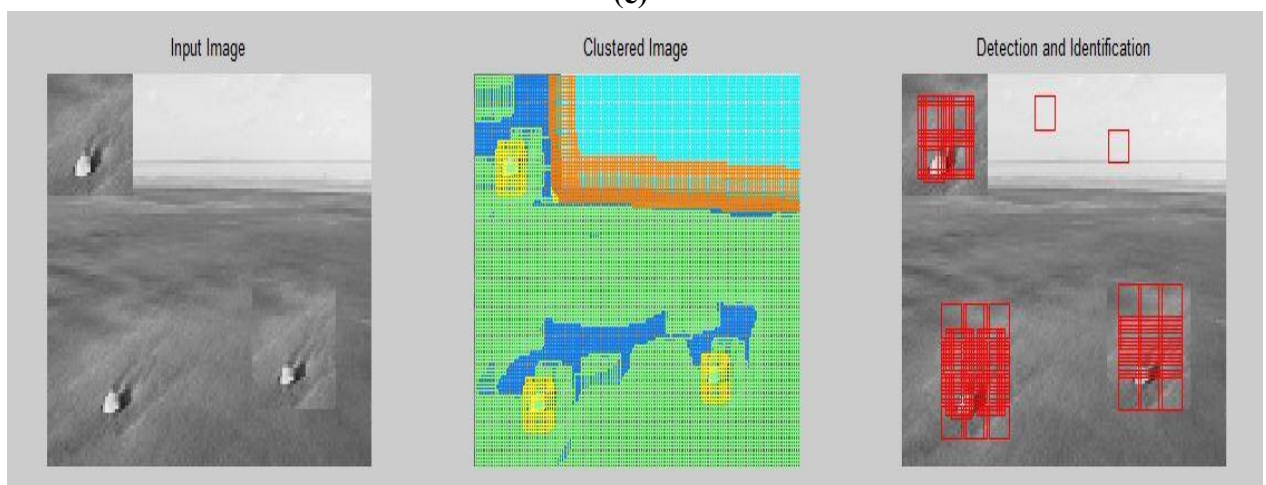
(c)



(d)



(e)



(f)

Figure 6 Tampering detection after different conditions

Conclusion

Medical images are extremely sensitive and giving the state of the interior organs that cannot be viewed by eyes, therefore, they are distinct from other kinds of images. Consequently, the medical images tampering should be detected for providing authenticity and integrity. This paper proposed a blind forensic technique to detect medical images tampering. It is aimed to achieve higher performance by supporting copy and move forgery detection (even if the copied regions were rotated) in the DWT domain using the strategy of blocks matching. Additionally, this proposed technique can detect the tampering under the attacks of rotation, JPEG compression, blurring, and noise addition. In the experimental results, the obtained accuracy is high and the time to find tampering is low.

References

- Gadhiya, T.D., Roy, A.K., Mitra, S.K., & Mall, V. (2017). Use of discrete wavelet transform method for detection and localization of tampering in a digital medical image. *IEEE Region 10 Symposium (TENSYP), Cochin*, 1-5.
- Vaishnavi, D., & Subashini, T.S. (2019). Application of local invariant symmetry features to detect and localize image copy move forgeries. *Journal of Information Security and Applications*, 44, 23-31.
- Mahmood, T., Nawaz, T., Mehmood, Z., Khan, Z., Shah, M., & Ashraf, R. (2016). Forensic analysis of copy-move forgery in digital images using the stationary wavelets. *Sixth International Conference on Innovative Computing Technology (INTECH), Dublin*, 578-583.
- Aydin, Y., Muzaffer, G., & Ulutaş, G. (2018). Detection of copy move forgery technique based on SIFT and SURF. *26th Signal Processing and Communications Applications Conference (SIU), Izmir*, 1-4.
- Aya, H., Ahmed, T., & Mazen, M.S. An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal. *Journal of King Saud University - Computer and Information Sciences* 2019.
<https://doi.org/10.1016/j.jksuci.2019.07.007>
- Jun-Liu, Z., & Chi-Man, P. (2020). Two-pass hashing feature representation and searching method for copy-move forgery detection. *Information Sciences*, 512, 675-692.
- Huang, H., Coatrieux, G., Shu, H.Z., Luo, L.M., & Roux, C. (2011). Medical image integrity control and forensics based on watermarking Approximating local modifications and identifying global image alterations. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Boston, MA*, 8062-8065.
- Arsalan, M., Saeed Qureshi, A., Khan, A., & Rajarajan, M. (2017). Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. *Applied Soft Computing*, 51, 168-179.
- Huang, H., Coatrieux, G., Shu, H.Z., Luo, L.M., & Roux, C. (2011). Blind forensics in medical imaging based on Tchebichef image moments. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Boston, MA*, 4473-4476.
- Govarthini, S., & Vadivel, M. (2014). Integrity vérification of medical images using blind forensic method. *International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai*, 1-6.