Available online at www.sciencedirect.com

ScienceDirect

AASRI Procedia 9 (2014) 84 – 91

AASRI Procedia

www.elsevier.com/locate/procedia

2014 AASRI Conference on Circuit and Signal Processing (CSP 2014)

Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform

Mohammad Farukh Hashmi[a] *, Vijay Anand[b] , Avinas G. Keskar[c]

[a,b,c]*Department of Electronics Engineering, Visvesvaraya National Institute of Technology, Nagpur,440010, India.*

Abstract

In the present digital world, digital images and videos are the main carrier of information. However, these sources of information can be easily tampered by using readily available software thus making authenticity and integrity of the digital images an important issue of concern. And in most of the cases copy- move image forgery is used to tamper the digital images. Therefore, as a solution to the aforementioned problem we are going to propose a unique method for copy-move forgery detection which can sustained various pre-processing attacks using a combination of Dyadic Wavelet Transform (DyWT) and Scale Invariant Feature Transform (SIFT). In this process first DyWT is applied on a given image to decompose it into four parts LL, LH, HL, and HH. Since LL part contains most of the information, we intended to apply SIFT on LL part only to extract the key features and find a descriptor vector of these key features and then find similarities between various descriptors vector to conclude that there has been some copy-move tampering done to the given image. And by using DyWT with SIFT we are able to extract more numbers of key points that are matched and thus able to detect copy-move forgery more efficiently.

Peer-review under responsibility of Scientific Committee of American Applied Science Research Institute

Keywords: Digital Image Forgery; DyWT (Dyadic Wavelet Transform); SIFT (Scale Invariant Feature Transfrom).

* Corresponding author: Mohammad Farukh Hashmi. Tel.: +91-712-280-1355.
E-mail address: farooq78699@gmail.com, vijjanand117@gmail.com,agkeskar@ece.vnit.ac.in.

Peer-review under responsibility of Scientific Committee of American Applied Science Research Institute
doi:10.1016/j.aasri.2014.09.015

1. Introduction

In this digital savvy world "seeing is no more believing". Most of the information is carried in a digital form especially in the form of either digital images or digital videos. Thus, they form the main stream of the information carrier. These sources can be manipulated very easily. In this paper, we will focus on image forgery, which has become a topic of serious concern. The image editing software such as Adobe Photoshop is readily available using which any given image can be easily doctored, which can lead to serious consequences, as these tampered images can be presented as a part of evidence in the court room leading to a wrong decision and creating the false belief in many real-world applications. Therefore the issue of authentication of the images has to be taken very seriously. Most of the forgery detection techniques are categorized into two major domains: intrusive/non-blind and non-intrusive/blind [1] as shown in the Fig.1

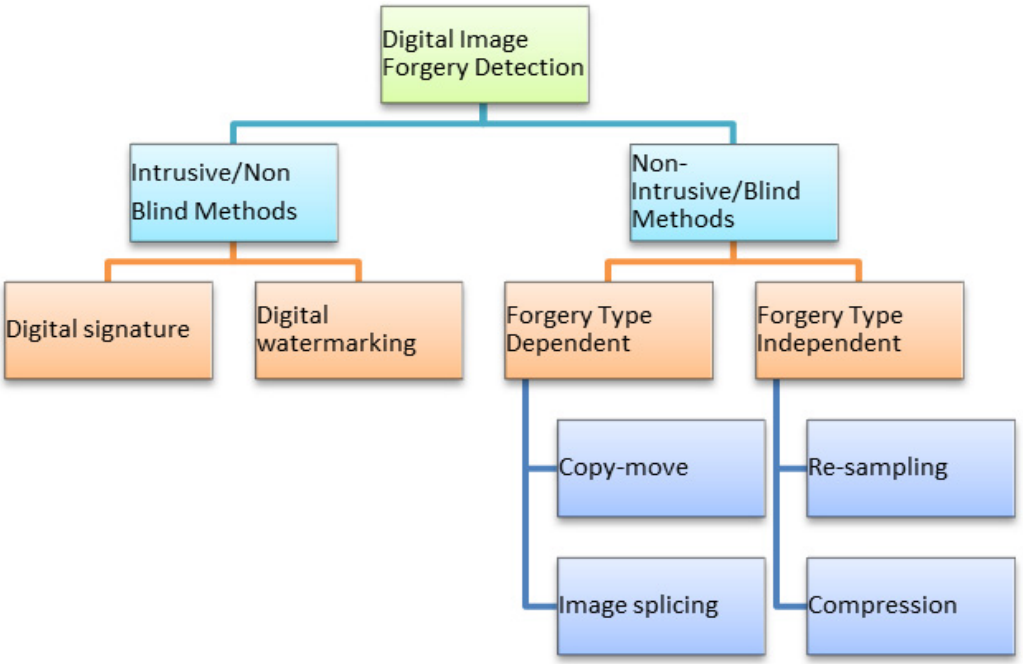


Fig.1. Classification of image forgery detection technique

Intrusive method which is also known as a non-blind method requires some digital information to be embedded in the original image when it is generated, and thus it has a limited scope. Some of the examples of these methods are watermarking and using digital signature of the camera and not all the digital devices can provide this feature. On the other hand, non-intrusive method which is also known as a blind method does not require any embedded information. A digital image is said to be forged when its original version is tampered by applying various transformations like that of rotation, scaling, resizing, etc. It may also happen that an image is tampered by adding noise or by removing or adding some objects to hide the real information [1]. Most commonly used image tampering method is copy-move image forgery in this a part of the original image is first copied and then pasted on other parts once or may be multiple times to hide some information.

Since it is very easy and effective to implement that makes it most common type of image forgery [2]. A copy-move forgery example is presented in Fig.2.

Fig.2. An example of Copy-Move Forgery

The remaining contents of the paper are presented in following manner. Next section deals with all previous work related to image forgery detection. Section 3 completely explains the proposed method, section 4 deals with simulation results and evaluation of performance parameter and in the end, we have conclusion and references.

2. Related Work

In this section, we have reviewed most of the blind methods of copy-move image forgery detection. Muhammad et al. [3] presented a blind and robust technique using dyadic (undecimated) wavelet transform (DyWT) which has better results than Discrete Wavelet Transform (DWT). Li et al. [4] discussed methods which reduce the overall computation load. It first applied DWT to decompose the given image into four different sub-bands LL, LH, HL, and HH. Since most of the information is present in the low frequency band thus low-frequency sub-band, i.e. LL band is divided into overlapping blocks. By doing this number of blocks have been reduced and the overall process has speed up. On these blocks, they applied SVD (singular value decomposition). H. Huang et al. [5] used SIFT algorithm to represent the features of the given image. SIFT algorithm is invariant to changes in illumination, rotation, scaling, etc. Amerini et al. [6], deals with detecting whether an image has been forged or not specially using copy-move forgery by using Scale Invariant Features Transform (SIFT). SIFT allow to understand that copy-move forgery has occurred, and it also recovers from geometric transformation used for cloning. Using this method we can also deal with multiple copy-move forgery. Hashmi et al. [10] provided an algorithm by combining DWT and SIFT to detect copy-move image forgery. Al-Qershi et al. [11] provided a state-of-art of passive detection of copy-move forgery in digital images. The key current's issues are discussed for developing robust passive copy-move forgery detection. Leida Li et al. [12] proposed an efficient method using local binary patterns, in this image is first image is filtered and then divided into overlapping circular blocks; features of these blocks are calculated using local binary patterns to detect the forged regions. Birajdar et al [13] summarized a complete survey on digital image forgery detection using passive techniques, which discussed currently available forgery detection techniques

and also provide further recommendation for future research. Mahalakshmi et al [14] provided detection of digital image forgery by exploring basic image manipulations done on the images. Here they have presented techniques to detect image is manipulated using basic method like copy-move, region duplication, splicing etc. Anand et al. [16] proposed an algorithm to detect the digital image copy move forgery to overcome the sustained attacks using SIFT and DyWT methods.

3. Proposed Methodology

Through this paper, we are going to propose a new technique for copy-move forgery detection. First image is transformed into wavelet domain and SIFT is applied on the transformed image to obtain the features. As wavelet produces multispectral components, features are more predominant [7]. Thus after obtaining interest point feature descriptor we go for finding matching between these feature descriptors to conclude whether tampering is done to the given image or not. Our works confirm that SIFT features are an optimal solution because of their high computational efficiency and robust performance.

3.1. Dyadic Wavelet Transform (DyWT)

In related work, we have seen that many previous techniques use DWT for copy-move forgery detection. DWT has its own drawback like it is shift invariant and thus less optimal for data analysis. Mallat and Zhong [8] introduced the DyWT to overcome the drawback of DWT. DyWT is shift invariant and is different from DWT because in DyWT there is no down-sampling like that of DWT. The DyWT of an image is computed using the algorithm [1].

3.2. Scale Invariant Feature Transform (SIFT)

A four stage filtering approach is used in the SIFT algorithm [9]:

a) Detection of Scale space Extrema which are the interest key points
b) Localization of key-points by taking into account only the stable key points
c) Orientation Assignment to the selected key points
d) Key-point Descriptor

After getting key point matching it may happen that to region of an image may have the same features legitimately. So we next go for clustering of key point and forgery detection and in final step estimates geometric transformation if tampering has been done to the given image.

3.3. Algorithm combining DyWT and SIFT

In order to determine copy-move forgery; first of all we apply dyadic wavelet transform on the given image which will decompose the given image in four parts LL, LH, HL, and HH. Since most of the information is contained in LL part thus we apply SIFT feature extraction on LL part as a result we have the feature descriptor vectors of the interest points, and finally, we go for finding the match between these feature descriptor vectors to mark the forged regions. The proposed algorithm block diagram is shown in Fig. 3.

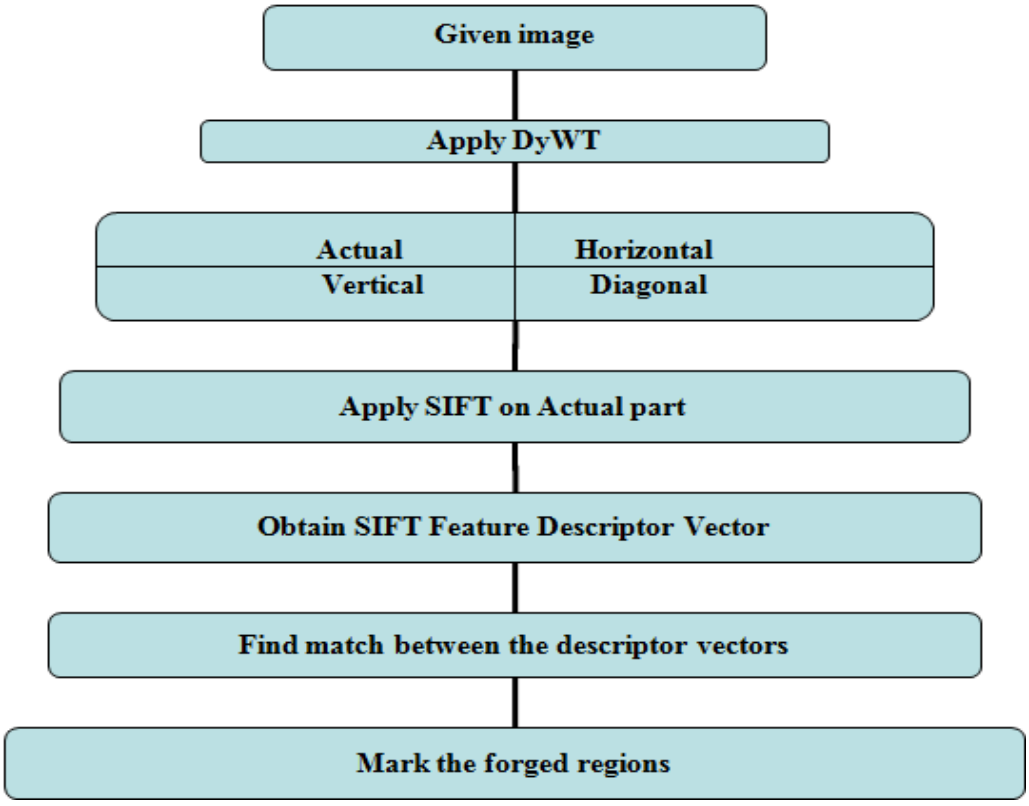
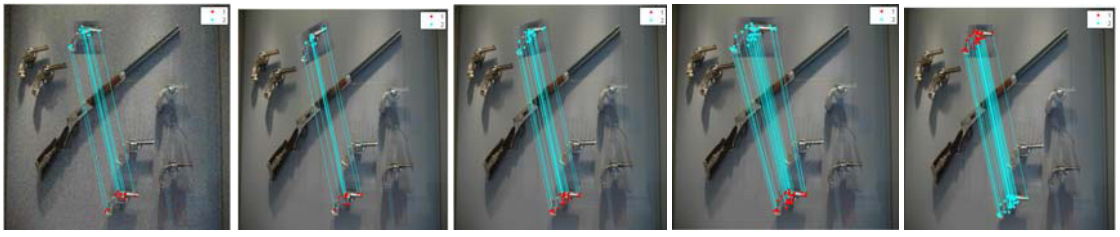


Fig.3. Block diagram of proposed algorithm

3.4. Testing robustness against various attacks

In order to test the robustness of our proposed method, we applied our method on a standard database MICC-F220 which contains non-tampered images as well as tampered one having scaled version and some have rotation and some have a combination of two or more attacks. Figures in Fig. 4 describe the forgery detection results under various attacks



(a) (b) (c) (d) (e)

Fig.4(a). Normal Copy-move forgery, 4(b). Scale version attack, 4(c). Rotation, 4(d). Rotation and scaling, 4(e). Noise addition

4. Simulation Results

In result analysis, we applied the proposed algorithm over a standard dataset MICC-F220 [6]. This simulation has been performed on MATLAB 2012a software with 32GB Ram and core i7 processor. DyWT of the test image is first calculated and on the low-frequency component of DyWT we apply SIFT to extract the features which are nothing but descriptor vectors of the object of interest in the test image and the final step is to go matching these features to detect copy- move forgery.

Images shown in Fig. 5 describe various processes involved in proposed method, Fig. 5(a) is the tampered test image on which our algorithm is applied, and finally, we got 2395 key-points and 66 matches, thus concluding that the given test image is forged.

(a) (b) (c) (d)

Fig.5(a). Tampered test image, 5(b). DyWT of test image, 5(c). LL or approximation part of DyWT, 5(d). Matching of similar feature using DyWT and SIFT.

We are focusing on two major performance parameters at the image level to determine the fact that an image has been tampered or not. Considering the image level some of the important measures are described in Table 1.

Table 1. Evaluation Measures Description

Evaluation Measures	Description
True Positive (T_P)	Number of images that have been correctly detected as forged
False Positive (F_P)	Number of images that have been falsely detected as forged
False Negative (F_N)	Number of images that have been falsely missed but they are forged.
False Positive (F_p)	Number of images that have been falsely missed but they are forged.

From the above mentioned measures we calculated Precision, p, and Recall, r which are defined as:

$$p = \frac{T_P}{T_P + F_P} \quad r = \frac{T_P}{T_P + F_N} \tag{1}$$

Precision represents the probability of truly detecting a forgery and Recall represents probability that a forged image has been detected; it may be either true or falsely forged. Recall is also called as True Positive

Rate (TPR) [15]. Thus after performing experiment on database of MICC F220, we tabulated the result obtained in Table 2.

Table 2. Performance Measure

Parameters	T_p	T_N	F_P	F_N	Precision (p)	Recall (r)	False Positive Rate (FPR)
SIFT	82	106	4	28	95%	74%	4%
DyWT +SIFT	88	99	11	22	88%	80%	10%

Precision, Recall rate and False Positive Rate of proposed algorithm is presented in Fig. 6

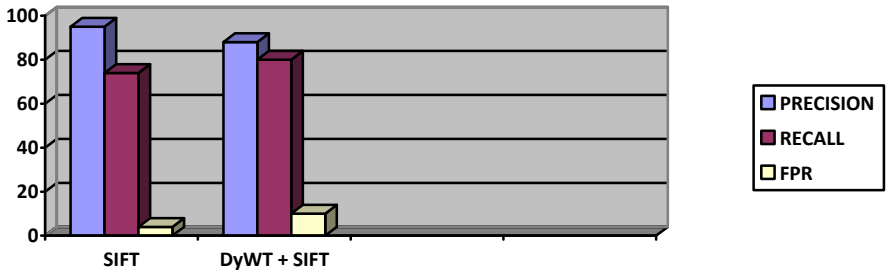


Fig.6. Performance parameters of proposed method

5. Conclusion

We thoroughly assessed different types of forgery techniques and decided to develop an algorithm which encompasses better performance and robustness for detecting the most common copy-move forgery. We proposed a method which combines DyWT with SIFT. Our efficiency of detection ranked much higher than the previously available methods. DyWT does not incorporate down sampling so the image size is intact and low frequency component contains most of the information on which SIFT is applied to extract the features and then matching is obtained between the feature descriptors to conclude that a given image is forged or not. Our algorithm has higher matching rate, and it is robust to most of the attack and pre-processing techniques and also we have better performance parameter's values on which we can conclude that it's a feasible one.

Acknowledgements

We would like to thank our guide and Coordinator of Centre of Excellence Dr. Avinash G. Keskar for his constant encouragement and guidance toward this project. This project is funded from Centre of Excellence (CoE), Department of Electronics Engineering, VNIT Nagpur. Special thanks to Director VNIT Nagpur for providing institutional facilities and needed administrative and authoritative support during the work at VNIT.

References

[1] Muhammad, Najah, Muhammad Hussain, Ghulam Muhammad, and George Bebis, "Copy-move forgery detection using dyadic wavelet transform.", In Proceedings of IEEE Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV-2011), pp. 103-108, 2011.
[2] Jing, Li, and Chao Shao. "Image Copy-Move Forgery Detecting Based on Local Invariant Feature." Journal of Multimedia, vol. 7, no. 1, pp.90-97, 2012.
[3] Muhammad, Ghulam, Muhammad Hussain, Khalid Khawaji, and George Bebis, "Blind copy move image forgery detection using dyadic undecimated wavelet transform" ,In Proceedings of IEEE 17th International Conference on Digital Signal Processing (DSP-2011), pp. 1-6, 2011.
[4] Li, Guohui, Qiong Wu, Dan Tu, and Shaojie Sun. "A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD", In Proceedings of IEEE International Conference on Multimedia and Expo., pp. 1750-1753,2007.
[5] Huang, Hailing, Weiqiang Guo, and Yu Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm", In Proceedings of Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA-2008), vol. 2, pp. 272-276, 2008.
[6] Amerini, Irene, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. "A sift-based forensic method for copy–move attack detection and transformation recovery", IEEE Transactions on Information Forensics and Security, vol. 6, no. 3 ,pp. 1099-1110, 2011.
[7] Amerini, Irene, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Luca Del Tongo, and Giuseppe Serra. "Copy-move forgery detection and localization by means of robust clustering with J-linkage." Signal Processing: Image Communication, vol. 28, no. 6, pp.659–669, April 2013.
[8] Mallat, Stephane, and Sifen Zhong, "Characterization of signals from multiscale edges", IEEE Transactions on pattern analysis and machine intelligence, vol.14, no. 7, pp.710-732, 1992.
[9] Lowe, David G., "Distinctive image features from scale-invariant key points", International journal of computer vision, vol. 60, no. 2, pp. 91-110, 2004.
[10] Hashmi, Mohammad Farukh, Aaditya R. Hambarde, and Avinash G. Keskar. “Copy Move Forgery Detection using DWT and SIFT Features.” In Proceedings of 13th IEEE International Conference on Intelligent Systems Design and Applications (ISDA-2013), pp.188-193, December 2013.
[11] Al-Qershi, Osamah M., and Bee Ee Khoo. "Passive detection of copy-move forgery in digital images: State-of-the-art." Forensic Science International, vol. 231, no. 1, pp. 284-295, 2013.
[12] Li, Leida, Shushang Li, Hancheng Zhu, Shu-Chuan Chu, John F. Roddick, and Jeng-Shyang Pan. “An Efficient Scheme for Detecting Copy-move Forged Images by Local Binary Patterns”, Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, pp. 46-56, January 2013.
[13] Birajdar, Gajanan K., and Vijay H. Mankar. "Digital image forgery detection using passive techniques: A survey." Digital Investigation, vol.10, no. 3, pp. 226–245, 2013.
[14] Devi Mahalakshmi, S., K. Vijayalakshmi, and S. Priyadharsini. “Digital image forgery detection and estimation by exploring basic image manipulations” Digital Investigation, vol. 8, no. 3, pp. 215–225, 2012.
[15] Christlein, Vincent, Christian Riess, Johannes Jordan, and E. Angelopoulou. "An Evaluation of Popular Copy-Move Forgery Detection Approaches.", IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp.1841-1854, December 2012.
[16] Anand, Vijay, Mohammad Farukh Hashmi, and Avinash G. Keskar. "A Copy Move Forgery Detection to Overcome Sustained Attacks Using Dyadic Wavelet Transform and SIFT Methods." In Proceedings of the 6th Asian Conference on Intelligent Information and Database Systems (ACIIDS 2014), Springer International Publishing, pp. 530-542, April 2014.