ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Copy-Move Detection of Image Forgery by Using DWT and SIFT Methodologies: A Review

Suvarna G. Upase[1], S. V. Kuntawar[2]

P.G. Student, Department of ECE, Ballarpur Institute of Technology, Ballarpur, India[1]

Professor, Department of ECE, Ballarpur Institute of Technology, Ballarpur, India[2]

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. And in most of the cases copy- move image forgery is used to tamper the digital images. As a solution to 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 Discrete Wavelet Transform (DWT) and Scale Invariant Feature Transform (SIFT). In this process first DWT is applied on a given image to decompose it into four parts. Since LL part contains most of the information, we 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.By using DWT 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.

KEYWORDS:DigitalImageForgery;DWT(DiscreteWaveletTransform);SIFT(ScaleInvariantFeatureTransfrom).

I. 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 Photo-shop 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

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, re-sizing, 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. 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,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

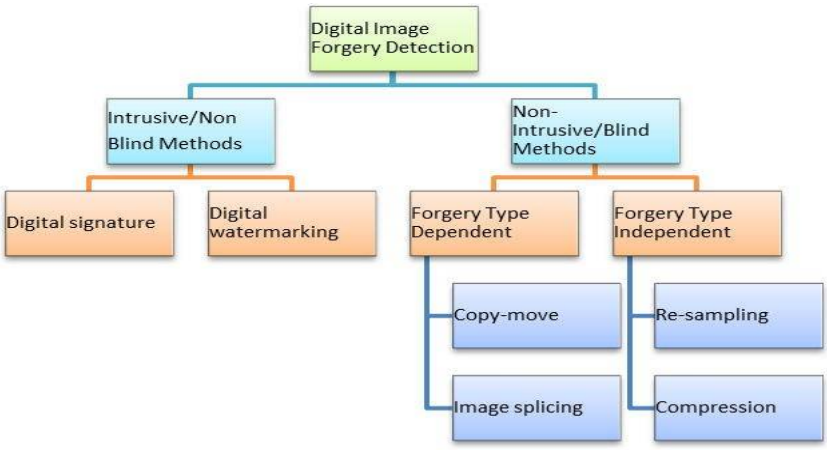

Fig.1. Classification of image forgery detection technique

section 4 deals with simulation results and evaluation of performance parameter and in the end, we have conclusion and references.

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 discrete wavelet transform (DWT). Li et al. [4] discussed methods which reduce the overall computation load. It first applied DCT 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.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 DWT methods.

II. 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 multi spectral 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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

A. Discrete Wavelet Transform (DWT)

Wavelet transform decomposes a signal into a set of basis functions. These basis functions are called wavelets. Wavelets are obtained from a single prototype wavelet y(t) called mother wavelet by dilation and shifting. In related work, we have seen that many previous techniques use DWT for copy-move forgery detection. The DWT of an image is computed using the algorithm [1].

B. Scale Invariant Feature Transform (SIFT)

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

1. Detection of Scale space Extrema which are the interest key points
2. Localization of key-points by taking into account only the stable key points
3. Orientation Assignment to the selected key points
4. 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.

C. Algorithm Combining DWT 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.

There are several methods used for Cop-move forgery detection technique, which is being listed as follows in Table no 01.

Table No. 01: Types of methods for forgery defections

Methods	**Methods Description**
PCA (Principal Component Analysis)	Mathematical procedure that uses orthogonal transformation Converts correlated variables to linearly uncorrelated variables
DCT (Discrete Cosine Transform)	Transforms image from spatial to “frequency domain” Discard high frequency “sharp variations” components
SIFT (Scale Invariant Feature Transform)	Scale space extreme detection Key point localization Orientation assignment Key point description
DWT (Discrete Wavelet Transform)	It decomposes a signal into a set of basis functions, called wavelets. DWT splits the signal into high and low frequency parts Low frequency part contains coarse information of signal while high frequency part contains information about the edge components.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

III. CONCLUSION

In this paper a special type of forgery detection is reviewed, which can detect the duplicated regions accurately and quickly. The efficiency of forgery detection can be improve by applying DWT (Discrete Wavelet Transform) & SIFT (Scale invariant Feature Transform).

REFERENCES

[1] 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.

[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] 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.

[4] 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.

[5] 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.

[6] 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.

[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] 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.