Copy-Move Detection of Image Forgery by using DWT and SIFT Methodologies

Suvarna G. Upase
M.Tech (ECE)
BIT, Gondwana University
Ballarpur, India

Sunil V. Kuntawar
Professor (ECE)
BIT, Gondwana University
Ballarpur, India

ABSTRACT

Copy move forgery is emerging as one of the research topic among researchers in the area of image forensic. Copy move forgery is basically concerned with duplicating one region in an image by pasting certain portion of the same image on it, many techniques have been used to detect such type of forgery. In this paper an enhanced way to detect copy move forgery is proposed. The proposed method use both block based method like Discrete Wavelet Transform (DWT) and feature based method like Scale Invariant Feature Transform (SIFT) to increase the robustness and accuracy of copy-move forgery detection. First of all DWT is applied on a given image to decompose the image into four parts LL, HL, HH and LH, Since LL part contains most of the information, so SIFT is applied to LL part only to further extract the key features of the image and match those features by using inter block matching and find the similar portion or parts between the images and marked them as forged. This method detect whether image forgery is occurred or not and also highlight the forgery more accurately.

Keywords

Digital Image Forgery; DWT (Discrete Wavelet Transform); SIFT (Scale Invariant Feature Transform).

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.

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 [6]. It may also happen that an image is tampered by adding noise or by removing or adding some objects to hide the real information.

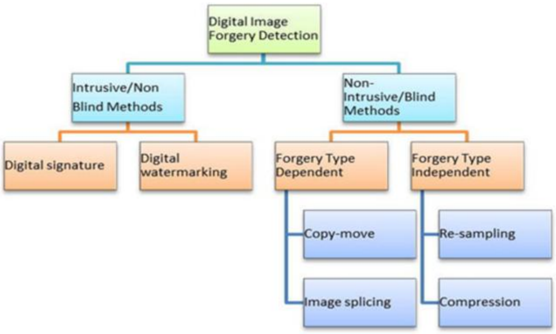
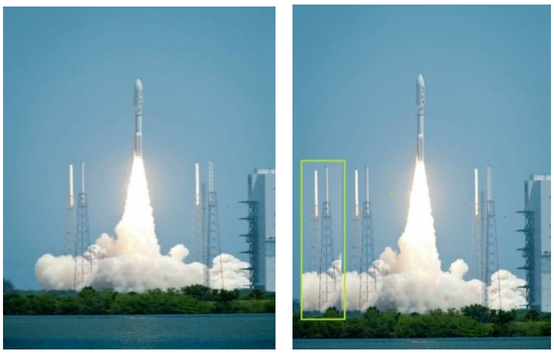


Fig.1. Classification of image forgery detection technique



a) Original image **b) Forged Image**

Fig 2: An example for copy move image forgery

2. RELATED WORK

Various blind methods of copy-move image forgery detection has been reviewed, Saika et al. [1] presented a blind and robust technique using discrete wavelet transform (DWT). Sunil Kumar al.[2] 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. [6] used SIFT algorithm to represent the features of the given image. SIFT algorithm is invariant to changes in illumination, rotation, scaling, etc. N.Anantharaj [7], 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. Amanpreet Kaur et al. [11] provided an algorithm by combining DCT and SIFT to detect copy-move image forgery. Salam A. Thajeel [12] provided a survey of copy move forgery detection techniques on digital images. Rohini.A.Maind [13] proposed an efficient method using local binary patterns, in this 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. Popescu et al [14] summarized a complete exposing digital forgeries by detecting duplicated image regions and also provide further recommendation for future research. Nandini Singhal et al [15] provided analysis of copy-move forgery image forensics. Vincent Christlein et al. [16] proposed an algorithm on an evaluation of copy-move forgery detection approaches.

3. METHODOLOGY

Concept behind this paper is to Detection of malicious manipulation with digital images. The input image is first decomposed using one of the DWT bases function from which SIFT features are extracted. Matching is done among the clusters and then the out liners are removed to give the final detection result.

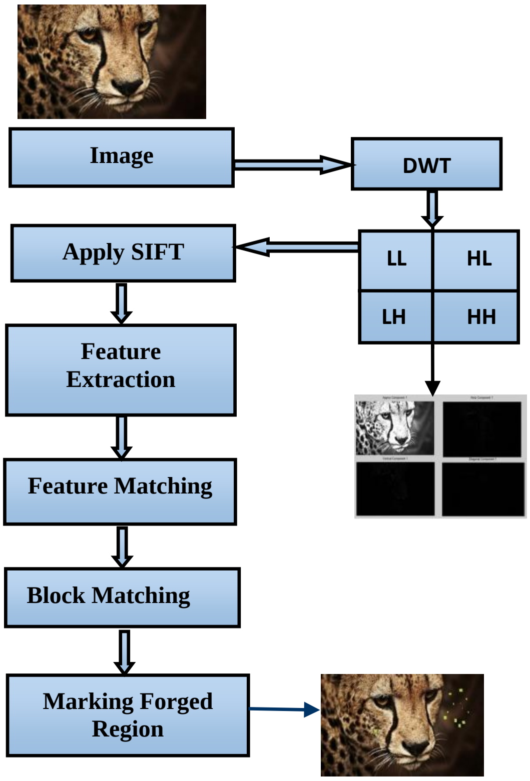


Fig 3: Proposed Algorithm Flowchart

3.1 Decomposing Using DWT

2D-DWT is applied in the initial stage of forgery detection process as it helps to extract more number of SIFT features which will help in better detection performance. DWT is applied on the image for copy-move forgery detection, the image is decomposed into four different sub-bands LL, LH, HL, and HH. Most of the data is concentrated in LL sub-band and it is considered as the approximation of the image. It represents the coarse level coefficients of the original image.

It is the LL sub-band which is decomposed into four sub-band at the next level. Size of the image is reduced at every level by the DWT transform. Fig. 4 shows the decomposing of Butterfly image after applying DWT on it, the image is divided in 4 parts in first level and in next level its LL sub-band is further decomposed.

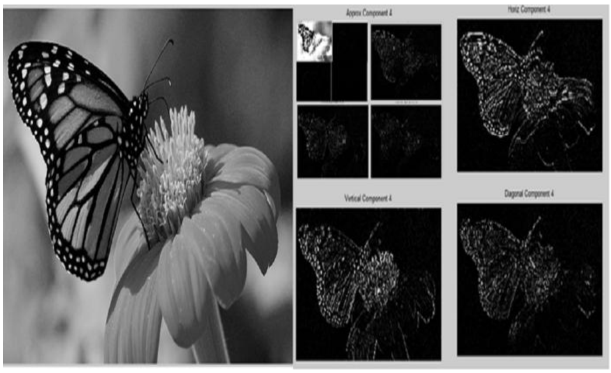


Fig 4: Illustration of 2-D Discrete Wavelet Transform

3.2 SIFT Feature Extraction

SIFT descriptors that are invariant to scaling, rotation and affine transformations are computed using the following three major steps.

3.2.1 *Scale Space Extrema Detection*

A function, L(x, y, σ) is defined as the scale-space of an image which is generated by the convolution of Gaussian function, G(x, y, σ), and an input image, I(x,y):

$$L(x,y,\sigma)=G(x,y,\sigma)*I(x,y)$$

$$G(x,y,\sigma)=\frac{1}{2\Pi\sigma^{2}}e-(x^{2}+y^{2})/2\sigma^{2} \qquad (1)$$

3.2.2 *Keypoint Localization*

Selection of keypoints from extrema is done by rejecting the points along image edges or those with low contrast as they are unstable over image variations. The Taylor expansion of scale- space function D (x,y, σ), shifted such that the sample point is origin:

$$D(x)=D+\frac{\partial D^{T}}{\partial x}x+\frac{1}{2}x^{T}\frac{\partial^{2}D}{\partial x^{2}}x \qquad (2)$$

3.2.3 *Keypoint Descriptor Generation*

The values of orientation histogram, in both image plane and scale space form the descriptor. With 4X4 array of histograms and 8 orientation bins in each, results in 4X4X8=128element feature vector.

3.3 Clustering

Extracted SIFT key point descriptors from the approximate sub image of the DWT decomposed original image are grouped using agglomerative hierarchical clustering. The clustering is completed by using one of the many linkage methods such as median, centroid or ward.

3.4 Key point matching

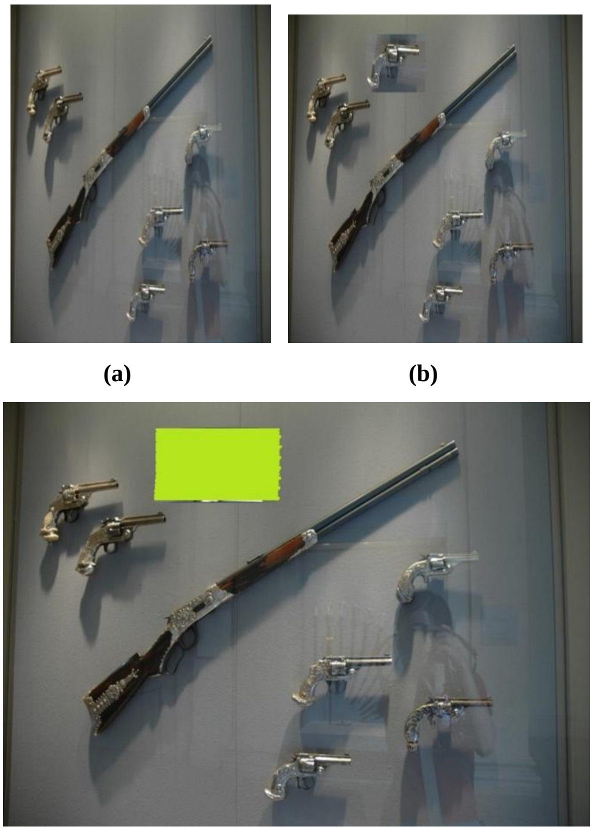
Key point matching is another important stage of the proposed method, which mainly concern with the matching of extracted feature keypoints from SIFT algorithm. In key point matching first reads the keypoint from given input image then, Compare the keypoints of images and if the keypoints matches then draw a line which indicating the matched keypoints, Then append the two images and draw a line which indicate the matches.

4. RESULTS

For performance evaluation of the copy move image forgery detection algorithm, simulation results are performed on a set of 50 images out of which 25 images are original i.e. unforged and 25 have been forged using copy move forgery. The image resolution lies in the range of 128 pixels to 640 pixels. The algorithm is coded in MATLAB R2013b on a machine equipped with Intel i3 2.5 GHz processor with 4GB DDR3RAM. The forged images contain either square or rectangular forged regions which have been copied and pasted. The following original images has been shortlisted from the MICC F220 datasets for running the program, shown in Fig. 5 & Fig. 6 below.

(a) **(b)**

Fig 5: Palace Image, (a) Original (b) No forgery is detected.



(a) **(b)**

(c)

Fig 6: Gun Image , a) Original Image b) Forged Image c) Forged area detected.

4.1 Performance of Proposed Method

Table 1. Execution time & No. of blocks with different block size using DWT and SIFT

Sr No	Image Size	Block Size	Execution Time (Sec)	No. of Blocks
1	**Palace,jpg (128*128)**	8	No forgery	No forgery
		16		
2	**Gun.jpg (512*512)**	16	1.5665	241
		32	0.4337	19
3	**Leopard.jpg (640*480)**	16	4.7760	824
		32	0.7680	140

4.2 Result of Proposed Method

Performance of the system is measured in the term of its accuracy, The images are randomly selected from database of MICC-F220. Time required for computation of different test images was found to be different and the average time centered around 2s.

- 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 2. Results of proposed methods

No of original image	No of forged image	TP	TN	FP	FN
25	25	24	22	1	3

$$Accuracy = \frac{TP + TN}{TN + FP + TP + FN}$$

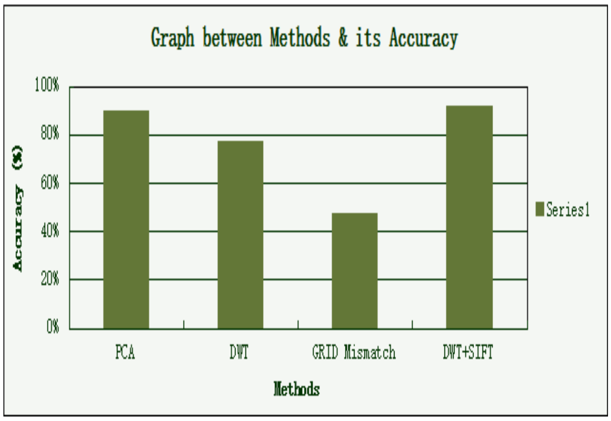
$$Accuracy = 92\%$$

4.3 Comparison with Exiting Methods

Table 3: Performance Comparison

Image	Block size	Execution Time in Seconds		Number of potentially similar blocks	
		Existing method	Propose method	Existing method	Propose method
Gun. bmp (640 *480)	8	17.8	6.5624	4685	2458
	16	25.10	4.4953	1560	824
Leopard. bmp (256 *256)	8	3.92	1.9189	4664	297
	16	5.43	0.2973	3469	99

Accuracy of various methods and the proposed method was compared between Zhang-2008 [6] achieved an accuracy of 77.32% with the tampered region size 64x64. The method proposed by Popescu-2004[14] managed an accuracy of around 90% for a tampered block size of 128x128 in an image of size 512x512 and JPEG quality factor of 85. Li- 2009 [10] was able to manage an accuracy of 47.21 %. However this low value of accuracy was compensated by high values of sensitivity and specificity. The proposed method achieved an accuracy of 92% over 50 images. It has to be noted that the proposed method is for detection of copy-paste forgery only.



Graph 1: Accuracy of Proposed Method with PCA, DWT, Grid Mismatch methods

5. CONCLUSION

In this paper discrete wavelet transform (DWT) has been used with Scale Invariant Feature Transform (SIFT) for reliable detection of the duplicated region in the copy move forged images. Simulation performed on original and forged images of the MICC-F220 dataset with different processing operations show's that combination of DWT and SIFT improves the detection performance as compared to discrete cosine transform (DCT) only. Overall accuracy was found to be 92% with a database of 50 images (25 original and 25 forged images),It is also observed that as the number of keypoints extracted from the DWT decomposed image increases. DWT with SFT shows the best detection results in terms of both accuracy and time taking for result computation as compared to the existing methods. Based on the performance of the improved method for "copy move forgery detection" in digital images, we can highly recommend extending this research in future to deal with problem such as rotation and scales and work on videos where search for duplicated blocks to perform on multiple image frames.

6. REFERENCES

[1] Saiqa Khan, Arun Kulkarni, "Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform" International Journal of Computer Applications (0975 – 8887) Volume 6– No.7,September 2010, pp 31-36.

[2] Sunil Kumar, Jagannath Desai, Shaktidev Mukherjee "A Fast DCT Based Method for Copy Move Forgery Detection", In Proceedings of 2013 IEEE second International Conference on Image information processing (ICIIP-2013), pp 649-654.

[3] Neha Jadhav, Suvarna Kharat, Punam Nangare " Copy Move Forgery Detection Using DCT", International Journal of Emerging Technologies and Engineering (IJETE)Volume 2 Issue 3, March 2015, ISSN 2348 – 8050, pp 38-42.

[4] Ashima Gupta, Nisheeth Saxena, S.K Vasistha, "Detecting Copy move Forgery using DCT", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013, pp 1- 4.

[5] 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.

[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.

[7] N.Anantharaj, "Tampering and Copy-Move Forgery Detection Using Sift Feature", International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014, pp 2132-2137.

[8] Prabhaka Telegarapu, V. Jagan Naveen, A. Lakshmi Prasanthi, G. Vijaya Sant, "Image Compression Using DCT and Wavelet Transformations", International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol 4, No.3, September 2011, pp 61-74.

[9] Xiaolong Li. "General Framework to Histogram-Shifting-Based Reversible Data Hiding", IEEE Transactions of image processing, Vol. 22, No. 6, June 2013, pp 2181-2191.

[10] Li, Weihai, Yuan Yuan, and Nenghai Yu. "Passive detection of doctored JPEG image via block artifact grid extraction." Signal Processing, vol. 89, no. 9, September 2009, pp 1821-1829.

[11] Amanpreet Kaur, Rich Sharma" Copy-Move Forgery Detection using DCT and SIFT" International Journal of Computer Applications , Volume 70– No.7 , May 2013 , pp 30-34.

[12] Salam A. Thajeel,.“A Survey of Copy Move Forgery Detection Techniques”, Journal of Theoretical and Applied Information Technology, Vol.70 No.1, 10th December 2014, pp 25-35.

[13] Rohini. A. Maind, “Image Copy Move Forgery Detection using Block Representing Method”, International Journal of Soft Computing and Engineering , Volume-4, Issue-2, , May 2014, pp 49-53.

[14] Popescu, Alin C. , and Hany Farid, "Exposing digital forgeries by detecting duplicated image regions", Department of Computer Science Dartmouth College, Technical Report, August 2004, pp 1- 11.

[15] Nandini Singhal and Savita Gandhani, “Analysis of Copy-move Forgery Image Forensics: A Review”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.7 (2015), pp.265-272.

[16] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, Elli Angelopoulou “An Evaluation of Popular Copy-Move Forgery Detection Approaches”, IEEE Transactions on Information Forensics & security, Vol 7, No.6, December 2012 , pp 1841-1854.