ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Comparative Analysis of Wavelet Transform Functions in Image Forgery Detection

Manjima Mishra[1], Dr.Preeti Rai[2]

Student, Department of CSE, GGITS, R.G.P.V. University, Jabalpur, India

Assistant Professor, Department of CSE, GGITS, R.G.P.V. University, Jabalpur, India[2]

ABSTRACT: Image forgery detection system is used to identify the authenticity of an image. With the availability of digital software and high resolution hardware, digital images can be easily tampered and manipulated. This is because now a days digital images can be manipulated in such a way that forgery cannot be detected visibly. This vogue directs major compulsion and decline the reliability of digital images. This paper presents comparative results of Wavelet Coefficients for copy move image forgery detection.

KEYWORDS: Copy-move, Discrete Wavelet Function, Image forgery detection, Feature extraction.

I. INTRODUCTION

Acquiring digital image as official document has become an accepted mode and the scope of low cost technology in which the image could be easily manipulated are two most denoting impression towards image forgery detection. Even though there are many technologies to identify the digital image forgery, their implementation is limited by the conditions imposed by many systems.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

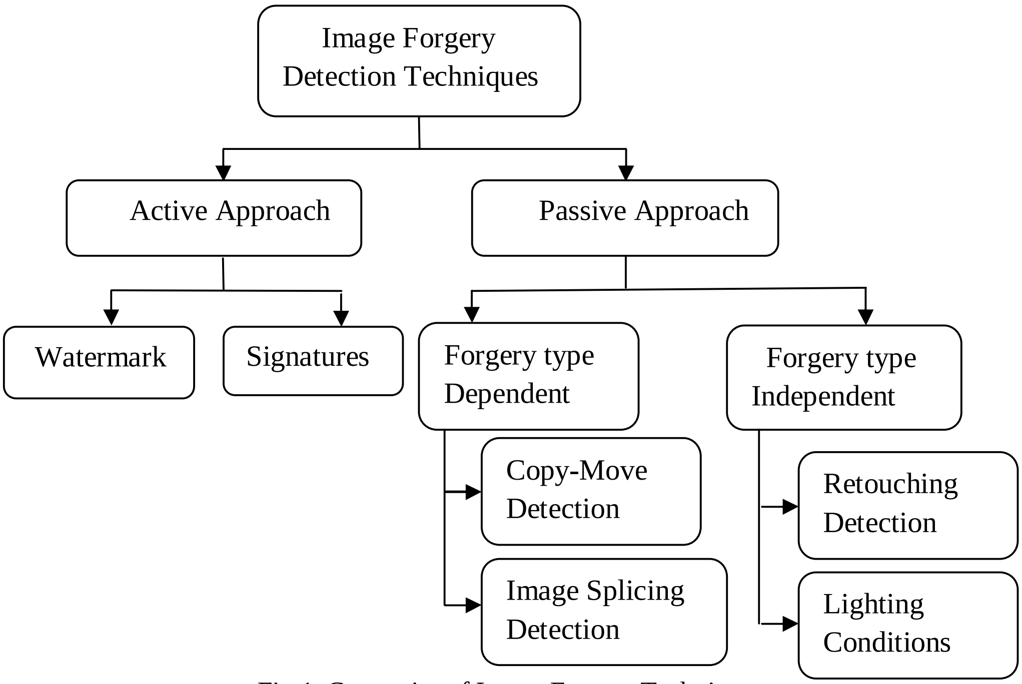


Fig.1. Categories of Image Forgery Techniques

Digital Image forgery techniques are divided in to two approaches (Fig 1). They are active approach and passive approach. In Active approach, the digital images desire some pre-processing such as watermark embedding or signature generation at the time of creating the image. There are many images in internet without water marking or digital signatures. In such case active approach could not be used to find the authentication of the image. So, the second approach is used.

The passive approach does not need any digital signature generated or watermark embedded in advance. Passive techniques are further classified as forgery dependent methods and forgery independent methods. Forgery dependent detection methods are designed to detect only certain type of forgeries such as copy-move and splicing which are dependent on the type of forgery carried out on the image while as forgery independent methods detect forgeries independent of forgery type but based on traces left during process of re-sampling & due to lighting inconsistencies.

A. *COPY-MOVE*

In this paper, we are considering a specific type of image forgery where a part of the image is copied and pasted on another part of the same image mostly to cover an important object. An example for this type of forgery can be seen in Fig 2. This process can be done without any modifications on the duplicated regions. It is not always necessary, some additional post processing operations are often performed either on the copied region before pasting it or on the whole forged image, to make the forgery concealed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

(a) (b)

Fig.2. An example of copy-move forgery (a): Original Image With three different Lids. (b): Forged Image with two same Lids.

II. RELATED WORK

Various methods of copy move image forgery has been reviwed. Suvarna G. Upase et.al.,[20] they use both block based method Discrete Wavelet Transform (DWT) and feature based method Scale Invariant Feature Transform (SIFT) to increase the robustness and accuracy of copy-move forgery detection. Ghorbani et. al.,[13] proposed DWT-DCT (QCD)-based copy-move image forgery detection. Authors used DWT and resolved the image into sub-bands and then performed DCT-QCD (quantization coefficient decomposition). A. C. Popescu et. al.,[4] state that PCA is efficient to extract the image features. Rajeev Kaushik et. al.,[18]propose a new approach here a slide window centred on every pixel of the suspicious image, then each window is passed through two dimensional discrete cosine transform ($2D - DCT$) to obtain the quantized coefficient matrix. Huang et al.,[11] develop a method based on Scale Invariant Feature Transform (SIFT) descriptors. After extracting the descriptors of different regions, they match them with each other to find manipulated area in images. Sutthiwan et. al.,[10] presented a method for passive-blind colour image forgery detection which is a combination of image features extracted from image luminance by applying a rake – transform and from image by using edge statistics. Leida Li et. al.,[15] this paper presents a method for detecting image forgery based on circular pattern matching. The tampered image is filtered and divided into circular blocks. Using Polar Harmonic Transform (PHT) rotation and scaling feature is extracted from each block. The feature vectors are lexicographically sorted and the manipulated regions are detected by finding the similar block pairs after applying post-processing.

III. PROPOSED ALGORITHM

The proposed algorithm contains the following steps for the proposed method:

1. Select a $P \times Q$ suspected image I (if the image is coloured, we can use the standard formula:
   $I = 0.228R + 0.587G + 0.114B$
   to convert into grey scale image).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

2. Slide window of size ($p \times p$) on the suspected image pixel by pixel from left to right and top to bottom. Each Sliding window is denoted as W_{ji}, where i and j indicates the starting point of the window's row and column, respectively.

$$W_{ji}(x, y) = I(x + i, y + j)$$

where $x, y \in \{0, 1, \cdots, p-1\}$, $i \in \{1, 2, \cdots, P-n+1\}$ and $j \in \{1, 2, \cdots, Q-n+1\}$.

Hence, we obtained the total number of overlapped image windows as

$$T_{windows} = (P - n + 1) \times (Q - n + 1)$$

from suspicious image I.

3. Coefficients matrix is obtained by applying DWT to each sliding window W_i,
$i = (P - n + 1) \times (Q - n + 1)$

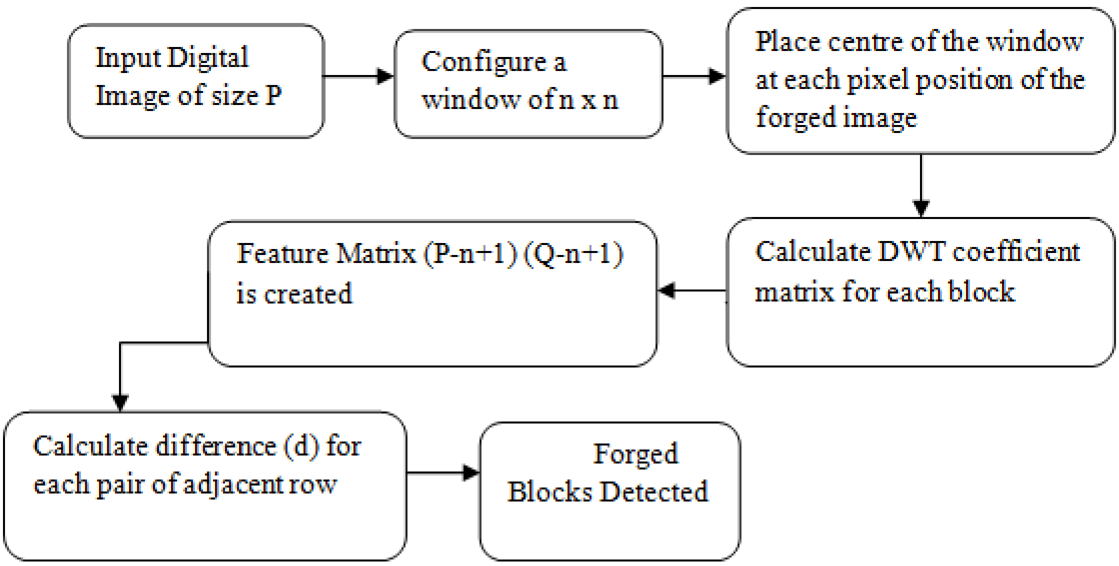


Fig.3: Image Forgery Detection Flow Chart

4. The feature vectors extracted from each quantized matrix W_i obtained in step 3, are arranged in a matrix, denote as F with the size of $(P - n + 1)(Q - n + 1)$ and defined as

$$F = \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_{(P-n+1)(Q-n+1)} \end{bmatrix}$$

5. Record the location of each block of each sliding window W_i in matrix row and column wise.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

6. The difference between adjacent pairs of rows of matrix F is calculated by:

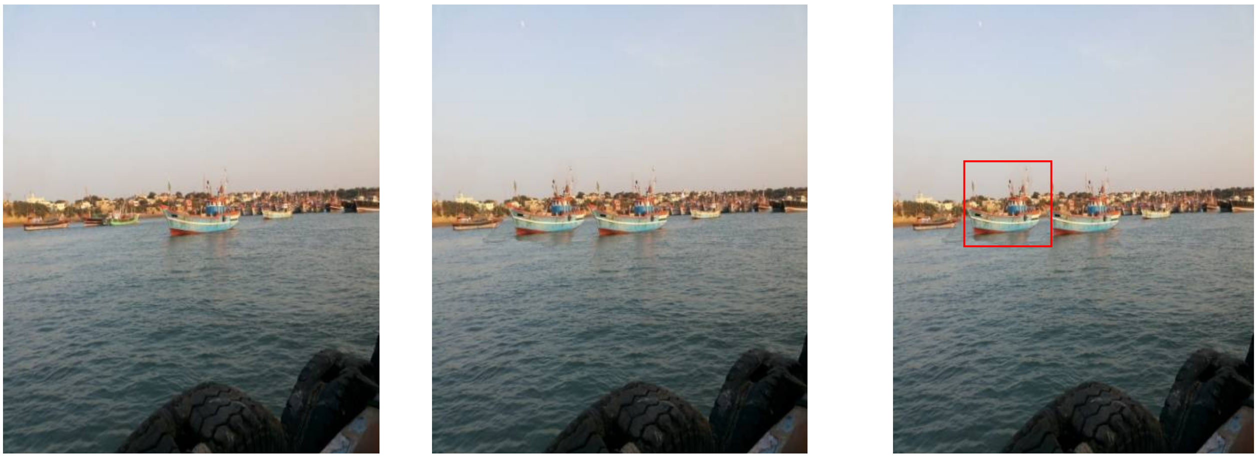
$$d(f_i, f_{i+1}) = \sqrt{\sum_{k=1}^{4}(f_i - f_{i+1})^2}$$

IV. SIMULATION RESULTS

For performance evaluation of the copy move image forgery detection algorithm 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 150 pixels to 350 pixels. The algorithm is coded in MATLAB R2012b on a machine equipped with Intel i3 1.90 GHz processor with 4GB RAM. The forged images contain either square or rectangular forged regions which have been copied and pasted. The following original images have been shortlisted from the VLC datasets for running the program, shown in Fig.4, Fig.5. & Fig.6. below.

(a) (b)

Fig.4. Lids Image (a) Original Image (b) No forgery Detected



(a) (b) (c)

Fig.5. Boat Image (a) original image (b) tampered image (c) detection result

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

(a) (b) (c)

Fig.6. Tree Image (a) original image (b) tampered image (c) detection result

TABLE: I COMPARITIVE ANALYSIS OF WAVELET FUNCTIONS

Images	**Coefficient**	**Forged Blocks**	**Execution Time (sec)**
Lids Image	**Detail**	No Forgery Found	2.452
	Approximation		3.718
Boat Image	**Detail**	432	2.005
	Approximation	422	2.000
Tree Image	**Detail**	354	3.128
	Approximation	350	4.899

V. CONCLUSION AND FUTURE WORK

In this paper functions of DWT has been used for reliable detection of the duplicated region in the copy move forged images. Detail coefficients performed on VCL dataset show's that combination of DWT and detail improves the detection performance as compared with approximation coefficients. DWT with detail coefficients shows the best detection results in terms of both accuracy and time taking for result computation as compared to approximation coefficients. Based on the performance of the improved method for "copy move forgery detection" in digital images, it is highly recommend extending this research in future to deal with problem such as rotation and scales where search for duplicated blocks to perform image frames.

REFERENCES

1. Mohd Dilshad Ansari, S. P. Ghrera & Vipin Tyagi, "Pixel-Based Image Forgery Detection: A Review", IETE Journal of Education, August 2014.
2. Ashima Gupta, Nisheeth Saxena, S.K Vasistha, "Detecting Copy Move using DCT", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013.
3. Vivek Kumar Singh and R.C. Tripathi, "Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method " International Journal of Advanced Science and Technology Vol. 35, October, 2011.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

4. A. C. Popescu, and H. Farid, “Exposing digital forgeries by detecting duplicated image regions”, Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.
5. J. Zhang, Z. Feng, and Y. Su, “A new approach for detecting copy-move forgery in digital images,” in IEEE International Conference on Communication Systems, China, 2008.
6. XiaoBing KANG, ShengMin WEI, “Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics”, IEEE International Conference on Computer Science and Software Engineering, Wuhan, Hubei, p. 926 – 930, 2008.
7. M. K. Bashar, K. Noda, N. Ohnishi, and K. Mori, “Exploring Duplicated Regions in Natural Images”, IEEE Transactions on Image Processing, May 25, 2010.
8. P. Kakar and N. Sudha, “Exposing post processed copy-paste forgeries through transform-invariant features”, IEEE Trans Inf Forensics Security, vol. 7, no. 3, (2012), pp. 1018–28.
9. Muhammad, M. Hussain and G. Bebis, “Passive copy move image forgery detection using undecimated dyadic wavelet transform”, Digital Investigation, vol. 9, (2012), pp. 49–57.
10. P. Sutthiwan, Y. Q. Shi, S. Wei and N. Tian-Tsong, “Rake transform and edge statistics for image forgery detection”, Proc. IEEE International conference on multimedia and Expo (ICME), (2010), pp. 1463–8.
11. Huang H, Guo W, Zhang Y. Detection of copy-move forgery in digital images using SIFT algorithm. In: Proc. IEEE Pacific-Asia workshop on Computational Intelligence and Industrial Application 2008; 272–276.
12. Fridrich J, Soukal D, Luk, J. Detection of copy-move forgery in digital images. In: Proceedings of Digital Forensic Research Workshop 2003.
13. M. Ghorbani, M. Firouzmand, and A. Faraahi, “DWT-DCT (QCD) based copy-move image forgery detection,” in 18thIEEE International Conference on Systems, Signals and Image Processing (IWSSIP), 2011, pp. 14.
14. S. D. Lin et al., “An integrated technique for splicing and copy move forgery image detection,” in IEEE 4th International Congress on Image and Signal Processing (CISP), Vol. 2, 2011.
15. Leida Li, Shushang Li, Hancheng Zhu, Xiaoyue Wu ‘Detecting copy-move forgery under affine transforms for image Forensics”, Elsevier Computers and Electrical Engineering 40, 2014.
16. Saba Mushtaq and Ajaz Hussain Mir “Digital Image Forgeries and Passive Image Authentication Techniques: A Survey” International Journal of Advanced Science and Technology Vol.73 2014.
17. Tu K.Huynh, Khoa V.Huynh, Thuong Le-Tien, Sy C.Nguyen “A Survey on Image Forgery Detection Techniques” IEEE RIVF International Conference on Computing & Communication Technologies, Research, Innovation, and Vision for Future (RIVF) 2015.
18. Rajeev Kaushik, Rakesh Kumar Bajaj, Jimson Mathew “On Image Forgery Detection Using Two Dimensional Discrete Cosine Transform and Statistical Moments” 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015.
19. Chi-Man Pun, Xiao-Chen Yuan, Xiu-Li Bi “Image Forgery Detection Using Adaptive Over segmentation and Feature Point Matching” IEEE Transaction on information forensics and security, Vol. 10, No. 8, August 2015.
20. Suvarna G. Upase, Sunil V. Kuntawa “Copy-Move Detection of Image Forgery by using DWT and SIFT Methodologies” International Journal of Computer Applications (0975 – 8887) Volume 148 – No.7, August 2016.