Detection of Copy-Move Forgery of Images Using Discrete Wavelet Transform

Preeti Yadav

[1]Department of Computer Science and Engineering, RITEE
CSVTU, Raipur
Chhattisgarh India
preetiyadu@yahoo.co.in

Yogesh Rathore

[2]Department of Computer Science and Engineering, RITEE
CSVTU , Raipur
Chhattisgarh ,India
yogeshrathore23@gmail.com

Abstract-Digital images are used everywhere and it is easy to manipulate and edit because of availability of various image processing and editing software. In a copy-move image forgery, a part of an image is copied and then pasted on a different location within the same image. A copy-move image forgery is done either for hiding some image object, or adding more details resulting in at least some part being cloned. In both the case, image reliability is lost. In this paper an improved algorithm based on Discrete Wavelet Transform (DWT) is used to detect such cloning forgery. In this technique at first DWT (Discrete Wavelet Transform) is applied to the input image for a reduced dimensional representation. Then the compressed image is divided into overlapping blocks. After that Lexicographic sorting is performed, and duplicated blocks are identified. Due to DWT usage, detection is first carried out on lowest level image representation. This approach increases accuracy of detection process and reduces the time needed for the detection process.

Keywords- Copy-Move forgery, Digital Tempering, DWT, Cloning.

I. Introduction

Because of different types of digital cameras and user-friendly image editing software people can create and manipulate digital images easily. A digitally changed photograph can be indistinguishable from an authentic photograph. As a result, photographs no longer hold the unique stature as recording of events.

Copy-Move forgery is performed with the intention to make an object “disappear” from the image by covering it with a small block copied from another part of the same image[1]. Because the copied part come from the same image, noise components, Brightness, the color palette, and the other properties will be well-matched with the rest of the image, therefore it is very difficult for a human eye to detect such forgery.

Since the key characteristics of Copy-Move forgery is that the copied part and the pasted part are in the same image, one method to detect this forgery is exhaustive search, but it is computationally complex and more time is needed for detection.Therefore to increase the speed of operation process many researchers use blocking approaches [2]. D. Soukal, proposes DCT based copy-move forgery detection in a single image, In which The image blocks are represented by quantized DCT (Discrete Cosine Transform) coefficients, and a lexicographic sort is adopted to detect the duplicated image blocks [3]. A. C. Popescu and H. Farid proposed a similar detection method [4], in which the image blocks are reduced in dimension by using Principal Component Analysis (PCA). But the efficiency of detection algorithm was not good, because, blocks are directly extracted from the original image, resulting in a large number of blocks, G.Li, Q.Wu, D.Tu developed a sorted neighborhood method based on DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition) [5].In this method the computation of SVD takes lot of time and it is computationally complex.B.L.Shivakumar and Dr. S.Santhosh Baboo have proposed copy-move forgery detection method based on SURF, which detects duplication region with different size. Experimental result shows that the proposed method can detect copy-move forgery with minimum false match for images with high resolution[6] .

To further reduce the amount of computation, this paper proposes wavelet based approach where the use of wavelet transform reduces the dimensional representation of tampered images and shift vector is used as similarity checking criterion for identifying duplicity of overlapping blocks formed from the tampered images.

(a) (b)

Figure 1. Example of Copy-Move forgery (a) original image(b) tampered image

II. Proposed Method

In this proposed method of copy-move image forgery detection following steps are used

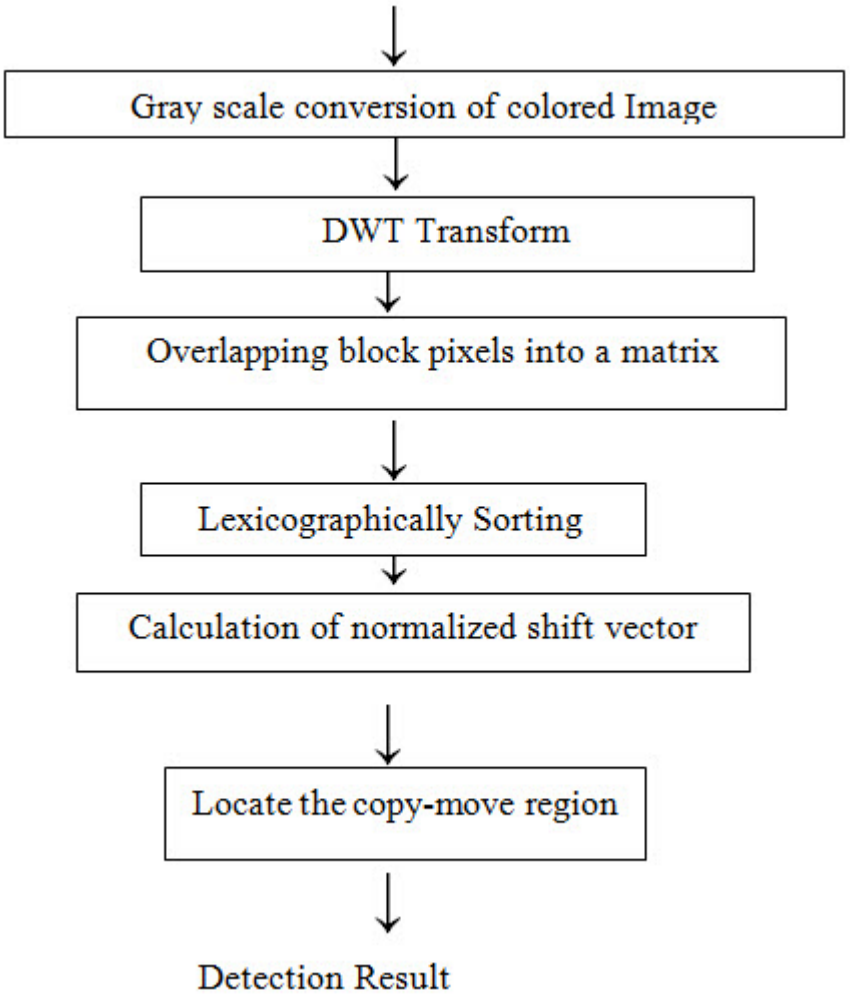

Fig 2. Forgery detection steps

Step I

Read the image selected by the user as input. If the input image is not a gray scale image then convert it into a gray scale image

Step II

DWT Transform: The Discrete Wavelet Transform is basically used to reduce the size of the image at each level, e.g., a square image of size $2^i \times 2^i$ pixels at level L reduces to size $2^{i/2} \times 2^{i/2}$ pixels at next level L+1.The image is decomposed into four sub images, at each level. The sub images are labeled LL,LH, HL and HH[7]. LL corresponds to the coarse level coefficients or the approximation image. This image is used for further decomposition.

.

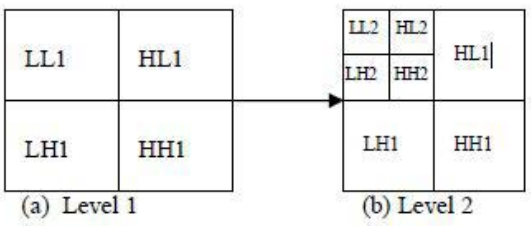

FIG 3. (a) level-1 dwt (b) level-2 dwt

After that a $B\times B$ block is slided over the resulting imag e and image is scanned from the upper left corner to the lower right corner.The DWT transform is calculated, For each block ,the DWT coefficients are stored as one row in the matrix *A*. The matrix will have $(M-B+1)\times(N-B+1)$ rows and $B\times B$ columns,Where M and N represents number of rows and columns of input image respectively.

Step III

Lexicographically Sorting: In this step lexicographic sorting is performed on the rows of matrix *A.* Now,in place of comparision of the pixel representation DWT coefficients for each block are being compared, if two consecutive rows of the sorted matrix *A* are found, the algorithm stores the positions of the identical blocks in a separate list B and increments a shift-vector counter *C*.

Step IV

Normalized shift vector Calculation: Now shift vector is calculated for a suspected pair of blocks, which are at the same vector distance from the corresponding block[8]. The shift vector *v* between the two matching blocks is calculated as

$$v = (v1, v2) = (x1 - y1, x2 - y2)$$

Where (x_1, x_2) and (y1, y2) are the positions of the two matching blocks.

After that shift vectors *v* are normalized, because the shift vectors –*v* and v correspond to the same shift. Then we increment the normalized shift vector counter *C* by one, for each identical pair of blocks:

$$C(v1, v2) = C(v1, v2) + 1$$

All normalized shift vectors are compared with user-defined threshold T, then the algorithm finds all normalized shift vectors v(1),v(2), …, v(*K*), whose occurrence exceeds a user-specified threshold *T*.

$$T: C(v(r)) > T \text{ for all } r = 1, \ldots, K.$$

Step V

Match block detection: To identify the segments that might have been copied and moved, the matching blocks that contributed to that specific normalized shift vectors are colored with the same color.Thus the threshold value *T* is related to the size of the smallest segment that can be recognized by the algorithm.

III. Experimental Results

(a) (b) (c)

Figure 3. Forgery detection result (a)Original image (b) tampered image (c) detection result

(a) (b) (c)

Figure 4. Forgery detection result (a)Original image (b) tampered image (c) detection result

Figure 5 Multiple Copy-Move Forgery detection result (a) Original image (b)tampered image (b) detection result

IV. Conclusion

In this paper an algorithm based Discrete Wavelet Transform (DWT) is Proposed for detecting copy move forgery,and experimental results show that compared with the existing related algorithms the dimension of the features is reduced. The algorithm gave best performance for detection of small size copy move forgery and can also detect multiple copy-move forgery. The algorithm has lower computational complexity because detection is first carried out on lowest level image representation.

V.Future Work

In future , I would like to apply Principal Component Analysis(PCA),to the feature vector to reduce its dimension, So the algorithm can gave more better results and time complexity will be further reduced.

References

[1] B.L.Shivakumar,Lt. Dr. S.Santhosh Baboo"Detecting Copy-Move Forgery in Digital Images: A Survey and Analysis of Current Methods "Global Journal of Computer Science and Technology Vol. 10 Issue 7 Ver. 1.0 September 2010

[2] Sarah A. Summers, Sarah C. Wahl "Multimedia Securityand Forensics Authentication of Digital Images" http://cs.uccs.edu/~cs525/studentproj/proj52006/sasummer/doc/cs525projsummersWahl.doc

[3] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copymove forgery in digital images," Proceedings of the Digital Forensic Research Workshop. Cleveland OH, USA, 2003.

[4] A.C.Popescu and H.Farid, "Exposing digital forgeries by detecting duplicated image regions," Dartmouth College, Hanover, New Hampshire, USA: TR2004-515, 2004.

[5] G.Li, Q.Wu, D.Tu, and Shaojie Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," IEEE International Conference on Multimedia & Expo, 2007.

[6] "Detection of Region Duplication Forgery in Digital Images Using SURF" B.L.Shivakumar and Lt. Dr. S.Santhosh Baboo IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

[7] Sunil Kumar, P. K. Das, Shally. "Copy-Move Forgery Detection in Digital Images: Progress and Challenges" International Journal on Computer Science and Engineering (IJCSE) February 2011 .

[8] 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.
[9] Rafael C. Gonzalez, Richard E. Woods, Steven L.Eddins,"Digital Image Processing using MATLAB",Second Edition, Pearson Publications, 2004.

AUTHORS PROFILE

Mrs Preeti Yadav is Assistant Professor in Department of Computer Science and Engineering at MM College of Technology, Raipur, C.G. ,India.she has received the Bachelor's degree in Computer Science Engineering from Chhattisgarh swami vivekanand University C.G. India in 2003,and Pursuing Master's degree(M-Tech 4th semester) in Computer Science From Chhattisgarh swami vivekanand University C.G.,India. Currently. Her research interest includes: Image Processing and Cryptography,Information Systems Security.

Mr. Yogesh Rathore is a Sr. Lecturer in Department of Computer Science and Engineering, Raipur Institute of Technology, Raipur (c.g.) . His area of interest include Digital image processing & Computer Graphics.