Copy Move Image Forgery Detection using Wavelet transform

L.V Santosh Kumar Y [#1], Ch. Sravani [*2], K.S Ravi Kumar[#3]
[#1,2,3]*Assistant Professors & Electronics and Communication Engineering*
Raghu Engineering College, Dakamarri.

Abstract— *Image manipulation is not a new trend and it exists from the time when photography was innovated. In the recent years, many forgery detection methods and techniques are proposed. Photo image forgery may include Copy-Move Forgery or Cloning and Copy-Create Image Forgery. There are few methods for forgery detection. Though many image forgery detections previously exist, with the change in algorithms the efficiency in the outputs will also be varied. The algorithm that implemented, identifies the forged part in the copy move forged input image. The algorithm is implemented using wavelet transform. For feature extraction, average information, that is, entropy of blocks of the image is calculated. The algorithm could able to identify the forged part in image which was copied and moved or copied, moved and scaled. Due to result efficiency we can use it in identifying forged images in civil, military and in other security essential services.*

Keywords — *Wavelet transforms, Copy-Move Forgery or Cloning and Copy-Create Image Forgery.*

I. INTRODUCTION

Image forgery detection techniques[1] are divided

into two categories:-

1. Active approach

2. Passive approach.

In the Active approach, Digital images require some pre-processing like Watermarking, or Digital Signatures etc. Digital Watermarking technique is the process of inserting a digital watermark (a known authentication code) into the image at source side, and then this code is being used for verification of digital information at the time of detection. Watermarks are inseparable from the images. There are more than millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authenticity of the image.

Passive approach is also called Blind approach which requires no prior information about the image. Image forensics is a passive approach that works on the assumption that these forgeries leave no visual traces; they might alter the statistical properties of the image, referred to as the fingerprints of image that characterizes the life cycle of image from its acquisition to its processing. Passive approach determines the location and amount of forgery in the image.

I.I FORGERY:

The process of altering an image for the sake of deceiving or change the public perception is called as "Forgery". Image forgery detection plays a significant role as digital images play a significant role in simplifying the way of representing and transferring ideas flexibly. There are two techniques for detecting the forgery. They are Active approach and Passive approach. In Active approach, it requires prior knowledge of the original image and it also requires human intervention and some specially equipped cameras. Because of these drawbacks, we chose passive approach. Passive approach is again divided into three types. They are Image Splicing, Image re-sampling and Copy-move forgery. Copy-move forgery is most commonly used forgery technique.

I.II COPY-MOVE FORGERY:

Copy move forgery is a type of forgery [2][3] in which a part of an image is copied from and pasted on a different location in the same image. As the copied part is from the same image, properties like noise components and color palette will be matched with the other parts of image and it makes more difficult to detect the forgery. One method for detecting such forgery is exhaustive search, but it is very complex and it requires more time for detection. There are two blocking approaches to reduce the time complexity. They are DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) which comes under frequency based techniques.

When DCT is applied to an image, it decomposes the image into frequency components. It can localize signals only in frequency domain. While re-constructing the image, there are certain blocking are facts that will affect the quality of image. Correlation of pixels inside the blocks is considered and the boundary pixels are neglected. There is no possibility for completely de-correlating the blocks at the boundaries using DCT. Due to these disadvantages, DWT [4] is used in the place of DCT. The paper organization is as follows: In section-I the introduction to image processing and the literature survey of image forgery and detection

and techniques to find about them are discussed. In section-II the proposed work is discussed which includes implementation of image forgery detection algorithm using wavelet transforms. The section-III includes original input images, forged input images and the simulated output results of forged input images. The paper was concluded in section-IV..

II. COPY-MOVE FORGERY BASED ON DISCRETE WAVELET TRANSFORM

Your DWT decomposes a signal into a set of basic 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. Wavelet decomposition of the images is used due to its inherent multi-resolution characteristics. The basic idea of using Discrete Wavelet Transform is to reduce the size of the image at each level, e.g., a square image of size $2^j \times 2^j$ pixels at level L reduces to size $2^{j/2} \times 2^{j/2}$ pixels at level L+1. Methods can differ in the type of the wavelet applied. At each level, the image is decomposed into four sub images. The sub images are labelled LL, LH, HL and HH. LL corresponds to the coarse level coefficients or the approximation image. This image is used for further decomposition. LH, HL and HH correspond to the vertical, horizontal and diagonal components of the image respectively. DWT offers a simultaneous localization in time and frequency domain. It is computationally very fast. It also separates the fine details in a segment.

II.I ALGORITHM

Step-1: Input

Consider a gray scale image or if any color image is selected convert it to gray scale image. As we detect copy move object or part in the input image, processing color image is not necessary. If we consider, there may be no change in the results but it takes more execution time as number of elements to be processed will be tripled. So, by considering the gray scale image as input to the system, it decreases execution time.

Step-2: Fitness function

After considering the image, fit the image to the standard size 512 X 512 using fitness function. If all the images are of same dimension, the output results can be more accurate than usual. It also increases the execution speed with accuracy.

Step-3: Image Segmentation

Now the 512 X 512 sized images is segmented into 'n' number of 'p X q' sized image blocks.

Where, 'n' represents total number of blocks, 'p' and 'q' represents total number of rows and columns in a block respectively.

This image segmentation is very much helpful in attaining the characteristics of the image accurately. While segmenting the image into different uniform sized blocks, one need to see that dimensions mismatch should not occur, and image reconstruction should be possible.

Step-4: Discrete Wavelet Transform

To all the segmented blocks, the discrete wavelet transformation (DWT) is applied. In DWT, low pass approximation, horizontal approximation, vertical approximation and diagonal approximation are calculated. Among all the approximations, low pass approximation is considered to the next level process of execution.

Step-5: Output Feature extraction

Calculate features like entropy, heuristic variance, skew, kurtosis etc for the output of DWT blocks. By extracting such features, the properties of the image can be known and is used to discriminate from block to block.

Entropy gives the average amount of information. It is given by the equation

$$\mathbf{E} = \frac{\mathbf{1}}{\mathbf{p_i}} \sum_{\mathbf{i=1}}^{\mathbf{N-1}} \mathbf{log}\ \frac{\mathbf{1}}{\mathbf{p_i}}$$

In this paper entropy of every individual output block of DWT is calculated.

Step-6: Feature extraction

The image is segmented into blocks by maintaining the uniform dimensions, so that no mismatch occurs while comparison. After segmentation, the entropy of every individual block is calculated.

Step-7: Overlapping blocks:

The feature extracted values of every individual block of output are overlapped onto each other for the comparison of similarities.

Step-8: Lexicographically sorting:

The compared values of overlapped blocks are sorted lexicographically. The positions of least values are identified and represented as the block number.

Step-9: Locating the forged region

The identified block after lexicographical sorting is replaced with black color.

Step-10: Output display

The image is reconstructed and displayed. The forged part[5] is displayed with black block replaced on it.

The algorithm is represented in flowchart and shown in figure 1.

III. S IMULATED RESULTS

Figure 2 shows the actual original images without any forgery. The forged images of the images in figure 2 are shown in figure 3.

All the input images are in RGB format, to attain their properties gray scale image will be sufficient, where the processing speed can be more. So, the algorithm is strictly designed based on gray scale images only.

If colour image is taken it is converted to gray scale image. In figure 4 the output i.e., the forged part in the image is highlighted and displayed. The black blocks on the image represents the forged part i.e., copy move part in the image.

In the three input images considered, in figure 3 (a), image 1 represents copy move part, in figure 3 (b) image 2 represents copy move and scaled part. Figure 3 (c) image 3 also represents copy move part. All the forged parts are identified in the figure with red colour circles.

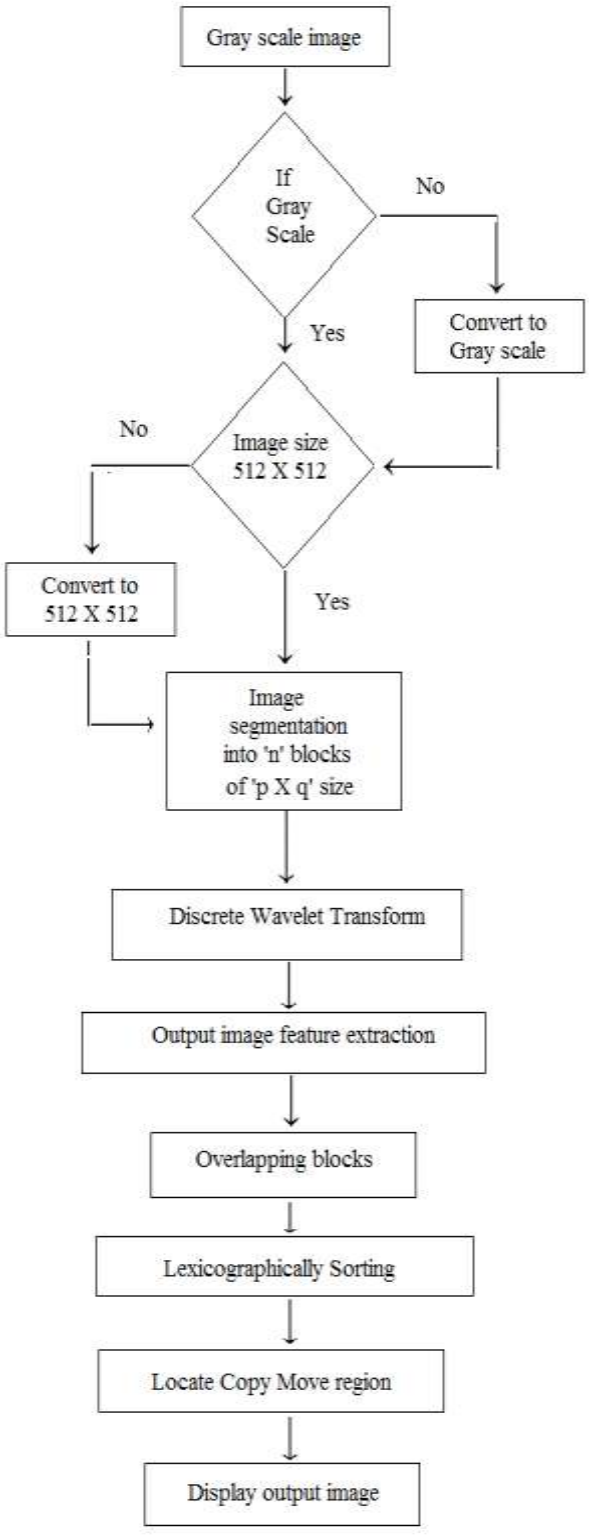


Figure 1: Flow chart of Image forgery detection.

A) Image 1

B) Image 2

C) Image 3

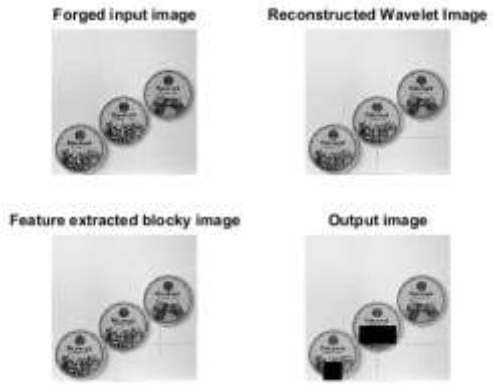
Figure 2: Unforgered image

A) Image 1

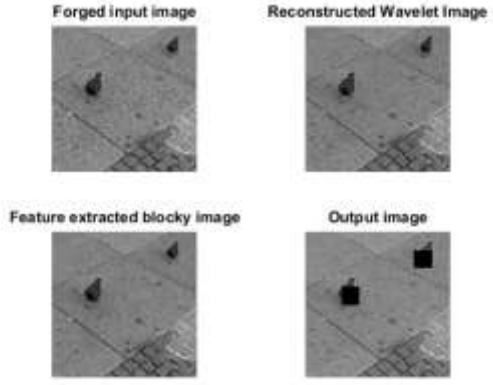
B) Image 2

C) Image 3

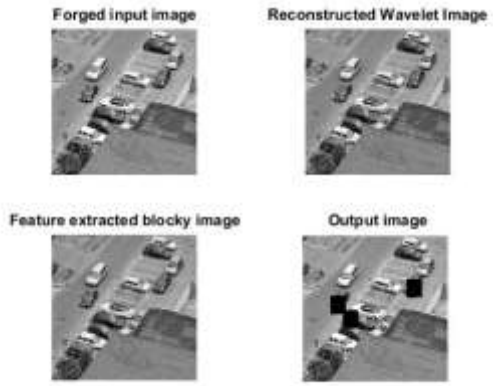
Figure 3: Forged image; forged part is in circle



a) Output Image 1



b) Output Image 2



c) Output Image 3

Figure 4: Output images

III. CONCLUSIONS

From the Outputs obtained, we have observed that the algorithm have given efficient results, the forged part, that is the part which was copied and moved from the same image was identified. The algorithm could able to identify the forged part within five sorted blocks. So, it is highly efficient in identifying the forged part. The algorithm has lower computational complexity because detection is first carried out on lowest level of image representation. As the results are much efficient we can use it in identifying forged images in civil, military and in other security essential services. By finding still more features may add complexity to the algorithm but can be still more efficient. In future, by finding variance, skew, kurtosis and any related features can increase the accuracy.

Acknowledgment

We express our deep sense of gratitude and thanks to Chairman **Sri. Raghu Kalidindi**, Raghu Educational Institutions, Principal Dr. R.Kameswara Rao, and Head of the Department ECE Mr. K. Phaninder Vinay, Raghu Engineering College, Dakamarri, Visakhapatnam, India for providing us the required infrastructure and support required.

References

1. Salam A.Thajeel and Ghazali Bin Sulong "state of the art of copy-move forgery detection techniques: a review" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013.
2. Pradyumna Deshpande , Prashasti Kanikar "pixel based digital image forgery detection techniques" International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 3, May-June 2012.
3. Hany Farid, "image forgery detection", ieee signal processing magazine, march 2009.
4. Preeti Yadav and Yogesh Rathore "detection of copy-move forgery of images using discrete wavelet transform", International Journal on Computer Science and Engineering (IJCSE) Vol. 4 No. 04 April 2012.
5. Deepika Sharma, Pawanesh Abrol "digital image tampering – a threat to security management" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2013.