AN OPTIMIZED APPROACH FOR FAKE CURRENCY DETECTION USING DISCRETE WAVELET TRANSFORM

T.Manikyala Rao[1], Dr. Ch. Srinivasa Rao[2]

Research Scholar, Department of Electronics and Communication Engineering, JNTU Kakinada[1]
Professor, Department of Electronics and Communication, UCEV[2]

ABSTRACT:

With the increase of modest technology, copy-move forgery detection has grown in a rapid rate that new era of forged images came true which has the same resemblance as the old ones i.e. difficult to find out with naked human perception. Fake currency detection is one in the effect that currency note is tampered in a way such it has the similar resemblance as the original one. So in order to find out the duplicate or forged portion of the image we go for different splicing algorithms using different techniques. Image forgery results to various security issues. Hence an efficient algorithm is required to detect the forgery in images. By using DCT algorithm blocks of the image are represented by DCT coefficients. Presence of blocking articrafts in DCT makes the method to be a drawback. Hence we propose DWT for segmentation of image. Lexicographical sorting is utilized to find out the cloned image blocks. Finally normalization is applied to find the distance in between similar vectors. In DWT provides better resolution and segmentation compared with DCT. In this paper, due to DWT, Image Forgery detection is done on low-level image representation. By using DWT better accuracy in finding out the forgery is achieved in a less time which gradually reduces complexity.

KEYWORDS:

Fake Currency detection, DCT, DWT.

1. INTRODUCTION:

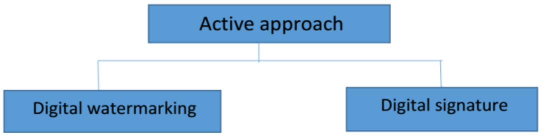
Forgery is the process of making, adapting, or imitating objects, statistics, or documents with the intent to deceive for the sake of altering the public perception, or to earn profit by selling the forged item. [1.]

Forging money or currency is widely often termed as fake or imitation of the original currency. Detection of Image Forgery is done in two techniques:

1. Active Approach
2. Passive Approach

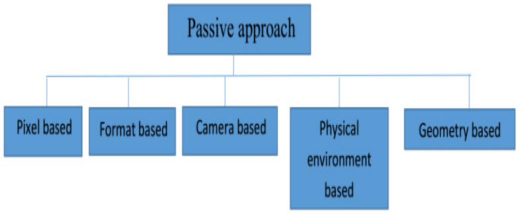
DOI: 10.5121/ijci.2016.5423

Active 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.

Passive Approach:



Passive approach is also called Blind approach which requires no prior information about the image. Passive approach clarifies both the location and the amount of forgery is done in an image.

Passive approach has two methods:-

1. Image Source Identification and
2. Tampering Detection

2. Image Tampering using Copy-Move Forgery Detection:

It is the widely used technique of copying and replacing the part of an image in context to change the meaning or to hide information of an image [1]. Hence a strong correlation exists between these that can be used as an evidence to detect image tampering or any Copy-move forgery.

If the copied parts are from the same image then it is very difficult to find the original one by extracting hue or any saturation points from the segments as they have the same gradient values and if the copied part of the image has any noise components or any distorted parameters then it is very difficult to find out the segment where it is copied and pasted. And because due to the dawn of new software’s these type of image tampering will be very essential to find out.

There are three techniques used to manipulate digital images. They are:

1. **Copy-Move**: This method defines the exact measure of cut, copy and move of one segment of image to other.

2. **Tampering**: it defines the manoeuvring of an image to achieve a drastic change in the other image.
3. **Splicing**: photographic manipulation in which two or more images can be super imposed on a particular image.

Image Tampering Detection based on Frequency Method (Discrete wavelet Transform):

Our method on image tampering detection is completely based on the frequency. The quantization levels are used to calculate the DCT Coefficients by taking a value called as quantization factor Q. By choosing the certain level of Q-factor lexicographically sorting is done before matching. The algorithm used for the DCT may give false positives by matching even mutual errors. However the algorithm cannot differentiate large identical textures of the natural image. Hence we preferred to detect the forged image using DWT and pixel matching. In this method we convert the forged image into Gray-scale image and calculate the DWT to the whole image to obtain sub bands and calculate the offset between copied and pasted regions. As the spatial offsets of the copied and pasted regions of the image are same, we obtain the part where the image is tampered.

Example of a Tampered Image:

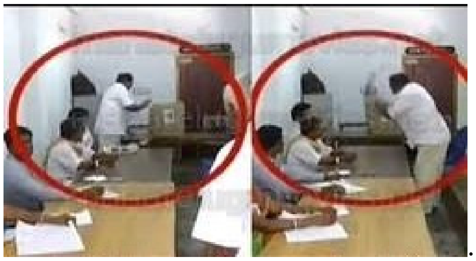


Fig1. The left part of the image is the original image taken in the pooling booth during local elections and the right part shows the tampered image.

Example 1. Shows the tampering of an image for the photo taken during elections. The person in the photograph (voter) has shifted from the left part of the image to the right. This image proves how the image tampering provides a disasterous effects during elections.

3. COMPARISON OF DIFFERENT FORGERY DETECTION TECHNIQUES

S.NO	Technique Name	Merits	Demerits
1.	Moment based 1. Blur	1. Lower Computational cost and time. 2. Fast Computation and effective blur identification 3. Less Complexity and need not necessary to know the original image information. 4. Segment of interest is able to identify effectively.	1. Not effective for complex image 2. helpful for small depth of field image 3. large database sampling is needed to prior of detection

			4.Only helpful to motion blur image
	2.HU	1.Robust and effective method detection 2. noise addition , blurring and compression etc., are done for post processing	1. Have many false Positives.
	3.Zernike	1.Flat regions of forgeries are detected	1. Calculating Zernike moment coefficient is complex.
2.	Dimensionality Reduction based 1.PCA	1.Efficient Method 2.Low false Positives	1. Low Efficient for low quality images 2.Low SNR and small blocks
	2.SVD	1. It can accurately measure	
	3.KPCA	1. Exact copy-move region is detected. 2. Works well in noisy compressed image	1. High noised and compressed image 1. block size should be much less than the duplicated image.
	4.PCA-EVD	1. The dimensions of the features are reduced. 2.The accuracy of the detection is good	1.Less Performance in detecting forgeries involving scaling, rotation etc.,
3	Intensity-Based 1.LUO	1.This method is efficient 2.It detects even JPEG compression and Gaussian noise	1. It fails when tampered region is rotated at some arbitrary angles
	2.BRAVO	1.It can accurately detect duplicated	1. Detect

		region	duplication in the region of uniform luminance
	3.CIRCLE	1.Working for post processing like noise addition, blurring , rotating etc	1.Scaling and geometric transformations cannot be detected.
4.	Frequency-Based 1.DCT	1.Copy move region is detected effectively	1.Less performance for any noisy image
	2.DWT	1.Exact copy move region will be detected	1.Works well in noisy and compressed region

In the above table of comparison for different Image Forgery Detection techniques or Real Segment identification of the forged image we are going to perform discrete wavelet Transform which gives better performance in noisy regions and also in the compressed regions. In our Paper, Fake currency note is identified by comparing the threshold values for each and every segment and whenever there is an error in the segmented portion of the image then it is so called tampered portion and it is identified and easily removed by using discrete wavelet transform.

4. Proposed Method for Image Tampering in Forgery Detection Using DWT:

Detection of the tampered images (Forged images) can be easily identified using dwt algorithm. In our paper, we first convert the Original RGB image into a Gray scale image and then observe the quantization levels of the image by using pixel intensity. And if we found any change in quantization values or pixel intensity values then the tampered portion of the image is identified and is shown when the image is converted into its real form as displayed in the results.

Proposed Algorithm Using Discrete Wavelet Transform:

The study of different Seismic signals can be done using different tools of the wavelet known as wavelet transformations. To find out the discrete components of a signal or a part of an image then we go for discrete wavelet transformation by using any of the series of the wavelets i.e. Haar wavelet, Mexican Hat wavelet and Shannon wavelet (which has the poor time resolution).

The proposed algorithm in our project is done in two Phases:

Phase I:
Identification of Matched and Reference Blocks:

In the current Phase of the paper the tampered image is first converted into a gray scale image and then we apply wavelet transformation and convert the overlapping pixels into matrix format and select the block which has the maximum contrast or max pixel intensity and sort the matrix. After sorting compare the phase correlation between the rows and sort the block into a new matrix which is the detected tampered segmented part of the image.

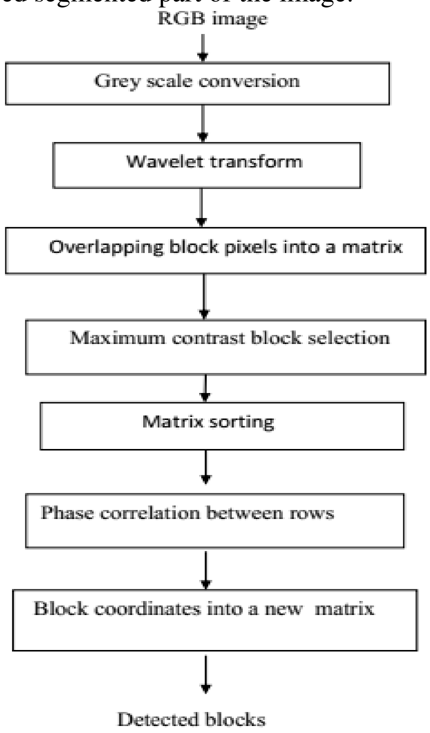

RGB image
Grey scale conversion
Wavelet transform
Overlapping block pixels into a matrix
Maximum contrast block selection
Matrix sorting
Phase correlation between rows
Block coordinates into a new matrix
Detected blocks

Fig2. Identification of Matched and Reference blocks

Phase II:
Verification on Resembling of Matched and Reference Blocks:

In this phase, a verification on resembling of matched and reference block is done in a robust method as shown in below figure 4.

At first we verify the candidate block of the LL-I image and compare with each and every block in the region of LL-I then compare the region directly with the image LL-II. So we can easily obtain the tampered portions or blocks of an image in a very ideal manner with less noise but the main point to be considered in this phase is the robustness of the algorithm or the process while verifying the identification of the matched and the original image.

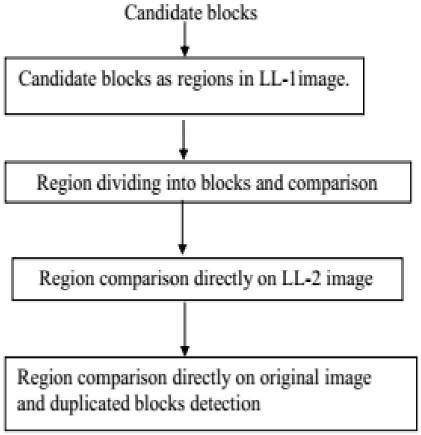

Candidate blocks
Candidate blocks as regions in LL-1image.
Region dividing into blocks and comparison
Region comparison directly on LL-2 image
Region comparison directly on original image and duplicated blocks detection

Fig3. Verification on resembling of matched and reference blocks

Proposed Algorithm:

The basic idea of using DWT is it reduces the size of the image at each level, e.g., a square image of size 2k ×2k pixels at level L reduces to size 2k/2 × 2k/2 pixels at level L+1. At each level, the image is spliced into four sub images labelled as LL, LH, HL and HH. LL corresponds to the coarse level coefficients or the approximation image.

In the First Phase the real image is converted into Gray scale image and segmented blocks of tampered image is identified and in the second phase, the discrete wavelet transform is applied for each and every wavelet of the segmented blocks and the tampered parts will be marked and displayed as a result.

Algorithm for Identification of Matched and Reference Blocks: [3]

```
1. User's image is taken as the input.
2. Convert the RGB image into a Gray scale image.
3. Apply discrete wavelet transform up to level L to the converted gray image.
4. For each overlapping m × m block in the LLL image
    4.1. Form a matrix X of dimension m2 columns and (Km+1) × (L-m+1) rows by extracting the resulting pixel values by rows into a row of X.
    4.2. Create another matrix Y same as X with two additional columns for storing top-left coordinates.
5. End
6. Highlight blocks where contrast is low.
7. Sort matrix X lexicographically.
8. for each row of X
    8.1. Compute the phase correlation for the block corresponding to the current row with the blocks corresponding to "x" rows above and below the current row.
    8.2. If the computed maximum phase correlation value exceeds a preset threshold value "T", then store the top left coordinates of the corresponding reference block and the matching block from Y matrix in a new row of a matrix.
9. End
```

Algorithm for Resembling Verification of Matched and Reference Blocks: [3]

```
1. For LLL-1 level in the image pyramid
 1.1. For each row of the matrix
  1.1.1. Form a reference region by padding “l” pixels on all the sides of the m × m reference block.
  1.1.2. Form a matching region by padding “l” pixels on all the sides of the m × m matching block.
  1.1.3. For each m × m overlapping of the reference region.
   1.1.3.1. Find corresponding match in matching region based on Phase correlation but search process has to be opted for selected part of matching region.
   1.1.3.2. If the computed maximum phase correlation value exceeds a preset threshold value, then the top left coordinates of the corresponding reference block and the matching block are stored in a new row of a matrix.
 1.2. End
2. End
3. For LLL-2 level to original image in the image pyramid
 3.1. For each row of the matrix
  3.1.1. Form a reference region by padding “l” pixels on all the sides of the m × m reference block.
  3.1.2. Form a matching region by padding “l” pixels on all the sides of the m × m matching block.
  3.1.3. Compare them using Phase Correlation.
  3.1.4. If the computed maximum phase correlation value exceeds a preset threshold value, then store the top left coordinates of the corresponding reference block and the matching block in a new row of a matrix.
 3.2 End
4. End
5. Plot the blocks as tampered regions on the given input image.
```

5. FLOW CHART AND BLOCK DIAGRAM OF THE PROPOSED WORK:

Fig4. Flow Chart of the Proposed Work using DWT

Fig5. Block Diagram of Proposed work using DWT

Procedure for Tampered Image Identification and Marking:

P1: Select any particular image if it is assumed to be tampered and convert the Real image into Gray scale if the image at the input is not represented in Gray level.

P2: Apply Discrete Wavelet Transform

In this step, by applying the discrete wavelet transformation the original size of the image is reduced to half and transmitted to the next level.If the size of the image taken in a square matrix is 2j*2j, then the reduced image using DWT will be 2j/2*2j/2 and the level L is incremented to the next level L+1 which is as shown in the reference image below.

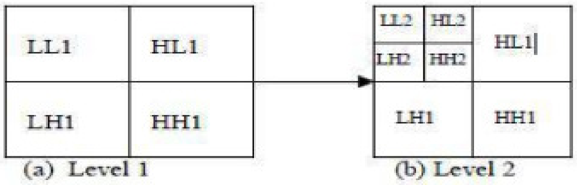


Fig6. (a.) Level 1 and (b.) Level 2

In the next level the image is decomposed into sub images with levels LL, LH, HL, HH as shown in the figure 7.

P3: Lexicographically Sorting:

In this method, the blocks in the matrix "X" is compared instead of Pixels and if it has the same values the algorithm stores the positions of the identical blocks in a separate other matrix "Y" and the counter is incremented with a value.

P4: Normalized shift vector Calculation:

Now the blocks having same segmented values will be compared with a shift vector "S", which increments the shift vector counter "C" to "C+1", after the shift has done and compares it with the normal positioning threshold of the image. The shift vector S can be written as

$$S = (s1, s2) = (p1 – q1, p2 –q2)$$

Where P1, P2 and Q1, Q2 are the positions of the matched blocks.

P5: Match Block Detection

The Blocks which has the same segmented values will be compared with the threshold value which has the smallest size of the segment and the image is re-coloured to show on which part of the image is tampered.

6. SIMULATION OUTPUTS:

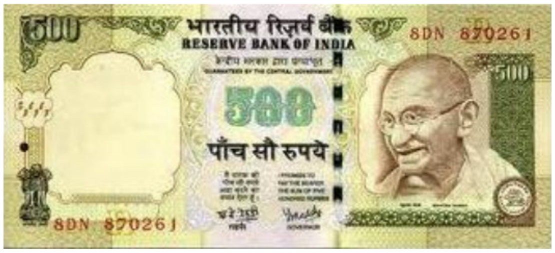


Fig7. Original Note

The figure 8, Represents an original 500 rupee note. This note has been forged and we need to identify those tampered regions by using DWT algorithm. This can be done by first converting the RGB colour image into grey scale image this is shown below.

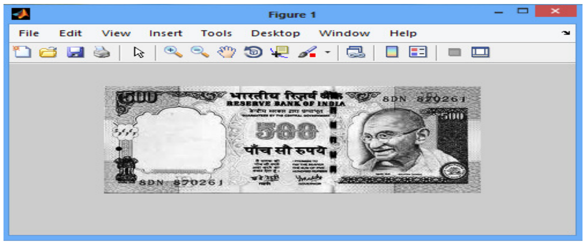


Fig8. Original RGB Converted into Gray scale

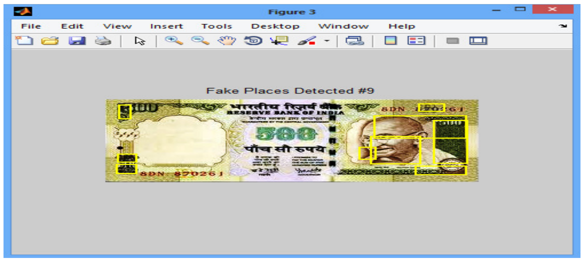


Fig9. Detection of Tampered Regions

The Resultant figure represents the regions in which tampering takes place. This is identified by applying DWT transform and calculating distance between the pixels. If the distance among the neighbouring pixels are same then that regions are said to be forged.

7. CONCLUSION:

Fake currency detection is one in the effect that currency note is tampered in such a way it has the similar resemblance as the original one. Hence an efficient algorithm is required to detect the forgery in images. By using DCT algorithm blocks of the image are represented by DCT coefficients. Presence of blocking articrafts in DCT makes the method to be a drawback. Hence we propose DWT for segmentation of image. Lexicographical sorting is utilized to find out the cloned image blocks. Finally normalization is applied to find the distance in between similar vectors.

REFERENCES:

[1] 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.

[2] Salam A.Thajeel and Ghazali Bin Sulong "STATE OF THE ART OF COPYMOVE FORGERY DETECTION TECHNIQUES: A REVIEW" IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 2, November 2013.

[3] 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.

[4] 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.

[5] Hashmi, Mohammad Farukh, Aaditya R.Hambarde, and Avinash G. Keskar. "Copymove forgery detection using DWT and SIFTfeatures", 2013 13th InternationalConference on Intellient Systems Design andApplications, 2013.