International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

Image Forgery Detection Method for Copy- Move and Splicing Attacks Using Block wise DCT, DWT and Correlation

Shankar A [1], Dr. V. Prakasam [2]

1(GCET,JNTUH Affiliated, Hyderabad, India)

2(ECE, PBR VITS Nellore,India),

Abstract

Images are used to enhance the news articles in the newspapers, evidence in the court of law, legal documents and mostly in social networking sites, etc. But with the advancements in image editing tools, images are open to several falsifications, therefore tampered images are easily created that are difficult to be recognized through naked eye. To carry out such forensic analysis, several technological detections have been developed in the literature. However, most of them are less precise and time-consuming. In this paper, the image authentication technique is based on Discrete Cosine Transform, Discrete Wavelet Transform and Correlation which detects the forgery accurately. DCT, DWT are used for dimensionality reduction. The compressed image is divided into overlapping blocks of fixed size. Correlation is then performed between the blocks which detects the region of forgery. Edges of forged region are detected by Canny edge detector. Proposed method improves the detection time, precision, recall, accuracy. It is robust to rotation, noise, scaling and multiple copy-move forgeries and splicing attacks.

Keywords- *copy-move,correlation, canny edge detection, DCT, DWT,Image forgery, splicing*

1. Introduction

Our mind interprets visual imprints very rapidly. Images can explain any incidence in much better than thousands of words. Since computers were not available earlier, everyone used to believe whatever is visible in the image through newspapers, articles, magazines, etc. Using powerful image editing tools such as Adobe Photoshop, an image can be altered with a wide variety of manipulation techniques such as scaling, rotation, blurring, resampling, filtering, cropping, etc. Due to which authenticity of the image is lost. With the advancement in information technology, digital images can be sent from one place to another place very easily and hence false information is spread in news, social media, TV.

Forgeries in an image can be done by adding, removing, changing the features of an image. Image forgery results in significant alteration in image data and can change the sense of information shown by the image. Thus, authentication of originality of images is required in variety of applications such as forensics ,military, media, newspapers, etc.

ISSN: 2454-9665

In Copy-Move Forgery, a portion of the original image is copied and pasted at different location on the same image. The detection of Image Forgery is unidentifiable through the naked eye because the segment is from the same image so the characteristics like noise, color patterns all are compatible to the rest of the image. In Image Splicing Forgery, a portion of the original image is copied and pasted in different images.This type of forgery introduces additional objects and appears as a real image. The sole purpose of image splicing forgery is to bring additional information or hide an important data in an image which is originally not present. Hence, detection of such forgeries are essential as they lead to misinformation.

Forgery may be performed in many different ways. Out of these, the commonly used method is copy move forgery and image splicing. Existence of two same regions is not common in natural images and this property is exploited to detect copy move forgery. Even after applying some post processes, like edge smoothing, and noise adding to remove the visible clues, there exist two extremely similar regions in the manipulated image. One of the most frequently used methods to detect such type of forgery is to use block matching algorithm. In the block matching algorithm the image is divided into overlapping blocks and the blocks are matched to find the duplicated region. Many people have used it to find duplication of the region with different features representing one block of the image.

2. Literature survey

Kumar, et al. [3] presented the fast DCT based copy-move image forgery detection method, where input image is selected and then divided into overlapping blocks after that DCT is applied to extract the features of the blocks and sorting blocks and performing block matching then highlighting the duplicated region. Fattah, et al. [2] presented 2D-DWT method in which block matching is performed when all overlapping blocks are compared with selected candidate non- overlapping blocks to detect the forged region. Ketenci, et al. [5] presented Copy-move forgery detection in images via 2D Fourier Transform, in this the input image is divided into overlapping blocks then four dimension features are extracted using 2D-FT on each blocks and uses block matching algorithm to detect the forged region.

Harpreet Kaur and Sheenam Malhotra, et al. [8] proposed the method that improves copy-move forgery detection using DCT, correlation, and sobel edge detector. Here, the image is first compressed using (DCT) Discrete cosine transform is used to compress an image and introduce blocking artifacts at the block boundaries which helps to detect forgery. Fahime Hakimi et al [10] proposed a method of detecting image splicing using Local Binary Pattern and DWT.Maind et al.[1] proposed Copy-Move Forgery Detection using Block Representing, where DCT is applied to generate the quantized coefficients and then representing the each quantized block by a circular and extracting appropriate feature from each circle block and then search for similar block match. Block representing have been suggested to detect copy-move forgery but one of the major issues of this method is detection time.

International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

3. Proposed approach

In proposed approach, as shown in Fig 1 forgery is detected by using Discrete Cosine Transform and Discrete Wavelet Transform.DCT is applied to forged image for dimensionality reduction which introduces blocking artifacts which helps us detect forgery. Then DWT is applied on the DCT compressed image.In DWT, the compressed image divided into 4 sub-bands – LL, LH, HL and HH. The LL sub-band is divided into fixed size overlapping blocks of B*B pixel.

The division of compressed image into overlapping blocks is again to improve the speed of computation and ability to find the region of forgery accurately in less time. The same process is carried out for the original image. Then, correlation is performed between the blocks of the forged image and original image which yields the forged region. The correlated image is then converted to binary image and then edges are extracted using canny edge detector. Refinement of the edges detects the forged region accurately.

3.1. Convert Color Image into Grayscale Image

For the implementation of proposed method, the colour input image Im of size M x N is converted to a grayscale image using Im = 0.229R+ 0.587G+0.114B(1) where R, G and B are red, green, and blue components of image Im, respectively.

3.2. Discrete Cosine Transform

Discrete cosine transform is applied to the image for dimensionality reduction or compression. DCT is used for faster computation of detection of forgery. The Discrete cosine transform has the ability to detect the tampered region accurately.

The DCTequation F(u,v) is given below,

$$= \frac{2}{N} c(u)c(v) \sum_{x=1}^{N} \sum_{y=1}^{N} f(x,y) \cos\left[\frac{(2x+1)u\pi}{2N}\right] cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (2)$$

After compression, images are reconstructed from its transform using Inverse-DCT equation f(x,y) is

$$= \frac{2}{N} c(u)c(v) \sum_{x=1}^{N} \sum_{y=1}^{N} F(u,v) \cos\left[\frac{(2x+1)u\pi}{2N}\right] cos\left[\frac{(2y+1)v\pi}{2N}\right] \quad (3)$$

International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

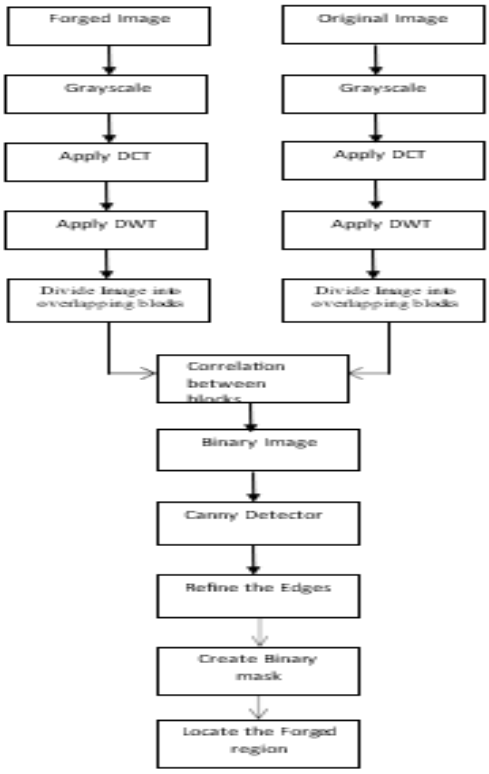


Fig 1: Block diagram of proposed approach

33 . Discrete Wavelet Transform

Discrete Wavelet Transform (DWT), a multi-level decomposition method. In the proposed approach, Haar wavelet is used to reduce the dimension of the image, and then four sub-bands LL, LH, HL and HH are output. Since the LL sub-band contain the maximum data, it is taken for further procedure. The two-dimensional wavelet and scaling functions are obtained by taking the tensor products of the one-dimensional wavelet and scaling functions. The two-dimensional DWT leads to a decomposition of approximation coefficients at level j in four components: the approximation at level $j + 1$, and the details in three orientations (horizontal, vertical, and diagonal). The following chart describes the basic decomposition steps for images as shown in Fig 2.

International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

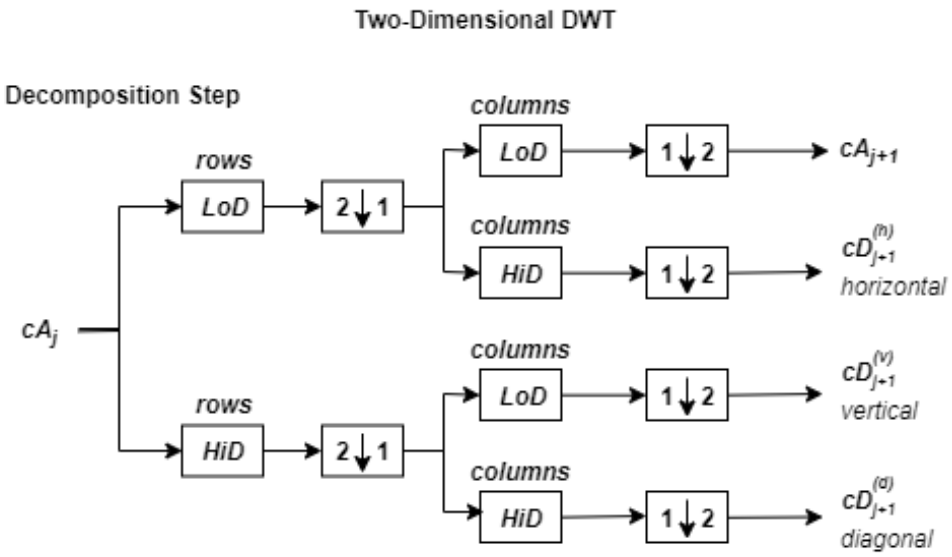


Fig 2

where

- 2↓1 —Down sample columns: keep the even-indexed columns
- 1↓2 — Down sample rows: keep the even-indexed rows
- rows X — Convolve with filter *X* the rows of the entry
- columns X —Convolve with filter *X* the columns of the entry

The decomposition is initialized by setting the approximation coefficients equal to the image *s*: $cA_0 = s$.

3.4 . Divide Image Into Overlapping Blocks

The image after compression using DCT, is divided into fixed size blocks such as M x N grayscale image first split up into overlapping blocks of B x B pixels. The blocks are slid by one pixel along the image from the upper left corner to the lower right corner.

$$B_{ij}(x, y) = f(x + j, y + i) \quad (4)$$

where x, y belongs to {0,… B-1}, i belongs to {1,…M-B+1}, j belongs to {1,….N-B+1}.

ISSN: 2454-9665

The number of overlapping blocks can be obtained by using the following equation,

N blocks =(M-B+1) (N-B+1)

3.5. Correlation Between The Blocks

Correlation method is used as a statistical tool to establish the association between two variables. The 2D correlation is defined as follows,

$$\frac{\sum_m \sum_n (A_{mn}-\bar{A})\ (B_{mn}-\bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn}-\bar{A})^2)(\sum_m \sum_n B_{mn}-\bar{B})^2)}} \quad (5)$$

where A, B are means of forged and original image, M x N is size of image, m=1,2,3,4,…M, n=1,2,3,…N.

3.6. Binary Image

The image obtained after correlation is then converted to its binary form that is into black and white pixels. Black pixels represents the forged region and white pixels represents unforged region. This binary form is useful as it neglects the unnecessary grayscale pixels.

3.7. Canny Edge Detector

The Canny edge detector is an edge detection operator that uses a multi-stage algorithm to detect a wide range of edges in images. It was developed by John F. Canny in 1986.The algorithm runs in 6 separate steps:

3.7.1. Smoothing: Removal of noise from the image.

3.7.2. Determination of gradients: The edges are marked where the gradients of the image has magnitudes.

3.7.3. Calculation of direction: In this step, direction of edge should be calculated.

3.7.4. Non maximum suppression: Only local maxima are marked as edges.

3.7.5. Double thresholding: Potential edges are determined by thresholding that uses two thresholds high and low. The values higher than high threshold is considered as strong edge and the values lower than low threshold are discarded and the values between high and low thresholds are considered to be weak pixels.

3.7.6. Edge tracking : Lastly, edges are determined by suppressing all edges that are not connected to very certain (strong) edge

3.8. Refine the Edges

Refinement of the edges of detected region and remove the objects that have fewer pixels from binary image using morphological operations.

3.8.1. Locate the forged area

The forged area can be highlighted with purple colour which gives us actual tampering location.

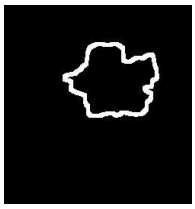
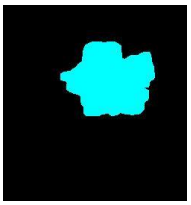
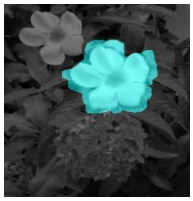
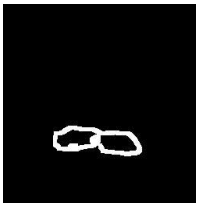
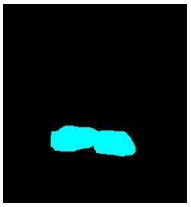
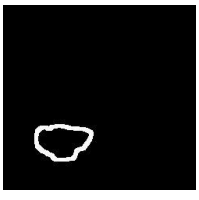
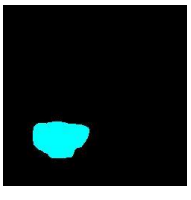
International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

4. Experimental results

The proposed approach is performed on a personal computer with Intel 1.80 GHz Core i5 processor and using MATLAB Online 2020b software. Adobe Photoshop is used to forge the images. The performance of the proposed technique is evaluated on dataset of 40 images in which 20 are original images and 20 are forged images. The dataset consists images of size 256 x 256 pixels. In the experimentation , block size is considered

10x10.

a.Copy- move image forgery detection

Original Image	Forged Image	Correlated Output	Refined output	Color Mask	Identification of Forgery
					
					
					

International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

b) Image splicing forgery Detection

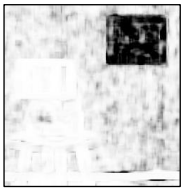
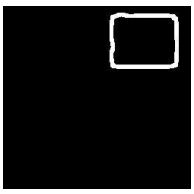
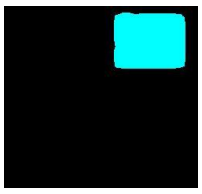
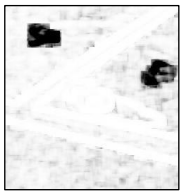
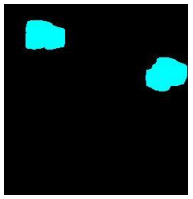
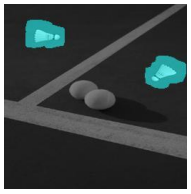
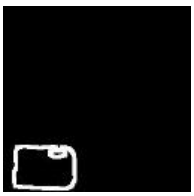
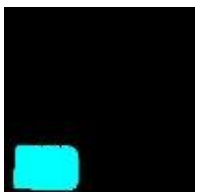
Performance of proposed method is evaluated and compared with block representing method.

Table 1 :

Images	Block reprsenting method (in sec)	Proposed method (in sec)
Image1	48.05	10.301
Image2	49.4	8.3560
Image3	31.03	7.8943

4.1.Detection Time

For evaluation of results, comparion between proposed and block representing method on the basis of performance characteristics are shown in table1.

Original Image	Forged Image	Correlated Output	Refined output	ColorMask	Identification of Forgery
					
					
					

TP (True Positive) is number of forged images that have been perfectly detected as forged.

International Journal of Innovative Research in Science and Engineering
Volume 9, Issue 12, 2023
www.ijirse.com
ISSN: 2454-9665

Factors	Proposed Method
TP	11

FP (False Positive) is number of forged images that have been wrongly detected as forged.

FN (False Negative) is number of original images that have been wrongly missed but they are forged.

TN (True Negative) is number of original images correctly detected that have been truely detected as not-forged. **Table 2 :**

Parameters	Block Representing Method	Proposed Method
Precision	75.25%	91%
Accuracy	87.00%	96%
Recall	92.46%	100%

4.2. Precision

It is defined as the ratio of number of true positive to the sum of true positive and false positive.

$$\text{Precision Rate}=\frac{TP}{TP+FP} \times 100 \quad (6)$$

4.3. Accuracy

It is defined as the ratio of sum of the true positives and true negatives to the total.

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN} \times 100 (7)$$

4.4. Recall Rate

It is defined as the ratio of number of true postives to the sum of true positives and false negatives.

$$\text{Recall Rate} =\frac{TP}{TP+FN} \times 100 (8)$$

The comparision between block representing method and proposed method based on precision rate, accuracy and recall rate are as follows

ISSN: 2454-9665

Table 3 :

TN	10
FP	1
FN	0

5. Conclusion and Future scope

The objective of proposed image forgery detection method is recognize image manipulation and detect the region of forgery accurately in less time. The significant domain in digital image authentication is Copy-Move Forgery Detection (CMFD) and Image Splicing Forgery Detection (ISFD). Therefore, Discrete Cosine Transform , Discrete Wavelet Transform are applied for dimensionality reduction or compression and division of compressed image into overlapping blocks of size 10 x 10. Correlation is used for similarity measure which extracts a tampered region. The Canny edge can easily detect edges and their various orientations and the region forgery is detected accurately. From the results, a conclusion can be drawn that proposed method not only effectively detects multiple copy-move, image splicing forgeries and precisely locates the forged areas but also is robust to various attacks such as rotation, scaling, brightness, blur, noise. Compared with a block representing a method[1]and copy-move forgery detection [3], the detection time of proposed method is very less. Precision, recall, and accuracy is also higher than existing block methods [1][3].

The proposed method can be enhanced to abate the processing time to detect the forgery in the images to few seconds or even micro seconds. The accuracy of detecting forgery in image using traditional methods is attained to certain level, improvement in existing techniques is required for better accuracy and precision. Combination of machine learning algorithms could be a better option to yield accuracy in future.

References

[1] R. A. Maind, A. Khade, "Image copy move forgery detection using block representing method," International Journal of Soft Computing and Engineering," Vol. 4, Issue 2, pp: 49-53, May 2014.

[2] S. A. Fattah, M. I. Ullah, M. Ahmed, C. Shahnaz, "A Scheme for Copy Move Forgery in Digital Images based on 2D-DWT," IEEE, pp: 801-804, Oct 2014.

[3] S. Kumar, J. Desai, S. Mukherjee, "A fast DCT based method for copy move forgery detection," Second international conference on image processing, IEEE, pp: 649-654, May 2013.

[4]Y. Huang, W. Lu, W. Sun, D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Science International, pp: 178–184, July 2013.

[5] SenihaKetenci and GuzinUlutas, "Copy-move forgery detection in images via 2D Fourier Transform" , Telecommunications and signal processing (TSP), 36th International Conference, July 2013.

[6] Chhaya Saini, Priya Singh, Pramod Kr.Sethy, Raj Kumar Saini "Digital Image Forgery Detection using Correlation coeffcients", International Journal of Computer Applications(0975-8887), Volume 129- No., November, 2015.

ISSN: 2454-9665

[7] Rafeal C. Gonzalez, Richard E. Woods , Steven L. Eddins“ Digital Image Processing using MATLAB”, second edition.

[8] Harpreet Kaur , Sheenam Malhotra , “Improving copy-match forgery detection time by using DCT, correlation and sobel edge detector”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol.5 Issue I, January 2017.

[9] Abhishek Kashyap, Rajesh Singh Parmar, Megha Agarwal, Hariom Gupta, “An Evaluation of the Digital Image Forgery Detection Approaches”.

[10] Fahime Hakimi , Mahdi Hariri, FarhadGharehBaghi, “Image Splicing Forgery Detection using Local Binary Pattern and Discrete Wavelet Transform”, IEEE, 2nd International Conference on Knowledge-Based Engineering and Innovation, 2015.