Detection of Copy-Move Forgery Exploiting LBP Features with Discrete Wavelet Transform

Anuja Dixit
Madhav Institute of Technology & Science, Gwalior, India

Rahul Dixit
National Institute of Technology, Rourkela, India

R. K. Gupta
Madhav Institute of Technology & Science, Gwalior, India

ABSTRACT

Copy-move forgery is being used at various fields to hide significant information or to append additional information in image. Image forgery results in false interpretations. In this forgery, one section of image is copied and then it is pasted over the same image at different location. Although, various techniques are suggested by researchers but finding forged section of varying size and located at different locations on image is complicated. To resolve such problems we introduce a new hybrid approach for finding copy-move forgery based on Discrete Wavelet Transform with Local Binary Pattern. At First, image is moldered into three color components. Discrete Wavelet Transform is applied over the image which results in four sub bands. Approximation sub image contains low frequency components having maximum information. LL subimage is divided in overlapping blocks. Local Binary Pattern is calculated for blocks to generate descriptors to match similar blocks. Shift vectors are computed to find group of block pairs with similar shifting. It is observed by our experimental results that proposed method can efficiently detect manipulated images having different forgery size with high detection accuracy and low false positive rate as comparison to other state-of-the-art.

Keywords

Copy-move forgery, Discrete Wavelet Transform, Image forgery detection, Local Binary Pattern, Region duplication

1. INTRODUCTION

Nowadays, for transferring information images and videos are used widely. Visual media is adequate to explain, spread and reposition. These features allow them as substantial medium for transmitting information with information technology based communication devices. Images and videos have ability to influence judgments related to criminal investigation. They are considered as valuable evidence to reflect the veraciousness of any information. However, pictures losing their believability due to alteration in pictures referred as image forgery [1]. Several image processing application software are originating which are responsible for exponential increase in image manipulation [2]. Forgery over images can be done very easily by using these tools. Although, due to digitization and advent of information technology image domain is highly profited. Due to day by day elaboration in digital imaging [3], digital data is confronting many issues related to its robustness and reliability. On account of digital image processing software like GIMP, Corel Draw and Photoshop image forgery is very easy task. A person with little knowledge about these tools can do forgery without any effort. These tools facilitates various features and tractability for alteration in images but affecting integrity and authenticity of digital pictures [4]. To affirm the integrity and detection of authenticity of digital images is one of the hot research issue in image processing field. Due to wide acceptance and speedy growth of this discipline resulted in many researches in this field speculating lot of research publications in recent years [5].

Primarily, Image forgery is classified in three categories, which are image splicing [6], image retouching [7] and copy-move. This paper is based on providing a new approach for detection of copy-move forgery. In copy-move forgery a segment of the image is copied and pasted at different location on the same image for altering or to bring additional information in image. Broadly, image forgery detection method can be divided in two classes, which are active approach and passive approach. In active approach, digital watermarking [8] and digital signature [9] is used which is embedded in image. For checking authenticity of images, signatures and watermark are extracted from the image and compared to known signatures and watermark to verify the authenticity of images. Active approaches requires expensive equipment. Every image necessarily don't have signatures and watermarks embedded to them which could be exploited for forgery detection. In passive approach, no previous information about image is expected.

A novel method based on passive approach is proposed in this paper for copy-move forgery detection. In the proposed method, if input image is a color image then its color components, which are red, green and blue are extracted. Discrete wavelet transform (DWT) is applied over extracted components of input image. Image decomposed in four sub bands, which are LL, HL, LH, and HH. Approximation sub image (LL) contains low frequency components of image which are rich in information. Further, image is divided in overlapping blocks of fixed dimension. Feature are extracted from each block using local binary pattern (LBP). Features are stored and lexicographically sorted for detecting blocks with similar features. Shift vectors are computed to find group of blocks with similar shifting to reduce probability of false matches. Finally, the similar blocks are shown with different color to visualize forgery. This paper is organized as follows. A brief review to copy-move image forgery detection techniques is provided in section 2. Related technical background is discussed in Section 3. Section 4 depicts our proposed method. Experimental results are presented and discussed in Section 5. Finally, the paper is concluded in section 6 with future research work.

2. RELATED WORK

In recent years, many methods are suggested by researchers for copy-move image forgery detection. Fridrich et al. [10] used discrete cosine transform (DCT) for extracting features from blocks of input image. Q-factor is decided for quantization of coefficients. This algorithm produces less false matches and robust to 5^0 rotation. Zhang et al. [11] proposed a method using DWT. In their method image is decomposed in four sub bands. Spatial offset is computed between copied and pasted region of image to detect forged areas. Bayram et al. [12] presented a method for copy-move forgery detection based on Fourier Mellin Transform (FMT). They divided image in overlapping blocks. Fourier transform is calculated for each block. Euclidean distance between block pairs is calculated to detect connected group of blocks at similar distance. Copied blocks up to 10^0 rotation and scaled up to 10% can be detected by their method. Li et al. [13] revealed a method based on Polar Harmonic Transform (PHT) for detecting copy-move forgery. Features corresponding to blocks of input image are extracted using orthogonal moment. In their method image is divided in circular blocks. Lexicographical sorting is performed so that similar feature vectors can be in proximity to each other. Their method can detect rotated forged blocks of image but cannot efficiently detect blocks with scaling and bending. Ghorbani et al. [14] explained a method for copy-move forgery detection based on Discrete Wavelet Transform and Discrete Cosine Transform. DWT is applied for decomposing image in four sub bands. Approximation sub image divided in blocks. Using DCT feature vector for each block is extracted. Further, Quantization coefficient decomposition is applied over DCT coefficients. For finding similar block pairs matching is performed. Li et al. [15] described a method using LBP. LBP is capable of depicting image texture. They divided image in circular block and LBP is used for feature extraction [16]. LBP features are rotation invariant. Euclidean distance is calculated for detecting similar block pairs. In their method morphological operations are used for removing false matches. Mahdian et al. [17] proposed a method based on blur moment. Blur moments are invariant to blur degradation and noise. Blur invariants used as features of each blocks of image. Further, they used principle component Transformation (PCT) for feature vector dimension reduction. For identifying similarity present in blocks k-d tree representation is used. This copy-move forgery detection method has high computational complexity. A study by Zhang et al. [18] revealed a method based on Hu moments. They used Gaussian pyramid for reducing size of input image. Further, input image is divided in blocks and features are extracted applying Hu moments. Lexicographical sorting performed over feature vectors to locate similar features in neighborhood. Morphological operations are applied for matching. Their method is robust to blurring and JPEG compression. Mohmadian et al. [19] explained a method based on Scale Invariant Feature Transform (SIFT) with Zernike moments. SIFT features cannot detect flat forged regions so Zernike moments are computed. Key points are extracted using SIFT algorithm. To reduce false matches hierarchical clustering is used. For flat regions image is divided in blocks and features are extracted using Zernike moments. Using threshold value for matching similar blocks are detected.

3. DISCRETE WAVELET TRANSFORM & LOCAL BINARY PATTERN

This section provides conceptual introduction to techniques used in proposed method for copy-move forgery detection. Proposed algorithm works upon a hybrid approach using DWT and LBP.

3.1 Discrete Wavelet Transform

DWT is a linear wavelet transform [20]. It works over vectors. Length of vectors is always integer multiple of two which classifies data vector into distinct components of frequency. Working of one-dimensional DWT is shown in Fig. 1. ‘l and ‘h’ shows low-pass and high-pass filter, respectively. Using two factor down sampling, approximation coefficients are obtained. As output from low-pass filter. Detail coefficients are obtained as output from high-pass filter using two-factor down sampling. Approximation coefficients are used for succeeding levels of transform. Output of low-pass and high-pass filters can be given by (1) and (2).

$$b_{i+1}[m] = \sum_{n=-\infty}^{+\infty} l[n-2m] b_i[n] \qquad (1)$$

$$c_{i+1}[m] = \sum_{n=-\infty}^{+\infty} h[n-2m] b_i[n] \qquad (2)$$

Images are decomposed using wavelets. Wavelet has inbuilt multi resolution characteristic. DWT is applied over image for decomposition of image which reduces image size after each level of decomposition.

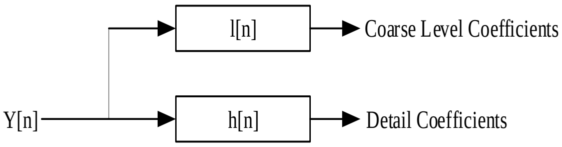


Fig 1: One-Dimensional DWT

Decomposition of an image using DWT is shown in Fig. 2. In two-dimensional DWT, DWT is applied for all rows then for all columns of an image. If input image is of size $2^k \times 2^k$ pixels at level L then after decomposition at level L+1 its size will be $2^{\frac{k}{2}} \times 2^{\frac{k}{2}}$ pixels. Different methods are used for applying wavelets over an image When DWT is applied over an image, at each level image get decomposed in four sub images. These sub images also known as sub bands. Four sub bands obtained after decomposition are LL, HL, LH and HH. HH, LH and HL sub images contains diagonal, vertical and horizontal component [21] of the image, respectively. LL is known as approximation or coarse level sub image. Subimages obtained after decomposition can be combined to regenerate the former image. DWT are applied for iterative comparison of similar blocks. If an image is decomposed to L levels then comparison of matching block of LL subimage at level L is indicated as LL_L.

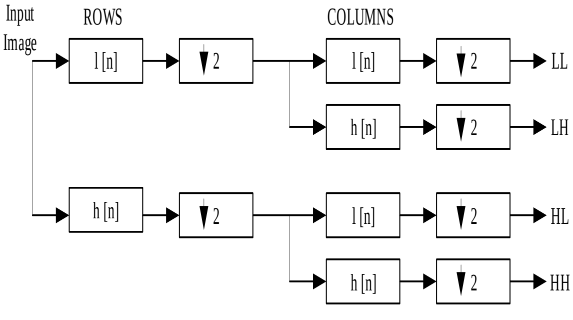


Fig 2: Image Decomposition using DWT

Overlapping blocks of iterative approximation band at different levels LL_L, LL_{L-1}, ……. LL_1. LL_L subimage is lowest resolution subband. Matching of overlapping blocks is performed at LL_L. Further, these blocks are promoted to succeeding higher level. Finally, matching is executed on original image. We are interested in using DWT because of it’s downsampling. Image size reduced for further analysis to find forgery involved in image.

3.2 Local Binary Pattern

LBP is a texture operator which extracts gray scale [15] values. LBP is used for identifying spatial image texture[22].

The texture pattern P of an image can be defined with distribution of V (V>1) gray level pixel values as in (3).

$$P = p(g_m, g_0, \dots\dots.., g_{V-1} \qquad (3)$$

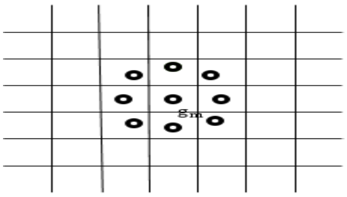
g_m is the gray level value of center pixel of local vicinity, $g_v(v = 0,1, \dots\dots\dots V-1)$ shows gray level values of neighboring pixels. If location of center pixel is assumed (0,0) and coordinate of local neighbours is shown by $(-R.\sin\left(\frac{2\pi v}{V}\right), R.\cos\frac{2\pi v}{V}))$. LBP is rotation invariant [23]. Three examples are shown in Fig. 3 for circularlt symmetric neighborhood for different values of (V,R). Interpolation is used for estimating the gray level values of local neighboring pixels which are not in center.

Gray level values of local neighborhood points are subtracted from the middle gray level value of circular symmetry as in (4).

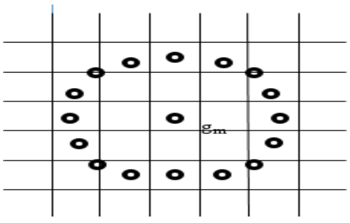
$$P = p(g_m, g_0 - g_m, \dots\dots\dots\dots, g_{V-1} - g_m \qquad (4)$$

If it is assumed that $g_c - g_m$ values (c=0, 1 ….V-1) are independent of middle gray level value g_m then (2) can be estimated as (5).

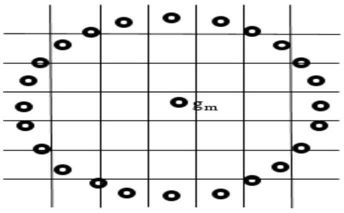
$$P \approx p(g_m)p(g_0 - g_m, \dots\dots\dots\dots., g_{V-1} - g_m \qquad (5)$$



(a) (V, R) = (8, 1)



(b) (V, R) = (16, 2)



(c) (V, R) = (24, 3)

Fig 3: Circular local neighbors for different values of (V,R)

Dispersion of gray level values of $p(g_{m)}$ is not associated with neighboring image texture [11]. According, no useful information can be achieved from them. Hence, (3) can be altered to (6) for explaining textural characteristics.

$$P \approx p(g_0 - g_m, \dots\dots\dots\dots, g_{V-1} - g_m \qquad (6)$$

Texture operator LBP is highly discriminative. It stores all patterns of neighborhood pixels. This operator stores deviation in gradient direction for regions lying at the edge (with low slope). Zero value is considered for the points lying at edge. Directions of neighboring points for every middle spots are different. Variation in mean luminance does not effectuate the signed difference $(g_v - g_m)$. Approximate values can be obtained using (7).

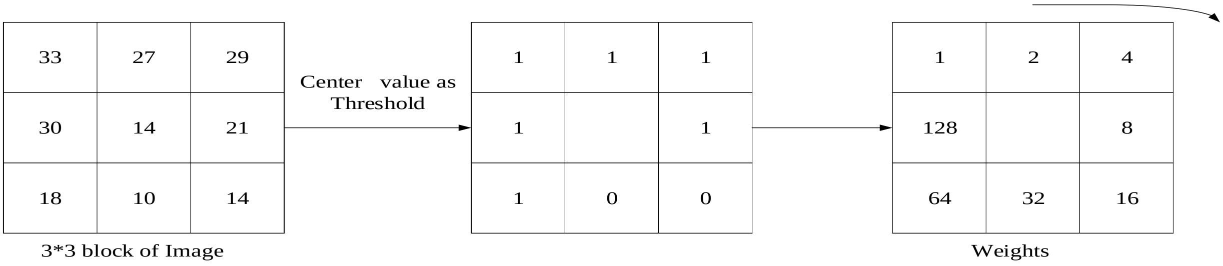
$$P \approx p(s(g_0 - g_m), \dots\dots\dots\dots, s(g_{V-1} - g_m) \qquad (7)$$

$$\text{Where } s(x) = \begin{cases} 1, \ x \geq 0 \\ 0, \ x < 0 \end{cases} \qquad (8)$$

Local image texture can be characterized into unique $LBP_{V,R}$ as in (9) using $s(g_v - g_m)$ as binomial factor2^v.

$$LBP_{V,R} = \sum_{v=0}^{V-1} s(g_v - g_m) 2^v \qquad (9)$$

When a region is copied from the image and it is pasted over the same image at different location, texture of copied and pasted segment remain similar even if post-processing operations are applied over copied segment. Hence, texture pattern analysis is effective in forgery detection. Fig 4 shows the calculation process of local binary pattern.



33	27	29
30	14	21
18	10	14

3*3 block of Image

Center value as Threshold

1	1	1
1		1
1	0	0

1	2	4
128		8
64	32	16

Weights

Fig 4: Calculation of Local Binary Pattern

LBP code for center pixel= 1+2+4+8+64+128
=207

4. PROPOSED METHOD

In this section, we proposed a copy-move forgery detection methodology. Operations of the proposed technique can be broadly divided in five primary steps which includes image decomposition, feature extraction, sorting of feature vectors, matching of similar blocks and removal of false matches using shift vectors. The operational flowchart representing the operation of the proposed method is shown in Fig. 5.

4.1. Preprocessing

The primary purpose of preprocessing is to setup image for feature extraction. In this step, image is decomposed in three color components: Red(R), Green (G) and Blue (B). These components are used for applying Discrete Wavelet Transform over image. Due to DWT image gets decomposed in four sub bands LL, HL, LH and HH. LL sub-band contain maximum information of an image. Hence, we selected it for further processing. As downsampling is used in DWT so image size get reduced to $1/4^{\text{th}}$ after each decomposition. Let input image is of size$M \times N$. M And N are number of rows and columns. Using DWT, its size reduced to$\approx (M \times N)/4$. In our method, image is divided in square blocks of dimension$B \times B$. Total no. of square blocks are$\left({}^{M}\!/_{2} - B + 1\right) \times \left({}^{N}\!/_{2} - B + 1\right)$.

4.2. Feature Extraction

In our method, texture operator local binary pattern (LBP) is used for feature extraction. For $\left({}^{M}\!/_{2} - B + 1\right) \times \left({}^{N}\!/_{2} - B + 1\right)$ number of blocks, features are extracted. For each block features are stored in a row vector. All feature vectors are stored in matrix$X$. Copied and pasted blocks have same feature vectors. To find similar blocks, we identified same feature vectors. If feature vectors are matched with each other for finding similarity then computational cost will be substantially high. For reducing matching time, lexicographical sorting is applied over matrix$X$. This sorting technique results in occupation of similar feature vectors in neighborhood of each other and similar feature vectors can be located in small-scale range. Fig. 6 show the process of feature extraction for an image block using LBP approach.

4.3. Feature Matching

The sole purpose of feature matching is to find similar blocks of image correctly. In proposed method, shift vectors are computed for finding blocks with similar shifting. Position of blocks corresponding to similar feature vectors are stored as center co-ordinates. Let (a_1, a_2) and (b_1, b_2) be the locations of two similar blocks. The shift vector between blocks can be computed as in (10)

$$sh = (sh_1, sh_2) = (a_1 - b_1, a_2 - b_2) \qquad (10)$$

$-sh$ And sh, both shift vectors represents same shifting so they can be normalized. If required, shift vector is multiplied with -1 such that$sh_1 \geq 0$. Counter value C of normalized shift vector increased (as shown in (11)) whenever block pair with same shifting is detected.

$$C(sh_1, sh_2) = C(sh_1, sh_2) + 1 \qquad (11)$$

Initially, counter value is set as zero. When this process finished, counter value shows frequency of occurrence of different shift vectors corresponding to matching blocks. A threshold is set for occurrence of normalized shift vectors$sh^{(1)}, sh^{(2)}, \ldots\ldots\ldots\ldots, sh^{(k)}$. Shift vectors having counter value greater than user defined threshold $C\left(sh^{(m)}\right) > Th$. Where, $m = 1, \ldots\ldots\ldots, k$. Block pair corresponding to shift vectors having counter value greater than threshold are considered as matching blocks. If threshold value is large then some matching blocks will be detected as non-match. For small value of threshold too many false matches will occur.

4.4. Post-processing

Using shift vectors, matched blocks are detected. Blocks with similar shifting are labeled with different color to show forged region of input image.

5. EXPERIMENTAL RESULTS & DISCUSSION

In this section our experimental results of proposed copy-move forgery detection methodology are presented. All experiments are performed over a machine with Intel core i3 2.40GHz processor, 32 bit operating system and 4GB RAM. MATLAB 2013a is used for analyzing results of image forgery. For analyzing forgery results, images are taken from three different databases which are CVG UGR Image Database [24], CoMoFoD database [25] and USC SIPI Image Database [26]. 100 different images are collected from these databases and they are manually forged to get results related

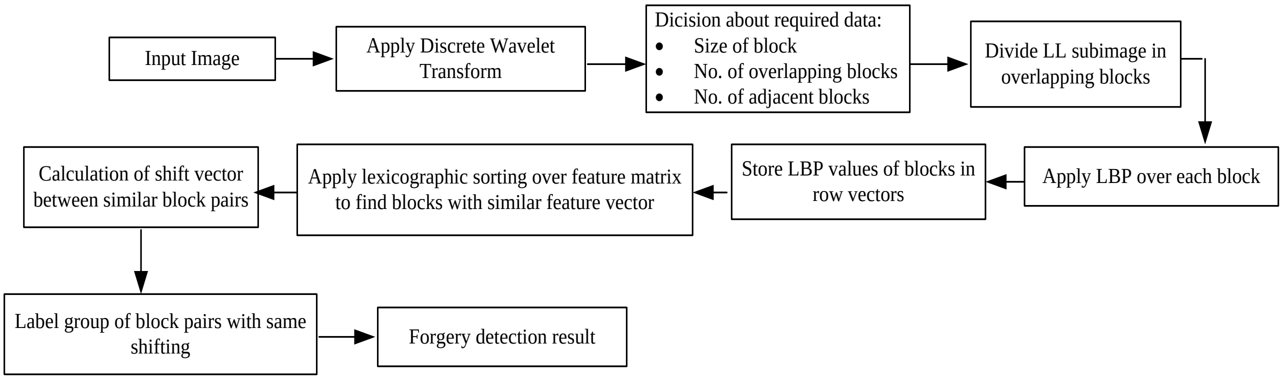

Input Image
Apply Discrete Wavelet Transform
Dicision about required data:
Size of block
No. of overlapping blocks
No. of adjacent blocks
Divide LL subimage in overlapping blocks
Apply LBP over each block
Store LBP values of blocks in row vectors
Apply lexicographic sorting over feature matrix to find blocks with similar feature vector
Calculation of shift vector between similar block pairs
Label group of block pairs with same shifting
Forgery detection result

Fig 5: Operational Flowchart of proposed methodology

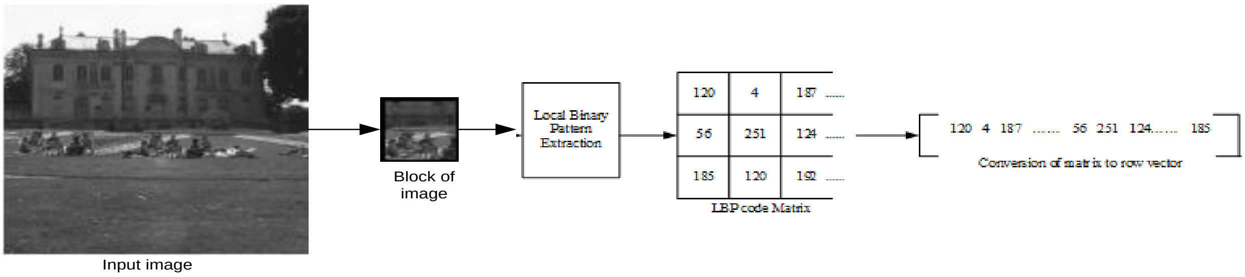


Fig 6: Feature extraction from image block

to different size of forgery performed over images. All images are of 256×256 dimension. We prepared our database on the basis of altered images with different forgery size. Forgery present in images is divided in three classifications which are small forgery size (30×60, 30×90 and 30×120 pixels), medium forgery size (90×60, 90×90 and 90×120 pixels) and large forgery size (120×120, 120×150 and 120×180 pixels).

5.1 Detection Accuracy and False Match Rate

Two parameters detection accuracy and false match rate are used for detecting the effectiveness and exactness of proposed method. Detection accuracy (DA) can be defined as ratio of number of forged pixels which are correctly matched to number of actually forged pixels as:

$$DA = \frac{No.\ of\ pixels\ correctly\ \ detected\ \ as\ copy-moved}{No.\ of\ pixels\ \ actu\,ally\ \ copy-moved} \times 100 \quad (12)$$

False Match Rate (FMR) shows the probability of original pixels of image to be identified as copy-move forged. Sections of images which does not consist any forgery but still they are represented as forged sections if FMR of copy-move forgery detection algorithm is high. FMR as shown in (13) of forgery detection algorithms should be low.

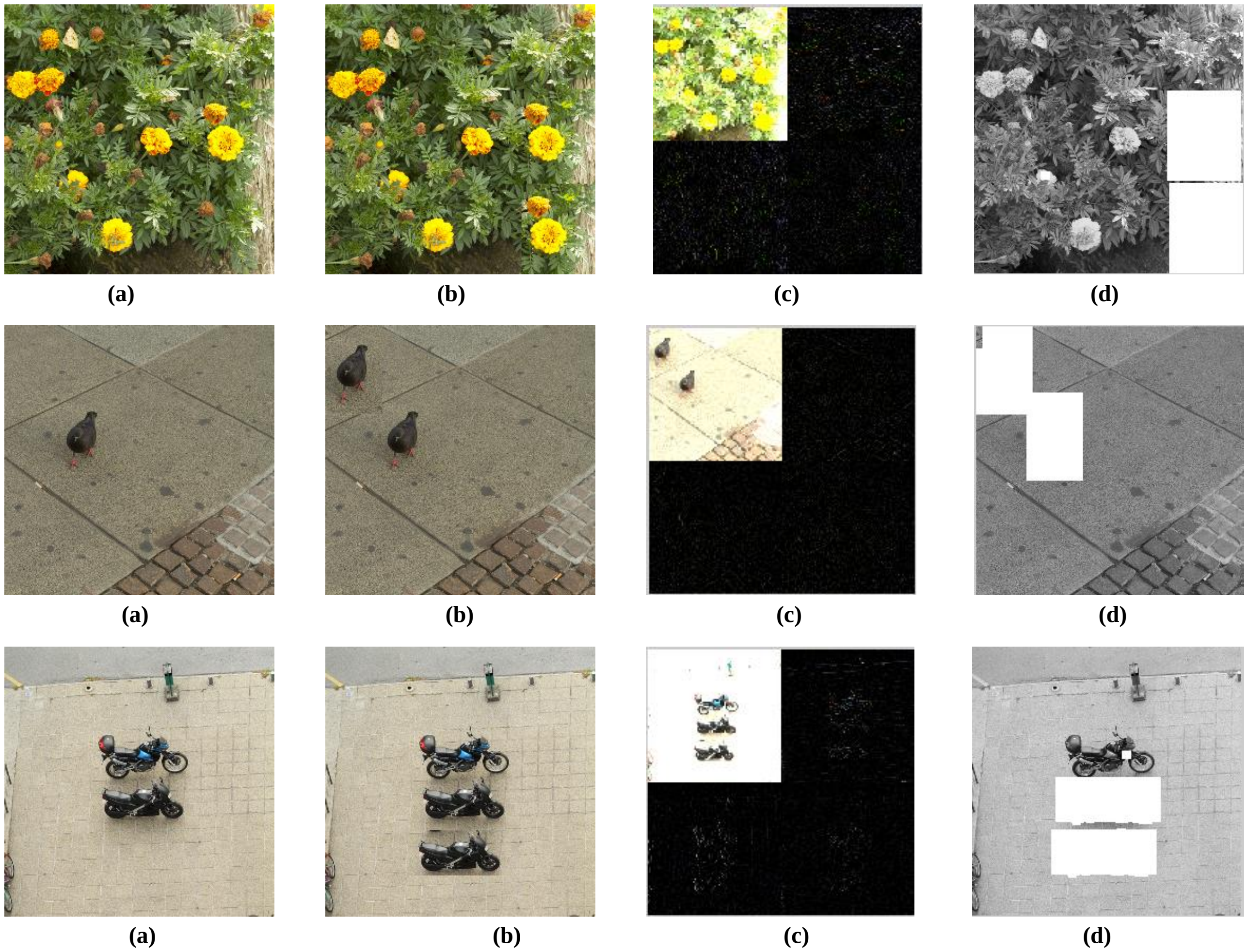
$$FMR = \frac{No.\ of\ pixels\ \ falsely\ \ detected\ \ as\ copy-moved}{No.\ of\ pixels\ \ actually\ \ copy-moved} \times 100 \quad (13)$$

Copy-move forgery detection image results are shown in Fig. 7. Four sub bands after applying DWT over forged image are shown. Copy and moved regions are shown.

Table 1, 2 and 3 represents detection accuracy and false match rate when small size of forgery present in image is analyzed. These results are obtained by dividing input image in different size of overlapping blocks. Table 4, 5 and 6 shows parameterized results for medium size of forgery present in the tampered image.

Table 1. Detection accuracy and False match rate for image forgery size 30×60 pixels

Block size (B*B Pixels)	**Detection Accuracy (%)**	**False Match Rate (%)**
7×7	98.2387	15.8398
11×11	98.1254	11.2352
15×15	97.8236	10.2154
19×19	96.2463	11.2110
23×23	96.1372	10.8073



(a) (b) (c) (d)

(a) (b) (c) (d)

(a) (b) (c) (d)

Fig. 7. (a) Input image (b) Forged image (c) First level image decomposition using DWT (d) Detected duplicate region

Table 2. Detection accuracy and False match rate for image forgery size 30×90 pixels

Block size (B*B Pixels)	Detection Accuracy (%)	False Match Rate (%)
7×7	98.3217	8.3164
11×11	98.1625	7.7089
15×15	97.0287	8.0342
19×19	97.0163	5.3281
23×23	96.9347	4.1651

Table 3. Detection accuracy and False match rate for image forgery size 30×120 pixels

Block size (B*B Pixels)	Detection Accuracy (%)	False Match Rate (%)
7×7	98.4136	5.8671
11×11	98.2087	5.3278
15×15	98.0169	3.0387
19×19	97.5324	3.0023
23×23	97.6153	3.8126

Table 4, 5 and 6 represents detection accuracy and false match rate when medium size of forgery present in image is analyzed.

Table 4. Detection accuracy and False match rate for image forgery size 90×60 pixels

Block size (B*B Pixels)	Detection Accuracy (%)	False Match Rate (%)
7×7	98.7324	5.7251
11×11	98.7103	4.7071
15×15	97.2654	3.9247
19×19	97.0368	3.8067
23×23	98.1053	2.0537

Table 5. Detection accuracy and False match rate for image forgery size 90×90 pixels

Block size (B*B Pixels)	Detection Accuracy (%)	False Match Rate (%)
7×7	98.8826	4.3570
11×11	98.8103	3.2270
15×15	97.9016	2.5560
19×19	97.8326	2.8722
23×23	98.1354	2.9976

Table 6. Detection accuracy and False match rate for image forgery size 90×120 pixels

Block size (B*B Pixels)	Detection Accuracy (%)	False Match Rate (%)
7×7	99.3267	3.7476
11×11	99.0312	2.1260
15×15	98.9025	2.0126
19×19	98.8872	1.0036
23×23	98.6927	3.6482

For images with medium size forgery false positives are less compared to images with small size of forgery. Similar trend for false match rate is observed for medium size of forgery. Table 7, 8 and 9 represents detection accuracy and false match rate when large size of forgery present in image is analyzed.

Table 7. Detection accuracy and False match rate for image forgery size 120×120 pixels

Block size (B*B Pixels)	Detection Accuracy (%)	False Match Rate (%)
7×7	99.2513	3.2187
11×11	99.0879	2.1069
15×15	98.8913	2.0073
19×19	98.9046	1.9231
23×23	98.5916	1.7062

Table 8. Detection accuracy and False match rate for image forgery size 120×150 pixels

Block size (B*B Pixels)	Detection Accuracy (%)	False Match Rate (%)
7×7	99.4285	3.0163
11×11	99.3168	2.0428
15×15	99.5637	1.4327
19×19	98.1258	2.4728
23×23	98.0326	3.1029

Table 9. Detection accuracy and False match rate for image forgery size 120×180 pixels

Block size (B*B Pixels)	Detection Accuracy (%)	False Match Rate (%)
7×7	99.7364	1.9126
11×11	99.2462	1.0007
15×15	98.8661	0.2134
19×19	98.7512	0.5116
23×23	98.9035	2.0064

Images with large size forgery shows highest accuracy and less number of false positives among all three cases of different forgery size image. Table 10 shows comparative results for copy-move forgery detection. Proposed method can accurately detect forged areas. Figure 12 and Figure 13 shows graphical results for detection accuracy and false match rate respectively for different size of square blocks (B×B) when small size forgery is present in altered image. Images with forgery size 30×120 pixels shows highest detection accuracy as well as False Match Rate is also less than other cases of small size forgery. Images with forgery size 30×90 pixels shows high detection accuracy but when block size increases from 11×11 pixels to 18×18 pixels it get reduced. Further, when block size increases detection accuracy increases and became higher than in 30×60 pixels forgery size images. For small block size False Match Rate is high for all three cases of forged images.

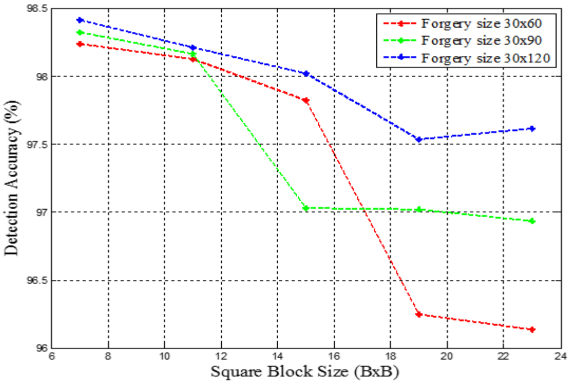


Fig 12: Detection accuracy for small size image forgery detection

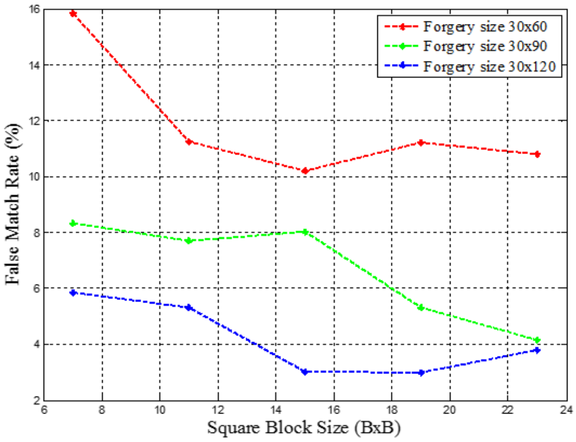


Fig 13: False match rate for small size image forgery detection

Figure 14 and Figure 15 shows graphical results of Detection accuracy and false match rate for medium size forgery detection respectively. For images with forgery size 90×120 pixels detection accuracy is highest. Detection accuracy decreases as forgery size increases. Forgery detection accuracy is smallest for forgery size 90×60 pixels. False match rate is highest when small size of blocks are used for dividing image.

Table 10. Comparison of existing methods and proposed method

Method	Detection Accuracy (%)	False Match Rate (%)
Fridrich et al. [10]	97.5647	7.2806
Zhang et al. [11]	98.1813	28.6482
Li et al. [17]	91.0263	9.6473
Muhammad et al. [28]	95.90	4.54
Mahdian & Saic [29]	81.18	10.03
DWT & LBP (Proposed)	98.3283	4.2522

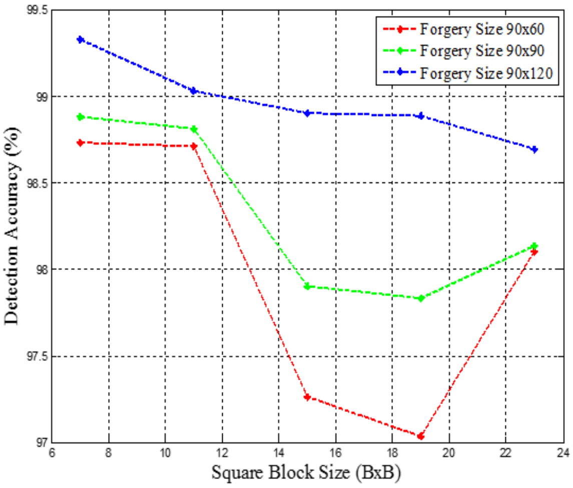


Fig 14: Detection accuracy for medium size image forgery detection

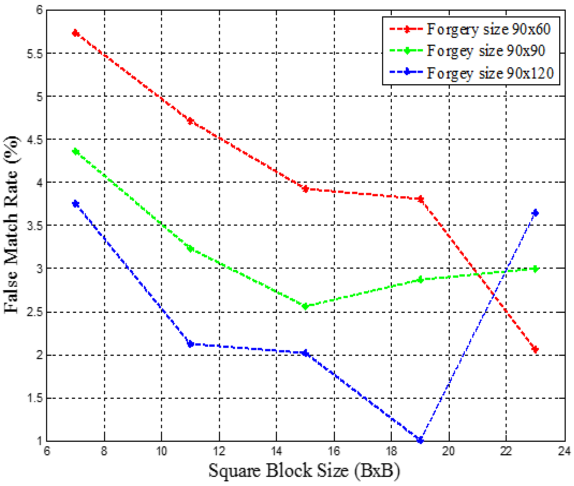


Fig 15: False match rate for medium size of image forgery detection

Figure 16 and Figure 17 shows graphical results for large size forgery detection using different size of square blocks (B×B). False match rate for forgery size 120×180 pixels is lowest among all three cases of large size forgery. Detection accuracy is highest when small size of blocks are used for image division. Results shows that for small and large size of blocks false match rate increases. For block size range from 11×11pixels to 19×19 pixels false match rate is low.

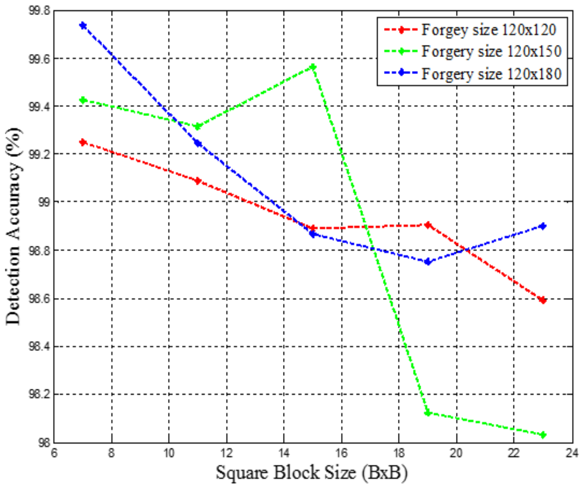


Fig 16: Detection accuracy for large size image forgery detection

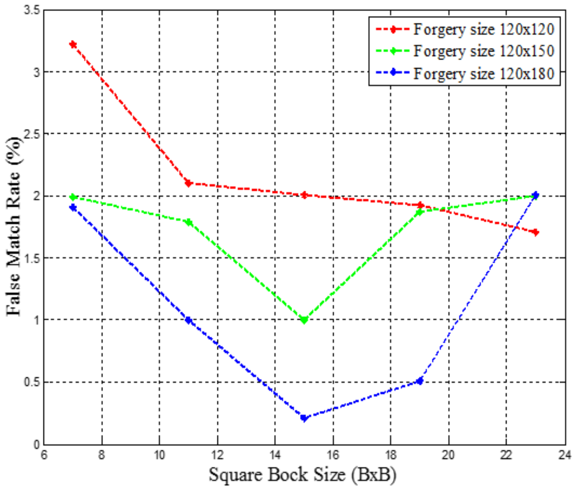


Fig 17: False Match Rate for large size image forgery detection

6. CONCLUSION & FUTURE WORK

In this paper, copy-move forgery detection algorithm based on DWT-LBP is discussed. In proposed algorithm, computational cost reduced due to use of DWT. Image analyzed for forgery detection reduced to $\frac{1^{th}}{4}$ of input image size. Texture operator LBP efficiently described the features of image blocks which were compared to find copy-move forged region. Shift vectors efficiently worked in reducing false matches. The performance of the proposed method has been observed in terms of detection accuracy and false match rate. It is found that detection accuracy of proposed algorithm is high when small block size is used for forgery detection. As block size increases so False matches get reduced. Proposed method can detect different size of forgery present in image with less complexity and small number of false matches which is very encouraging. Our method produces less number of features corresponding to each block of image which resulted in reduced size of matrix storing feature vector of blocks. Due to Lexicographical sorting, complexity of matching similar block pairs reduced. In future, development of image forgery detection methods will be widened to accurately detect forged regions of image with several post-processing operations applied (over copied segment before pasting it to original image) like rotation, scaling, blurring, noise addition, flipping and bending simultaneously with less complexity. Several methods based on PHT, (HU, BLUR) moments, Curvelets can be combined to deal with forged images with major alterations. Forgery detection methods are widely used in forensic investigations. Manipulating images for malefic purposes can be detected using image forgery detection methods. In future, other techniques can be detected to make forgery detection process less complex with high detection accuracy where multiple forged regions are present in an image.

7. REFERENCES

[1] J. Redi, W. Taktak and J. Dugelay, “Digital Image Forensics: A Booklet for Beginners,” Multimedia Tools and Applications, vol. 51, no. 1, pp. 133-162, January 2011.

[2] S. A. Alnesarawi and G. Sulong, “A Novel Approach for Detection of Copy Move Forgery using Completed Robust Local Binary Pattern,” Journal of Information Hiding and Multimedia Signal Processing, vol.6, no. 2, pp. 351-364, March 2015.

[3] S. Sadeghi, H.A. Jalab and S. Dadkhah, “Efficient Copy-Move Forgery Detection for Digital Images,” World Academy of Science, Engineering & Technology, vol. 71, pp. 543-546, November 2012.

[4] L. Jing and C. Shao, “Image Copy-Move Forgery Detecting Based on Local Invariant Feature,” Journal of Multimedia, vol. 7, no. 1, pp. 90-97, February 2012.

[5] V. Christlein, C. Riess and E. Angelopoulou, "A Study on Features for the Detection of Copy-Move Forgeries," Proc. Information Security Solution Europe (ISSE), vol. 2010, pp. 105-116, October 2010.

[6] J. A. Redi, W. Taktak, J. Dugelay, “Image splicing detection using 2-d phase congruency and statistical moments of characteristic function,” Society of photo optical instrumentation engineers (SPIE) conference, 2007.

[7] V. Savchenko, W. Kojekine, N. Unno, “A practical image retouching method,” Proceedings of First International Symposium on Cyber Worlds, pp. 480-487, 2002.

[8] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker "Digital Watermarking and Steganography, Morgan Kaufmann Publishers, 2008.

[9] L. Chun-Shien, H. Liao, "Structural digital signature for image authentication: an incidental distortionresistant scheme, IEEE Transactions on Multimedia, vol.5, no.2, pp. 161-173, 2003.

[10] A. J. Fridrich, B. D. Soukal and A. J. Lukas, ”Detection of Copy-Move Forgery in Digital Images,” in Proceedings of Digital Forensic Research Workshop, 2003.

[11] J. Zhang, Z. Feng and Y. Su, “A New Approach for Detecting Copy-Move Forgery in Digital Images,” Paper presented at the 11th IEEE Singapore International Conference on Communication Systems (ICCS), 2008.

[12] S. Bayram, H. T. Sencar and N. Memon, “An Efficient and Robust Method for Detecting Copy-Move Forgery,” Paper presented at the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2009.

[13] L. Li, S. Li and J. Wang, "Copy-Move Forgery Detection based on PHT," Paper presented at the World Congress on Information and Communication Technologies (WICT), 2012.

[14] M. Ghorbani, M. Firouzmand and A. Faraahi, "DWT-DCT (QCD) based Copy-Move Image Forgery Detection," Paper presented at the 18th International Conference on Systems, Signals and Image Processing (IWSSIP), June 2011.

[15] L. Li, S. Li, H. Zhu, S. C. Chu, J. F. Roddic and J. S. Pan, "An Efficient Scheme for Detecting Copy Move Forged Images by Local Binary Patterns," Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, pp. 46-56, January 2013.

[16] V. Kumar, A. S. Rao, YK S. Krishna, "Dual Transition Uniform LBP Matrix for Efficient Image Retrieval," International Journal of Image, Graphics and Signal Processing, vol. 7, no. 8, pp. 50-57, July 2015.

[17] G. Li, Q. Wu, D. Tu and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," IEEE International Conference on Multimedia and Expo, pp. 1750–1753, July 2007.

[18] B. Mahdian and S. Saic, "Detection of Copy–Move Forgery using a Method based on Blur Moment Invariants," Forensic Science International, vol. 171, no. 2, pp.180-189, September2 007.

[19] J. W. Wang, G. J. Liu, Z. Zhang, Y. Dai and Z. Wang, "Fast and Robust Forensics for Image Region Duplication Forgery," Acta Automatica Sinica, vol. 35, no. 12, pp. 1488-1495, 2009.

[20] Z. Mohamadian and A. A. Pouyan, "Detection of Duplication Forgery in Digital Images in Uniform and Non-uniform Regions," Paper presented at the UKSim, 2013.

[21] M. F. Hashmi1, A. Hambarde, V. Anand and A. Keskar, "Passive Detection of Copy-Move Forgery using Wavelet Transforms and SIFT Features," Journal of Information Assurance and Security, vol. 9, pp. 197-204, 2014.

[22] S. Khan and A. Kulkarni, "Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform," International Journal of Computer Applications, vol. 6, no. 7, pp. 31-36, 2010.

[23] D. Mustapha, R. Mohammed and T. Khadidja, "Multi-metric Based Face Identification with Multi Configuration LBP Descriptor," International Journal of Image, Graphics and Signal processing, vol. 4, no. 1, pp. 57-63, February 2012.

[24] G. J. Liu, J. W. Wang, S. G. Lian and Z. Q. Wang, "A Passive Image Authentication Scheme for Detecting Region-Duplication Forgery with Rotation," Journal of Network and Computer Applications, vol. 34, no. 5, pp.1557-1565, 2011.

[25] http://decsai.ugr.es/cvg/dbimagenes/c256.php.

[26] D. Tralic, I. Zupancic, S. Grgic and M. Grgic, "CoMoFoD- New database for Copy-Move Forgery Detection," in Proc. 55th International Symposium ELMAR, pp. 49-54, September 2013.

[27] http://sipi.usc.edu/database/database.php.

[28] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Digital Investigation, vol. 9, no. 1, pp. 49–57, 2012.

[29] B. Mahdian, S. Saic, "Using noise inconsistencies for blind image forensics", Image and Vision Computing, vol.27, no.10, pp. 1497–1503, 2009.