International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-5, Issue-5)

Research Article | **May 2016**

A Hybrid Method for Copy-Move Forgery Detection Based on Wavelet Transform and Texture Analysis

Anuja Dixit, R. K. Gupta
Madhav Institute of Technology & Science, Gwalior,
Madhya Pradesh, India

Abstract—

Nowadays, various forgery detection techniques are available. Copy-move image forgery is one of the most common image forgery technique. In this forgery, a segment of the image is copied and it is pasted at different location on the same image. Several operations are applied over copied region to make it harder to detect forgery in images. In proposed method block based technique is used for forgery detection. In our approach, first of all dimension of the input image is reduced using Discrete Wavelet Transform (DWT). Approximation band (LL) obtained after decomposition contains low frequency components which is used for further analysis. LL sub band is divided in fixed dimension of blocks. For each block of image features are extracted using Local Binary Pattern (LBP). Feature corresponding to each block are in form of matrix. They are converted in row vectors so that they could be compared easily. These feature vectors corresponding to each block are stored in a matrix. As in copy-move forgery we focus on compatible regions of image so lexicographical sorting is performed so that similar feature vectors could be in neighbourhood of each other. LBP is a texture operator which analyses texture of image to detect similar regions of image. Further, to reduce probability of false matches shift vectors are calculated. Group of block pairs with same shifting are detected using user defined threshold value for occurrence of similar shifting. As post processing step, block pairs with similar shifting are labelled with different colour to show forged blocks of the image.

Keywords— Local Binary Pattern, Discrete Wavelet Transform, Lexicographical sorting, Feature vector, Shift vector, Texture operator, Copy-move image forgery.

I. INTRODUCTION

Images are easily understood in comparison to thousands of words. Images are one of the most effective way of showing any incident. Images are used as evidence in courts of law. Images are used in Televisions, magazines, websites, advertisements and medical imaging. Due to development of technology various image editing software like adobe Photoshop, GIMP and CorelDraw are available. Peoples having very little information about these tools can manipulate images very easily. These tools are responsible for degradation in trust on images. Images are altered for various purposes. Images can be manipulated for enhancing original image to make it more attractive known as innocent editing. Malicious editing can also be done over an image for defaming a person, fun-making, rivalry or harassment purposes. Images are losing their credibility day by day. They are no longer trusted. Image forgery means changing original information of the image by adding, deleting or hiding objects of image. Image forgery techniques are widely used for black mailing peoples. Image forgery techniques can be classified in five categories: Image splicing, Image retouching, Image enhancing, Image morphing and copy-move.

In image splicing, segments of different images are used for making a forged image. As segments of forged image are taken from different images so such type of forgery are detected exploiting incompatibilities present in image.

In Image retouching, features of images are enhanced to make it more attractive. Operations like changing background colour of the image, filling of colours or edge sharpening are performed in image retouching forgery. Sometimes, it is also used for degrading the quality of the image.

Image enhancing is about providing a better and clearer view of an image. Image enhancement always results in better representation of an image.

Image morphing is about creating new object using two or more similar kind of objects taken from different images.

Copy-move is well known image forgery technique. In this forgery technique, a portion is copied from the image and after applying post-processing operations it is pasted on the same image at different location. The primary motive of such type of forgery is to increase the number of similar objects present in the information or to hide information shown by the image by pasting copied segment over it. As the copied segment is from the same image so for detection of copy-move forgery, we search for compatibilities present in segments of the image. Image forgery detection techniques are classified in two main categories: Active approach and Passive approach.

A. Active Approach

In active approach, Digital signatures and Digital watermarking schemes are used for detecting forgery present in image. Active approaches requires information about the original image for comparison. Various images don't have signatures or watermark information attached to them. Active approaches requires expensive equipment.

B. Passive approach

These techniques don't require any prior information about the image. Many methods are proposed by researches to detect image forgery based on the passive approaches. Passive image forgery detection techniques are classified in six categories: Pixel based, Geometry based, Source camera identification based, camera based, Physics based and Format based. In pixel based techniques, changes at pixel level are analysed for forgery detection. These techniques are used often for forgery detection. Pixel related characteristics are analysed for detecting forgery. In Geometric based techniques, projective geometric principles are used for forgery detection. In source camera identification technique, image forgery is detected utilizing the characteristics of source camera used for capturing image. In camera based techniques, steps of processing an image are exploited for forgery detection. Physics based techniques focus on finding physics based incompatibilities present in image like difference in lighting or brightness. In format-based techniques, forgery is detected using format of images to which they belong like JPG, PNG, TIFF, BMP etc. This paper is organized as follows. Section 2 describes the related work done in image forgery detection field. Section 3, explains conceptual framework of DWT and LBP. In section 4, proposed methodology is discussed. Section 5 shows results of copy-move forgery detection. Finally, this paper is concluded in section 5.

II. RELATED WORK

Popescu and Farid [1] suggested a method based on Principal Component Analysis (PCA). PCA is dimensionality reduction based method. In their method image id divided in fixed dimension of blocks. Further, using PCA feature vector corresponding to each block are extracted and compared to find copy-move image forgery. Ting and Rang ding [2] studied a method based on Singular Value Decomposition (SVD) for copy-move image forgery detection. In their method image is divided in fixed dimension of blocks. Using SVD feature matrix is decomposed in tree matrices. Two orthogonal matrix and one diagonal matrix having singular value s its diagonal components are achieved. Singular values corresponding to each block are compared to find forgery present in image. Basher et al. [3] proposed a method based on DWT- KPCA (Kernel PCA). In their method at first DWT is applied over input image. LL sub band is divided in fixed dimension of blocks. Features are extracted and KPCA is used for dimensionality reduction of feature vector storing features corresponding to each block of image. Zimba et al. [4] proposed a method based on DWT-PCA (EVD). In this method Eigen values are used as feature vectors and compared to detect copy-move image forgery present in image. Zhang et al. [5] studied a method based on DWT for copy-move image forgery detection. In this method input image is divided in four sub bands and Low frequency sub band LL is divided in blocks and features are extracted and stored in a matrix corresponding to each block. Feature vectors are compared to detect similarity present in image. Li et al. [6] proposed a new method for forgery detection based on LBP. Input image is divided in circular blocks. Using LBP feature vectors corresponding to each circular block is extracted. Feature vectors are stored in a matrix and further by using lexicographical sorting similar feature vectors are detected. Muhammad et al. [7] proposed a method for copy-move image forgery detection based on Dyadic Wavelet Transform (DyWT). In their method DYWT is applied over the image. Four sub bands are obtained. LL and HH sub bands are divided in fixed dimension of blocks. Euclidean distance between pair of blocks are calculated and stored in different lists for both LL (List1) and HH (List2) subbands.List1 is sorted in ascending order and list2 is sorted in descending order. Further both lists are compared to detect similar pair of blocks.

III. DISCRETE WAVELET TRANSFORM & LOCAL BINARY PATTERN

Discrete wavelet transform [8] is used for obtaining four sub bands of an image as shown in Fig. 1. Four sub bands are known as LL, LH, HL and HH. LL sub band also known as approximation sub band. LL sub band contains low frequency component of image. LH, HL and HH sub band shows vertical, horizontal and diagonal component of the image. HH sub bands consists detail coefficient [9] of the image. LL sub band consists coarse level coefficient.

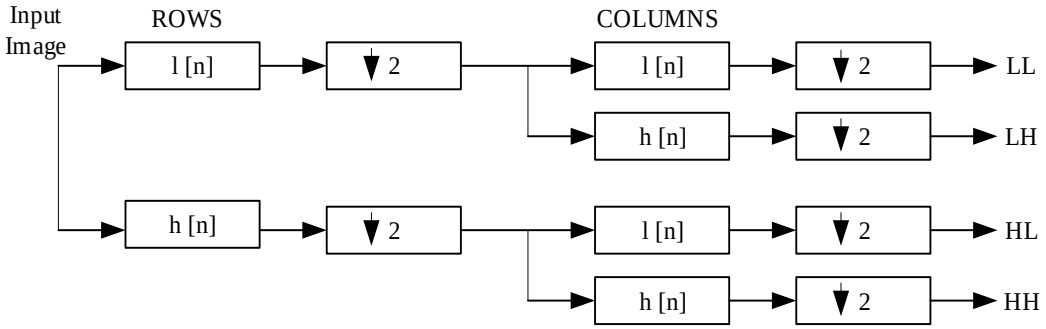


Fig. 1. Two-Dimensional decomposition of image using DWT

If input image goes through transformation using DWT then four sub bands of that image are obtained. If dimension of input image is $M \times N$. Decomposition using DWT results in four sub images each of dimension $\frac{M}{2} \times \frac{N}{2}$ as shown in Fig.2. The sub bands considered for further analysis is $\frac{1}{4}^{th}$ of the input image size which results in reducing computational cost for further operations.

Fig.2. Four sub images of an image obtained using DWT

Local Binary Pattern is a texture [10] operator. It is useful in extracting gray level values. For calculating binary patterns a block of image is considered for analysis. Center gray level value of pixel considered as threshold as shown in Fig. 3. Neighbours hold value '1' if gray level values of neighbour pixels are greater than threshold value. If gray level values of neighbour pixels are less than center value then neighbour location of binary pattern holds value '0'. Further, equivalent decimal value is calculated for binary pattern. Calculated decimal value is for centre pixel. Same procedure is applied for all values of a block to calculate local binary pattern.

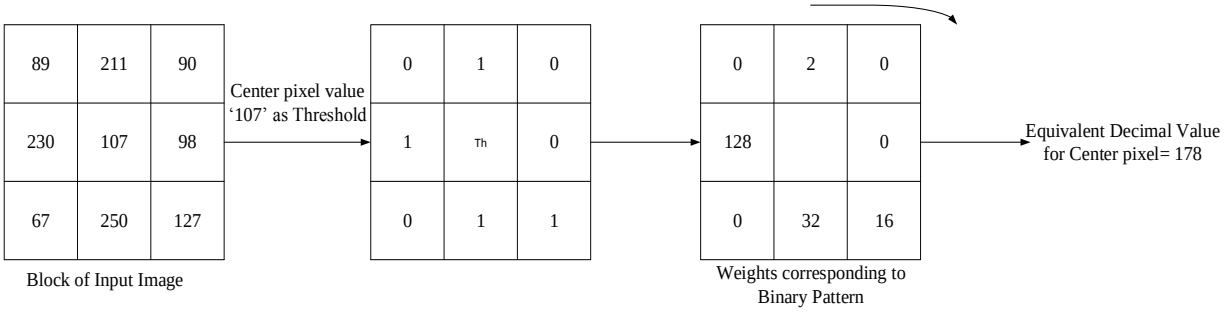


Fig. 3. Basic working of LBP

Even slight variation in noise level of the image can change the local binary pattern of the image blocks as shown in Fig. 4.

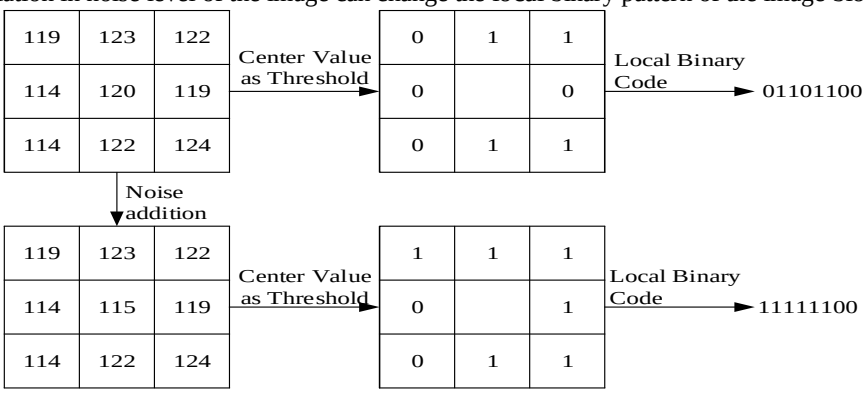


Fig. 4. Difference in Local Binary Pattern after noise addition

Local Binary Patterns are sensitive towards post processing operations done over the image. These patterns get changed due to rotation as shown in Fig. 5.

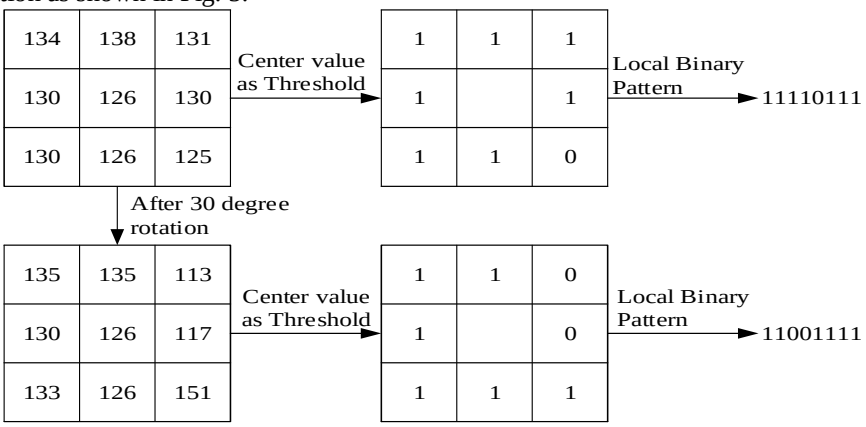


Fig. 5. Difference in Local Binary Pattern after 30 degree rotation

For forgery detection texture analysis is very effective. Texture of image does not get affected when section of image is copied and it is pasted to another position on the same image.

IV. PROPOSED METHODOLOGY

Our method is based on hybrid approach by using DWT for image decomposition and LBP for feature extraction. Copy-move forgery detection technique is based on finding compatibilities present in different portions of the image. For detecting forgery present in image well defined steps are followed as shown in Fig. 6.

Following steps are followed for image forgery detection:

- Input image.
- DWT is used for decomposing input image. When DWT is applied over image then it get divided in four sub images. These sub images are often known as LL, HL, LH and HH. LL sub bands also known as approximation sub band and contains coarse level coefficients. HL and LH contains horizontal and vertical component of the image respectively. HH sub image consists diagonal component of the image. The coefficients of HH sub band also known as detail coefficients. Due to decomposition the size of image get reduced to $\frac{1}{4}^{th}$ of its original size. If original image size is $M \times N$ then after decomposition each sub band is of dimension $\frac{M \times N}{4}$.
- Approximation sub band is taken for further analysis. For detecting forgery, approximation band divided in fixed dimension $B \times B$ overlapping blocks. For image size $M \times N$ total number of blocks will be $(M - B + 1) \times (N - B + 1)$. We considering only approximation band so, total blocks taken for analysis are $(\frac{M}{2} - B + 1)(\frac{N}{2} - B + 1)$.
- For each block features are extracted using LBP. Extracted values corresponding to each block will be in matrix form. As forgery is detected by comparing feature vectors so it is computationally efficient to convert feature matrix in row vector. For each block a feature vector is calculated. These feature vectors are stored in a matrix $'A'$. Matrix has rows equal to the number of blocks. Number of columns of the matrix will be equal to length of feature vector.
- For detecting forgery similar blocks has to be detected. Similar will have similar feature vectors. If feature vectors are compared to each other computational cost will be very high. So, Lexicographical sorting is performed. Due to sorting, same feature vectors will be in proximity to each other.
- Matching is performed between feature vectors. To reduce the probability of false matches shift vectors are calculated. Top-left corner of each block is considered as block location. Shifting between block pairs is calculated by subtracting respective x and y coordinates of block pair as shown in Eq. (1).

$$Sh_i = (x_{1i} - x_{2i}, y_{1i} - y_{2i}) \quad (1)$$

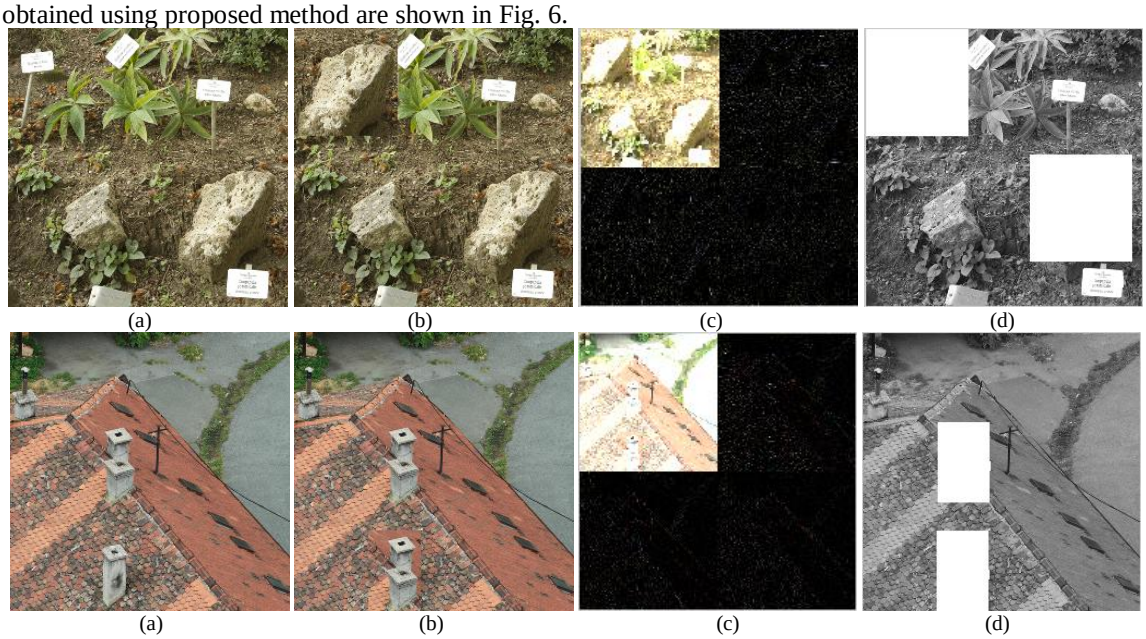
- Counter $'C'$ is initialized to zero. Whenever similar shifting between block pairs is achieved counter value is increased by one. Based on threshold value the pair of blocks are decided as forged as shown in Eq. (2).

$$C_{Sh_i} > Th \quad (2)$$

- Forged block pairs are labeled with different color to show forgery present in image.

V. EXPERIMENTAL RESULTS

For experiment Machine is used with Intel core i3 2.40GHz processor. 32 bit Operating system and 4GB RAM. For image forgery detection MATLAB 2013a is used. Three different datasets COMoFoD [11], CVG UGR [12] and USC SIPI [13] are used for verifying detection ability of proposed method. 50 distinct images are considered and manually forged to check the forgery detection results. Dimension of all images are 256×256. Copy-move forgery detection results obtained using proposed method are shown in Fig. 6.



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

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

Fig. 6. (a) Original Image (b) Forged image (Input image) (c) Image decomposition in 4 subbands using DWT (d) Forgery detection result

Results shows that our method is efficient in forgery detection. False matches are very less and the forged regions are detected accurarely. Proposed method is able to show both copied and the pasted regions in forged image.

VI. CONCLUSION

Due to rising development of image processing tools image forgery can be performed very easily. Copy-move forgery is the sizzling research topic among researchers. Our method reduces the computational complexity because the input image first reduced to $\frac{1}{4}^{th}$ of its original size. LBP is profient in extracting texture feature from the image so forgey dtection results are accurate. In our mehtod, shift vectors are calculated and used for reducing labeling of false matched block pairs due to which false matches are very less. Length of feature vector is also less so the dimensionality of matrix storing features corresponding to each block are also less. To reduce the complexity of matching, feature vectors are sorted lexicographically. In future, such methods can be developed which are robust to post processing opeartions [14] applied to images with less complexity. False match reduction during forgery detection is also a major issue when postprocessing operations are applied over copied segment.

REFERENCES

[1] C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Tech. Rep. TR2004-515, Department of Computer Science, Dartmouth College, Hanover, United States, 2004.

[2] Z. Ting and W. Rang-ding, "Copy-move forgery detection based on SVD in digital image," *in International Conference on image and signal processing*, 2009.

[3] M. Bashar, K. Noda, N. Ohnishi and K. Mori, "Exploring duplicated regions in natural images," *IEEE Transactions on Image Processing*, 2010.

[4] M. Zimba and S. Xingming, "DWT-PCA (EVD) Based Copy-move Image Forgery Detection", *International Journal of Digital Content Technology and its Applications*, Vol. 5, 2011.

[5] J. Zhang, Z. Feng and Y. Su, "A new approach for detecting copy-move forgery in digital images," *11th IEEE Singapore International Conference on the Communication Systems, ICCS*, 2008.

[6] L. Li, S. Li, H. Zhu, S. C. Chu, J. F. Roddick 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, pp.46-56, 2013.

[7] G. Muhammad, M. Hussain, K. Khawaji and G. Bebis, "Blind copy move image forgery detection using dyadic undecimated wavelet transform," *Digital Signal Processing DSP*, 2011.

[8] 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.

[9] 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.

[10] S. Bravo-Solorio and A. K. Nandi, "Automated detection and localization of duplicated regions affected by reflection, rotation and scaling in image forensics," *in Signal Processing*, Vol. 91, pp.1759-1770, 2011.

[11] 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.

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

[13] Available: http://sipi.usc.edu/database/database.php.

[14] 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.

