Detection of Digital Image Forgery using FFT

[1]*R. Alekya*
Assistant Professor
Department of Electronics and communication Engineering
St. Martin's Engineering College, Dhulapally
Secunderabad-500100

ABSTRACT

Multimedia security is one of the key challenges in today's world, as dependency on multimedia information is increasing day by day. Easily available image editing software have enabled every common user of a smart phone and computer, to hack into the information of the images and video and alter it to some extent. To authenticate the genuineness of images, detection of image tempering is need of the time. Various techniques have been proposed to use image features for detection of image forgery. The techniques of forgery detection work in two domains of image forgery; copy-move forgery detection (CMFD) and image splicing detection (ISD). This paper presents a comprehensive comparative analysis for the use of local texture descriptors i.e. local binary pattern (LBP) and local ternary pattern (LTP) for forgery detection in an image. The paper also presents a technique to integrate fast fourier transform (FFT) with local texture descriptors for image forgery detection using existing block-based methodology. Performance of the technique(s) and descriptor(s) is tested for benchmarked dataset CASIA v1.0. Results are evaluated by using standard detection metrics detection accuracy and recall. The paper also suggests a relatively better texture descriptor

Keywords: CMFD, LBP, LTP, FFT

INTRODUCTION

Multimedia security is one of the key challenges in today's world, as dependency on multimedia information is increasing day by day. Easily available image editing software have enabled every common user of a smart phone and computer, to hack into the information of the images and video and alter it to some extent. To authenticate the genuineness of images, detection of image tempering is need of the time. Various techniques have been proposed to use image features for detection of image forgery. The techniques of forgery detection work in two domains of image forgery,copy-move forgery detection (CMFD) and image splicing detection (ISD). This project presents a comprehensive comparative analysis for the use of local texture descriptors i.e. local binary pattern (LBP) and local ternary pattern (LTP) for forgery detection in an image. The project also presents a technique to integrate fast fourier transform (FFT) with local texture descriptors for image forgery detection using existing block-based methodology. So, the main objective of the project is to detect the forged/tempered part of the image. The image that has to be tested for genuiness is given as the input image. The input image can be either RGB or grey image. The given input image undergoes preprocessing part which involves conversion of RGB image into chrominance part of image and then block

processing is applied to divide the image into 3*3 or 4* 4 overlapping blocks. Then feature extraction of image is done by applying DWT and DCT algorithm and then the output is given to the image classifier SVM(support vector machine).The mentioned process is shown in the below figure.

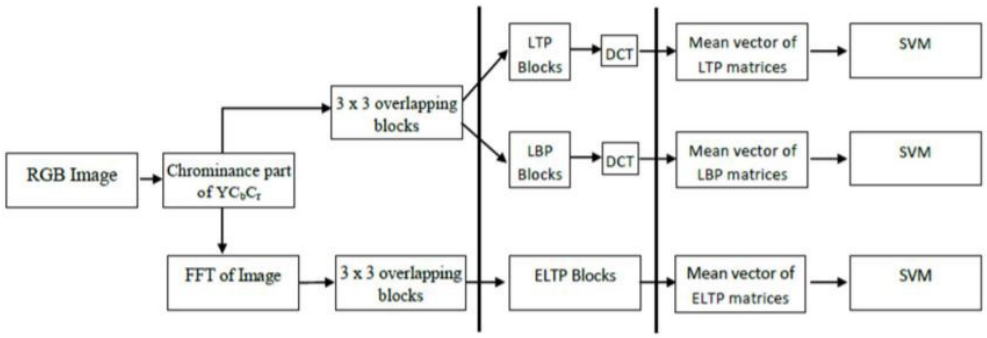

Fig 1 Overview of the Design

BLOCK DIAGRAM

The basic procedure that every image should go through during image forgery detection is shown the following block diagram. The first step includes preprocessing which is used for image enhancement and followed by block process to divide the image into 3*3 or 4*4 overlapping blocks and then DWT and DCT algorithm is applied followed by feature extraction and feature matching is done and post processing is done then output image is given to image classifier to detect the tampered part and the displayed as final output.

EXPERIMENTAL RESULTS

STEP -1: First an image that to be tested will be given as input.

Figure 3: Input Image

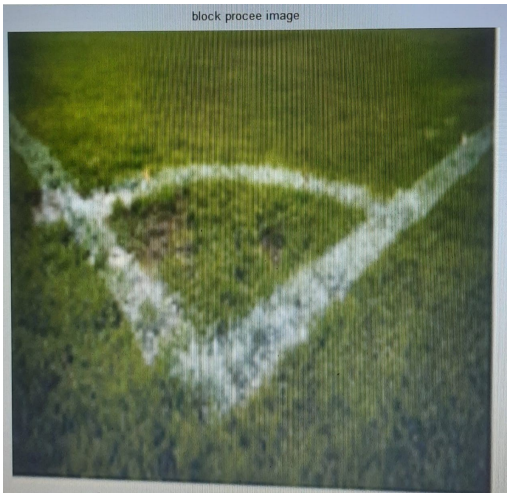

Figure 3: Block process

Step-2: As a step of pre-processing of an image block process is done.

Step-3: As a step 3 DWT is applied to the block processing image.It gives four types of image LL,LH,HL,HH based contrast and with respective coefficients

Figure 4: LL Image

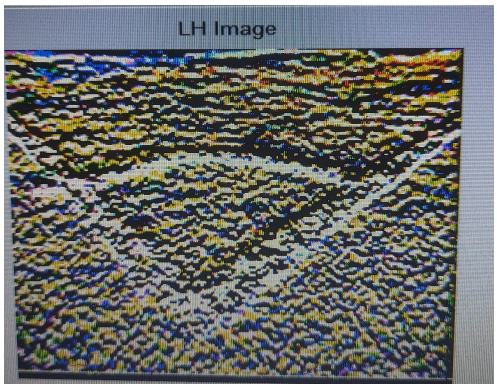

Figure 5: LH Image

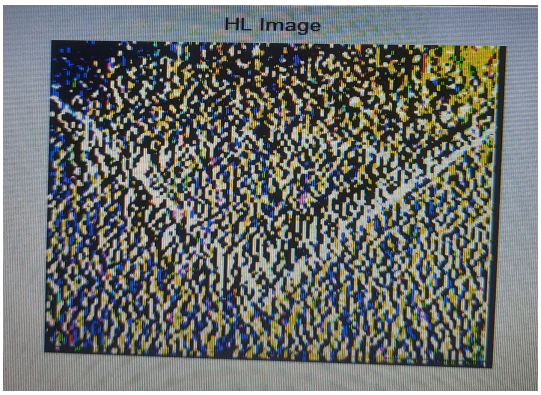

Figure 6: HL Image

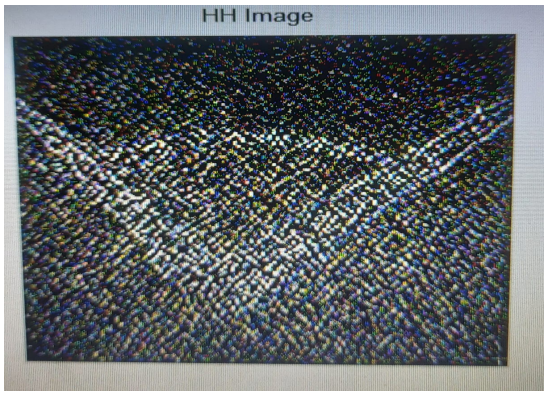

Figure 7: HH Image

Step4 : By Performing feature matching and sorting copy and move part is detected**.**

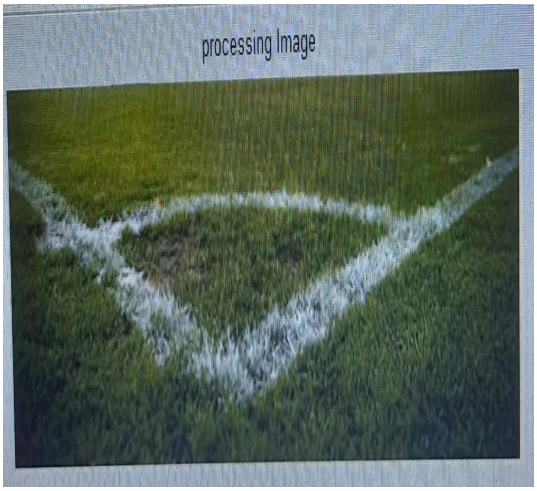

Figure 8:Post Processing

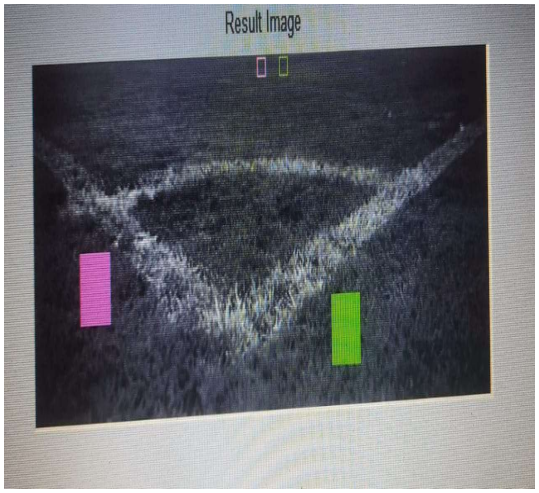

Figure 9: Final output

CONCLUSION

The proposed approach can be used to detect the digital image forgery by using FFT and Local features successfully. It can be observed that LBP and ELTP perform as better features to classify the image as forged or authentic. The presented approaches involve complex transformations like DCT and FFT which increases the complexity of the methodology. The accuracy of detecting the copied parts of the image is increased when compared to existing techniques. The time taken for detection of forgery is reduced. The proposed system had successfully overcome the difficulties in the existing techniques. The proposed forgery detection had used block-based division techniques and feature extraction and SVM for image classifiers for accuracy of detection.

FUTURE ENHANCEMENT

The proposed method consists of FFT and DCT as main algorithm which increases complexity of the system. In future development complexity can be reduced. In future based on key point division the forgery detection technique can be developed. Further accuracy and reduction of time can be achieved in future practices.

REFERENCES

[1] Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using dct and local binary pattern," Signal, Image and Video Processing, vol. 11, no. 1, pp. 81–88, 2017.

[2] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," Digital investigation, vol. 10, no. 3, pp. 226–245, 2013.

[3] Cavalin and L. S. Oliveira, "A review of texture classification methods and databases," in Graphics, Patterns and Images Tutorials (SIBGRAPIT), 2017 30th SIBGRAPI Conference on. IEEE, 2017, pp. 1– 8.

[4] A. Doegar, M. Dutta, and G. Kumar, "A review of passive image cloning detection approaches," in Proceedings of 2nd International Conference on Communication, Computing and Networking. Springer, 2019, pp. 469– 478.

[5] J. Dong, W. Wang, and T. Tan, "Casia image tampering detection evaluation database," in Signal and Information Processing (ChinaSIP), 2013 IEEE China Summit & International Conference on. IEEE, 2013, pp. 422–426.

[6] E.-S. M. El-Alfy and M. A. Qureshi, "Combining spatial and dct based markov features for enhanced blind detection of image splicing," Pattern Analysis and Applications, vol. 18, no. 3, pp. 713–723, 2015.

[7] H. Farid, "Digital doctoring: how to tell the real from the fake," pp. 162– 166, 2006.

[8] F. Hakimi, M. Hariri, and I. Azad, "Image-Splicing Forgery Detection Based on Improved LBP and K-Nearest Neighbors Algorithm," no. September 2015, 2015.

[9] F. Hakimi, M. Hariri, and F. GharehBaghi, "Image splicing forgery detection using local binary pattern and discrete wavelet transform," in Knowledge-Based Engineering and Innovation (KBEI), 2015 2nd International Conference on. IEEE, 2015, pp. 1074–1077.

[10] J. G. Han, T. H. Park, Y. H. Moon, and I. K. Eom, "Quantizationbased markov feature extraction method for image splicing detection," Machine Vision and Applications, vol. 29, no. 3, pp. 543–552, 2018.