A Review Paper on Image Forgery Localization by Integrating Tampering Possibility Maps

[1]Ms. Soniya Chopde, [2] Dr. P. R. Rothe, [3]Mr.Devendra O. Rapelli
[1] M.Tech Student , [2] Associate Professor, [3]AssitantProfessor,
[1]Electronics Department PCE, Nagpur, India

Abstract— Recently, many efforts have been made in passive image forensics. Although it is able to detect tampered images at high accuracies based on some carefully designed mechanisms, localization of the tampered region in a fake image still presents many challenges, especially when the type of tampering operation is unknown. It is necessary to integrate different forensic approaches to obtain better localization performances. However, some important issues have not been comprehensively studied. We propose a framework to improve the performance of forgery localization using a simple yet very effective strategy to integrate the tampering possibility maps to obtain final localization results.

Keywords—SVM (Support vector machine), ELM (Extreme learning machine), SURF(Speed up robust feature)

I. INTRODUCTION

Digital images can easily be modified with the help of powerful image editing software, without leaving any perceptible artifacts. Image forensics has attracted considerable attention during the past decade. Generally, there are two main problems in image forensics, one is forgery detection and the other one is forgery localization. Forgery detection aims to discriminate whether a given image is genuine or fake. For example, by exploiting camera related signals such as sensor pattern noise (SPN) and color filter array (CFA) it is possible to reveal tampered images via camera source identification. This is done by dividing the image into small blocks, and then each block goes through Feature Extraction and Feature Analysis. Then, the blocks are marked as genuine or forged, and output image is the forged part.

Forgery in an image can be done in a number of ways. There can be duplication within the image, addition or removal of a desired part, or addition of a foreign image into the concerned image. Previous approaches, such as copy-move detection based approach, or near-duplicate detection based approach etc could identify only a particular type of forgery. A particular approach would have been ineffective in detecting a different type of forgery. All the methods have their advantages and disadvantages.

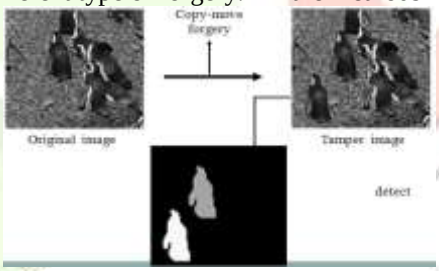


Fig. 1.1 Copy-move Forgery

For the image forgery detection, first, the concerned image is taken. The image is then divided into smaller parts, called blocks. These blocks, one by one, are then passed through thorough feature extraction. For feature extraction, we are considering two types of features, morphological features and the SURF features. The image is then subjected to feature analysis. Initially, a Support Vector Machine, Also called as SVM is used. Later, to improve efficiency and reduce time required for forgery detection, an Extended Learning Machine or an ELM is used, as efficiency of an ELM(75%) is greater than the SVM(60%).

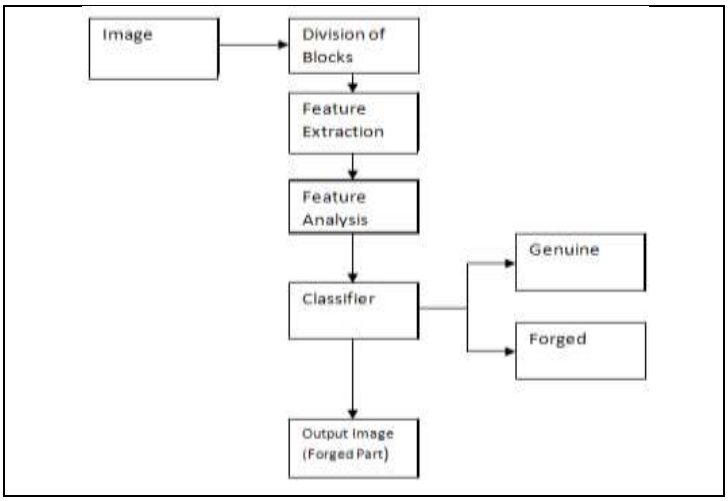


Fig. 1.2 Methodology

I. Dividing Image into Blocks

Any image that is under observation has a size big enough to be feature extracted. Hence, the image is divided into smaller, overlapping blocks. Then similarities between these blocks are compared.

Consider any given image of size m*n, divided into smaller square blocks of size b. These blocks are overlapping in nature. The blocks are divided such that the image becomes (m-b+1) (n-b+1)=N. These blocks are then applied DCT Transform, giving a DCT matrix and then the obtained values are compared.

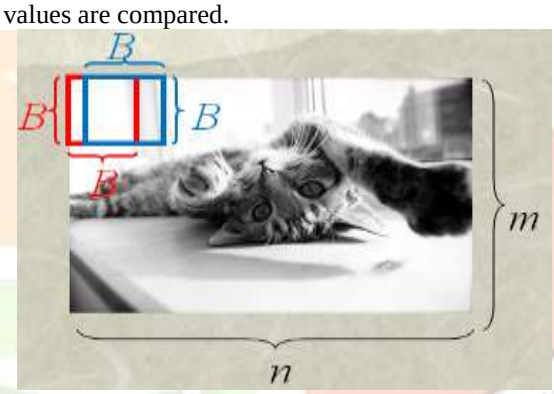


Fig 1.3 Division of Image into Blocks

II. Feature Extraction

This step deals with the extraction of features of the image that is already segmented into blocks. The blocks are smaller in size, and hence, are easier to extract features from. Here, two types of features will be extracted and studied. Morphology is a branch of biology the deals with the form and structure of the living animals and plants. Morphological image processing is used to extractor representation and description of region shape, such as boundaries, skeletons, etc. As features are extracted from multiple pixels, they can still be recovered even if some pixels are distorted.

The SURF or the speed-up robust features hares many conceptual similarities with the most widely used feature detector in the computer vision community, called SIFT, or the Scale Invariant Feature Transform. That SURF outperforms SIFT, has been experimentally demonstrated.

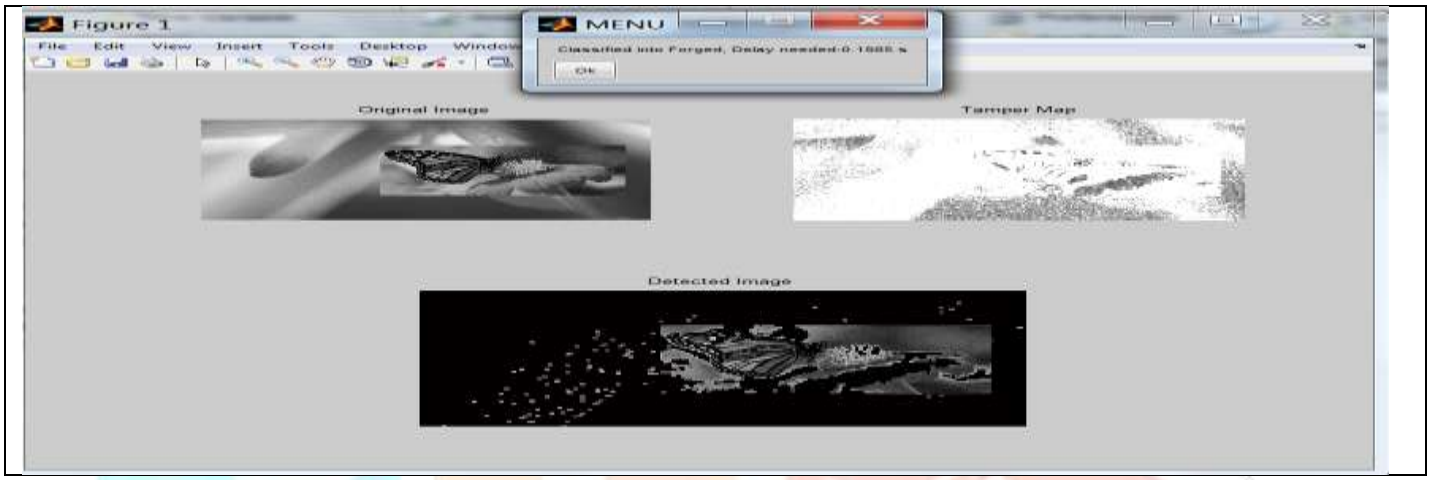
III. Feature Analysis

The main advantage of the SVM is its flexibility in choosing a similarity function. It gives sparse solution when dealing with large data. SVM has been successfully used in a large number of real life problem solving, for example image classification, bioinformatics and hand written character recognition. The weakness of SVM is that it is very sensitive to noise, a small number of mislabeled example can dramatically decrease its performance. This results in a slightly lower efficiency than ELM.

The ELM or the Extreme Learning Machine is a single hidden layer feed forward neural network based classifier. Its performance is better as it provides best generalization performance at extremely fast learning speed. Replacing an SVM with an ELM increases processing speed and efficiency of detecting forged parts. The classifier then gives the output as the forged part.

IV. RESULTS

In the images given below, (a) show the two original images, (b) gives us the tampered images, where different types of forgery have been done. Finally, image (c) gives us the final image, that has gone through feature extraction, feature analysis, forged parts detection and localising.



V. CONCLUSION

The experimental results shows that replacing SVM with ELM was able to achieve a considerable improvement in detection time and efficiency in detection. In this paper, we were able to devise a better and more efficient forgery detection and localization system, which can detect different types of forgery in real life tasks, and localize them.

VI. REFERENCES

[1] Haodong Li, Weiqi Luo and Xiaoqing Qiu "Image Forgery Localisation via Integrating Tampering Possibility Maps," IEEE transactions on Information Forensics and Security, Vol. 12, No. , May 2017.
[2] H. Farid, "Image Forgery detection, " IEEE *Signal Process. Mag*., Vol. 26, no. 2, pp. 16-25, Mar. 2009.
[3] M. C. Stamm, M. Wu and K. J. R. Liu "Information forensics: an Overview of the first decade," *IEEE Access*, vol. 1, pp. 167-200, May 2013.
[4] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling," *IEEE Trans. Signal Process.*, vol. 53, no. 2, pp. 758–767, Feb. 2005.
[5] B. G. Jeong, Y. H. Moon, and I. K. Eom, "Blind identification of image manipulation type using mixed statistical moments," *J. Electron. Imag.*, vol. 24, no. 1, p. 013029, 2015.
[6] G. Xu, J. Ye, and Y.-Q. Shi, "Experiments on digital image forgery detection using statistical-based approaches," presented at the IEEE Int.Workshop Inf. Forensics Secur. (WIFS), Nov. 2013.