



IMAGE FORGERY DETECTION USING COPY MOVE FORGERY

Mr. Dr. M. SIVA KUMAR, P. DURGA VASAVI, B. S. S. S. PRAVALLIKA, A. SAI. CHANDU,

P. KRUPAKAR, V. MONISH RISHI

Assistant Professor, Dept. Of ECE, PRAGATI ENGINEERING COLLEGE

UG Students, Dept. Of ECE, PRAGATI ENGINEERING COLLEGE

ABSTRACT:

In today's world scenario, image forgery is economical in the sense that its face value is greater than intrinsic value. It is also more elastic and stable, image forgery can be completed quickly, it is easy to move and safe to store. These all are the main reasons because of which counterfeit currency recognition is crucial. Forgery image cannot be identified by human vision and due to this recognition of forged images has become crucial problem because copying are using new and improved methods. The methods currently existing to determine whether the notes are real cannot be accessed by the common people and are also complex hardware-based methods. There are no applications or devices available through which image forgeries can be detected and identified easily by common people. The main purpose of the project is to identify image forgeries with a new methodical approach using Generative Adversarial Networks (GAN). In this system, the image forgery features would be primarily extracted using Convolutional Neural Networks (CNNs). The processed image data are then fed to a Generative Adversarial Network which helps to classify the image as either real or forgery. GAN consists of two main modules – Generator and Discriminator. The Generator generates forgery images and the Discriminator identifies and labels the real and forgery images.

INTRODUCTION

The world is becoming more advanced day by day as technology is growing rapidly. A human develops different software according to the type of wish he needs. Hence likewise now many images editing software are available. Using these tools the images get edited. This editing may have a positive face as well as a negative face. The negative face may cause a human life itself. Now different editing tools are available that can edit the image in any way they wish. Many morphological operations can occur in an image. These manipulations in an image are a serious issue regarding the authenticity, integrity, and reliability of the image. We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our email inboxes, doctored photographs are appearing with a growing frequency and sophistication. Over the past five years, the field of digital forensics has emerged to help restore some trust to digital images. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be roughly grouped into five categories:



- 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level;
- 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme;
- 3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post processing.

PROPOSED SYSTEM

The proposed copy-move forgery detection scheme. In the following experiments, the image dataset in is used to test the proposed scheme. The dataset is formed based on 48 high-resolution uncompressed PNG true color images. In the dataset, the copied regions are of categories of living, nature, man-made and even mixed, and they range from overly smooth to highly texture; the copy-move forgeries are created by copying, scaling and rotating semantically meaningful image regions. Fig. shows the copy-move forgery detection results of the proposed scheme. In the first column shows the forged images selected from the dataset; the second column shows the corresponding ground truth forged regions; and the third column shows the detected forgery regions. It can be easily seen that the proposed scheme can detect the forged regions very well.

A. Adaptive Over-Segmentation:

The proposed image forgery detection using adaptive over-segmentation in details. Figure shows the framework of the proposed scheme for image forgery detection. Firstly, the adaptive over-segmentation method is proposed to segment the host image into non-overlapping and irregular blocks. Then SLIC is applied into each block to extract feature points as block features which are matched with each other to locate the points which can approximately indicate the suspected forgery regions. Finally the forgery regions are detected according to the matched feature points.

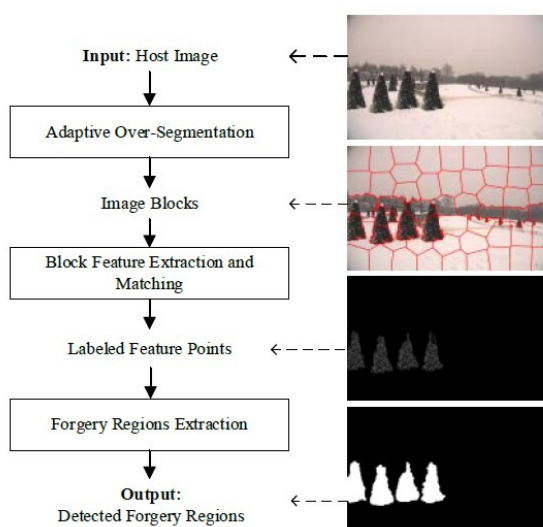


Figure.1 Flow chart for Adaptive over Segmentation

B. Copy Move Forgery



Digital images are easy to manipulate and edit due to availability of powerful image processing and editing software. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. As digital cameras and video cameras replace their analog counterparts, the need for authenticating digital images, validating their content, and detecting forgeries will only increase.

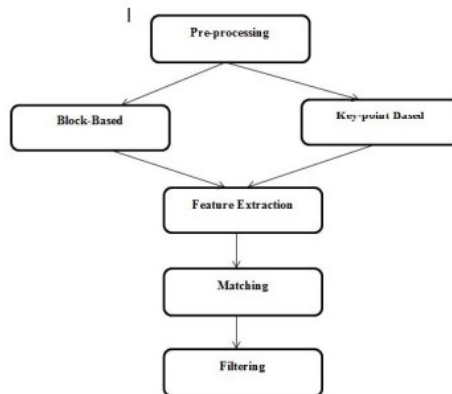


Figure.2 Flow diagram for copy move Forgery

STIMULATION RESULTS

In order to evaluate the performance of the proposed scheme, the precision and recall are calculated. We also give the Fscore, which is defined as a measure which combines the precision and recall in a single value.

$$precision = \frac{|R \cap R'|}{|R|}, \quad recall = \frac{|R \cap R'|}{|R'|}$$

Where R means the set of forgery regions detected by the proposed scheme for the dataset; and R' means the set of all forgery regions for the dataset $R \cap R'$

$$F = 2 \times \frac{precision \times recall}{precision + recall}$$





Figure. 6: Input Image

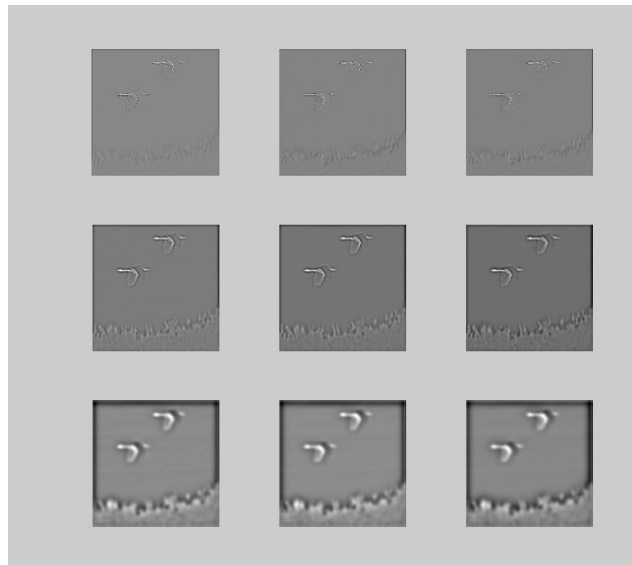


Figure.7 Copying, Scaling, Rotating

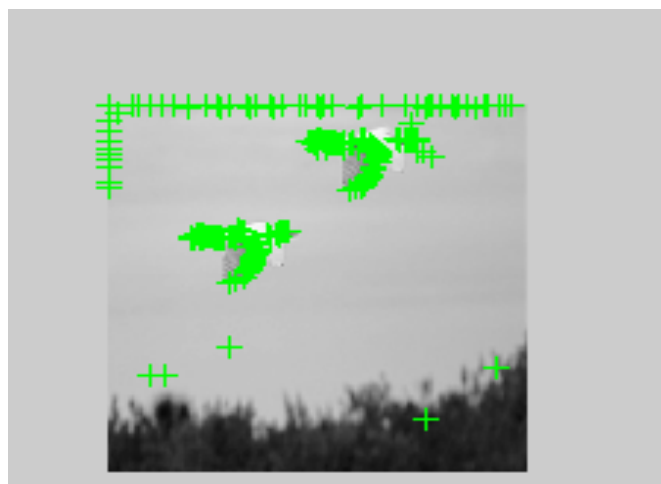


Figure.8 Key point Localization





Figure.9 Localized Forgery Extraction using SPP

Elapsed time is 1.943475 seconds.

Elapsed time is 5.779435 seconds.

Elapsed time is 3.334987 seconds.

Elapsed time is 2.763764 seconds.

Elapsed time is 0.380772 seconds.

Elapsed time is 0.535054 seconds.

ADVANTAGES

- **Authenticity Verification** – Ensures the credibility of digital images by detecting tampering.
- **High Accuracy** – Advanced detection algorithms (SIFT, SURF, DCT, DWT) provide reliable results.
- **Automation** – Can be implemented in software tools for automatic forgery detection.
- **Forensic Applications** – Used in cyber forensics and criminal investigations.
- **Robustness** – Can detect forgeries even under transformations like rotation, scaling, or compression.

APPLICATIONS

- **Digital Forensics** – Used by law enforcement agencies to analyze crime scene images.
- **Journalism & Media** – Prevents the distribution of manipulated images in news and social media.
- **Medical Imaging** – Ensures authenticity of medical reports and scans to prevent fraud.
- **Legal Evidence Verification** – Courts use it to verify the authenticity of image-based evidence.
- **Social media & Misinformation Detection** – Helps detect doctored images spreading fake news.

CONCLUSION

In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation. Adding further using Set partition of pixels (SPP) algorithm can adaptively segment the host image and later feature extraction done to irregular blocks already developed by copy move detection and block feature. In each block, the feature points are extracted and matched to indicate the suspected forgery regions. The Forgery Region Extraction algorithm is proposed to process the suspected feature points, thus generating the detected forgery regions and display output with its key point local feature and forged regions respectively. Experimental results show that the proposed scheme can achieve good performance under various challenging conditions such as geometric transforms, and JPEG compression.

Future work may focus on applying the proposed adaptive over-segmentation method into other kind of forgery such as splicing or other kind of media such as video and audio.

REFERENCES



- [1] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in in Proceedings of Digital Forensic Research Workshop, 2003.
- [2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Compute. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.
- [3] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, 2006, pp. 746-749.
- [4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in Multimedia and Expo, 2007 IEEE International Conference on, 2007, pp. 1750-1753.
- [5] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic science international, vol. 171, pp. 180-189, 2007.
- [6] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Computer Science and Software Engineering, 2008 International Conference on, 2008, pp. 926-930.
- [7] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.
- [8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in Multimedia Information Networking and Security, 2009. MINES'09. International Conference on, 2009, pp. 25-29.
- [9] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," Acta Automatic Sinica, vol. 35, pp. 1488-1495, 2009.
- [10] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, vol. 5, pp. 188-197, 2009