ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019

Image Forgery Detection using Adaptive Oversegmentation and Feature Point Matching

Angel Jeba Rathna.S[1], Priya.M[2], Sangeetha.N[3], Vellathai.P[4], Dr.Anitha.A[5]

[1](Dept. of IT, UG Scholar, Francis Xavier Engineering College, angeljr8778@gmail.com)
[2](Dept. of IT, UG Scholar, Francis Xavier Engineering College, priyadeekshi2408@gmail.com)
[3](Dept. of IT, UG Scholar, Francis Xavier Engineering College, sangeethasivayam2024@gmail.com)
[4](Dept. of IT, UG Scholar, Francis Xavier Engineering College, pvedhika04@gmail.com)
[5](Dept. of IT, Professor, Francis Xavier Engineering College, dr.aanitha@yahoo.com)

Abstract: A novel copy–move forgery detection scheme using adaptive oversegmentation and feature point matching is proposed in this paper. The proposed scheme integrates both block-based and keypoint-based forgery detection methods. First, the proposed adaptive oversegmentation algorithm segments the host image into nonoverlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, we propose the forgery region extraction algorithm, which replaces the feature points with small super pixels as feature blocks and then merges the neighboring blocks that have similar local color features into the feature blocks to generate the merged regions. Finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the proposed copy–move forgery detection scheme can achieve much better detection results even under various challenging conditions compared with the existing state-of-the-art copy–move forgery detection methods.

I. INTRODUCTION

With the development of computer technology and image processing software, digital image forgery has been increasingly easy to perform. However, digital images are a popular source of information, and the reliability of digital images is thus becoming an important issue. In recent years, more and more researchers have begun to focus on the problem of digital image tampering. Of the existing types of image tampering,a common manipulationof a digital image is copy-move forgery [1], which is to paste one or several copied region(s) of an image into other part(s) of the same image. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, and compression.

II. IMAGE FORGERY

We have performed a large number of experiments to seek the relationship between the frequency distribution of the host images and the initial size of the superpixels to obtain good forgery detection results. We performed a four-level DWT, using the 'Haar' wavelet, on the host image; then, the low-frequency energy ELF and high-frequency energy EHF can be calculated using (1) and (2), respectively. With the low-frequency energy ELF and high-frequency energy EHF, we can calculate the percentage of the low-frequency distribution PLF using (3), according to which the initial size S of the superpixels can be defined. Where S means the initial size of the superpixels; M × N indicates the size of the host image; and PLF means the percentage of the low-frequency distribution. In summary, the flow chart of the proposed Adaptive Over-Segmentation method is shown in Fig. 3. First, we employed the DWT to the host image to obtain the coefficients of the low- and high-frequency sub-bands of the host image. Then, we calculated the percentage of the low-frequency distribution PLF using (3), according to which we determined the initial size S, using (4). Finally, we employed the SLIC segmentation algorithm together with the calculated initial size S to segment the host image to obtain the image blocks. In this section, we extract block features from the image blocks (IB). The traditional block-based forgery detection methods extracted features of the same length as the block features or directly used the pixels of the image block as the block features; however, those features mainly reflect the content of the image blocks, leaving out the location information. In addition, the features are not resistant to various image transformations.

All Rights Reserved © 2019 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019

III. EXISTING SYSTEM

We demonstrate the effectiveness of the proposed scheme with a large number of experiments. Experimental results show that the proposed scheme can achieve much better detection results for copy-move forgery images under various challenging conditions, such as geometric transforms, JPEG compression, and down-sampling, compared with the existing state-of-the-art copy-move forgery detection schemes. Future work could focus on applying the proposed forgery detection scheme based on adaptive over-segmentation

IV. PROPOSED SYSTEM

A novel copy–move forgery detection scheme using adaptive over- segmentation and feature point matching.
An alternative to the block-based methods, key point based forgery detection methods were proposed. Key points are extracted and matched over the whole image to resist some image transformations. Though the pixel-level metrics are useful for assessing the general localization performance of the algorithm when the ground-truth data are available, the image-level decisions are especially interesting with respect to the automated detection of manipulated images

V. MATLAB

It is the high level language and interactive environment used my millions of engineers and scientists worldwide. It is used for machine learning, signal processing, image processing, computer vision, communications, computational finance, control design, robotics, and much more.

It has several advantages over other methods or languages. Its basic element is matrix. Several mathematical operations that work on arrays or matrices are built in to the Matlab environment. It is a dataflow graphical programming language tool for modelling, simulating and analyzing multi-domain dynamic systems. It allows us to incorporate MATLAB algorithms into models as well as export the simulation results into matlab.

Matlab programming language

There are very feasible in the following
MATLAB has its advantages too:
It has a solid amount of functions.
Simulink is a product for which there is no good alternative yet.It might be easier for beginners, because the package includes all you need, while in Matlab, we need to install extra packages and an IDE.
It is a high-level language and interactive environment for numerical computation, visualization and programming. Using this, we can analyze data, develop algorithms, and create models and applications.

Image Loading

Training Data We use 3 separate image datasets for training and testing.

ImageNetdataset ,Places2 dataset and CelebA-HQ . We use the original train, test, and val splits for ImageNet and Places2. For CelebA-HQ, we randomly partition into 27K images for training and 3K images for testing. Training Procedure we initialize the weights using the initialization method described in and use Adam for optimization. We train on a single NVIDIA V100 GPU (16GB) with a batch size of 6.

Initial Training and Fine-Tuning. Holes present a problem for Batch Normalization because the mean and variance will be computed for hole pixels, and so it would make sense to disregard them at masked locations. However, holes are gradually filled with each application and usually completely gone by the decoder stage. In order to use Batch Normalization in the presence of holes, we first turn on Batch Normalization for the initial training using a learning rate of 0.0002. Then, we fine-tune using a learning rate of 0.00005 and freeze the Batch Normalization parameters in the encoder part of the network. We keep Batch Normalization enabled in the decoder. This not only avoids the incorrect mean and variance issues, but also helps us to achieve faster convergence. ImageNetandPlaces2 models train for 10 days, whereas CelebA-HQ trains in 3 days. All fine-tuning is performed in one day.

Gray Image

Previous works generate blocks in their datasets by randomly removing rectangular regions within their image.We consider this insufficient in creating the diverse hole shapes and sizes that we need.As such, we begin by collecting masks of random streaks and blocks of arbitrary shapes. We found the results of occlusion/dis-occlusion mask estimation method between two consecutive frames for videos described in to be a good source of such patterns. We generate 55,116 masks for the training and 24,866 masks for testing. During training, we augment the mask dataset by randomly sampling a mask from 55,116 masks and later perform random dilation, rotation and cropping. All the masks and images for training and testing are with the size of 512×512. We create a test set by starting with the 24,866 raw masks and adding random dilation, rotation and cropping. Many previous methods such as have Image Forgery for Irregular Blocks Using Partial Convolutions 9

All Rights Reserved © 2019 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019

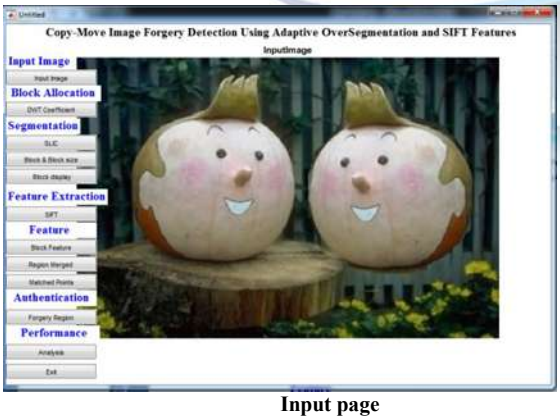
Gray Image

Some test masks for each hole-to-image area ratio category. 1, 3 and 5 are shown using their examples with border constraint; 2, 4 and 6 are shown using their examples without border constraint degraded performance at blocks near the image borders. As such, we divide the test set into two: masks with and without blocks close to border.

The split that has blocks distant from the border ensures a distance of at least 50 pixels from the border. We also further categorize our masks by hole size. Specifically, we generate 6 categories of masks with different hole-to-image area ratios: (0.01, 0.1], (0.1, 0.2], (0.2, 0.3], (0.3, 0.4], (0.4, 0.5], (0.5, 0.6].Each category contains 1000 masks with and without border constraints. In total, we have created 6×2×1000 = 12,000 masks. Some examples of each category's masks can be found ut border constraint degraded performance at holes near the image borders. As such, we divide the test set into two: masks with and without holes close to border.

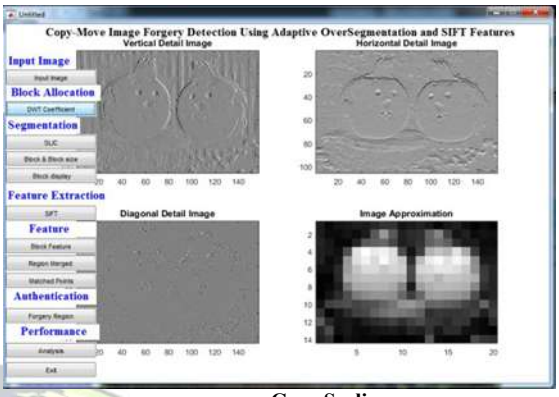
The split that has holes distant from the border ensures a distance of at least 50 pixels from the border. We also further categorize our masks by hole size. Specifically, we generate 6 categories of masks with different hole-to-image area ratios: (0.01, 0.1], (0.1, 0.2], (0.2, 0.3], (0.3, 0.4], (0.4, 0.5], (0.5, 0.6].Each category contains 1000 masks with and without border constraints. In total, we have created 6×2×1000 = 12,000 masks.

VI. SCREENSHOTS



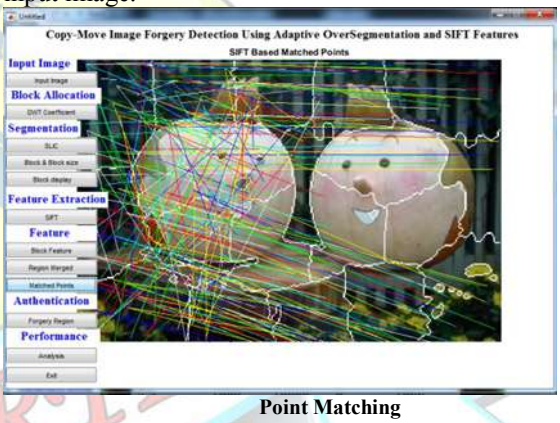
Input page

This is the page where we load the image by clicking load image button.



Gray Scaling

In this page the user has to type the patch sizeof the input image.



Point Matching

This is apply for the Gaussian Smoothing which is available in sigma, the use have to type the required size of the sigma.

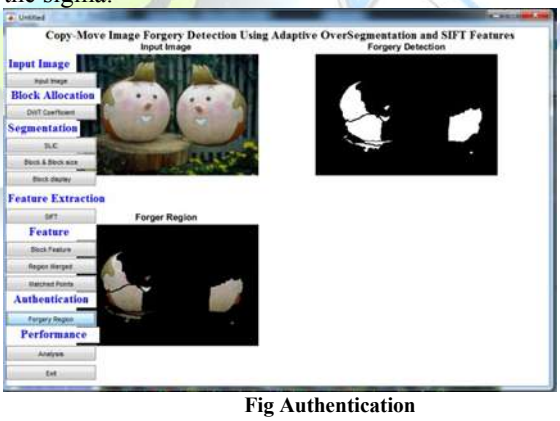


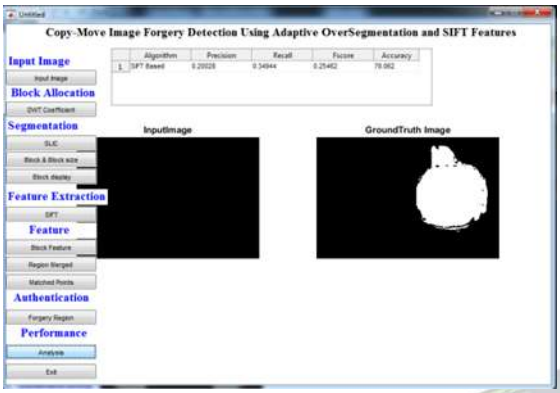
Fig Authentication

Now the input image is loaded and the use have to select the portion that the use has to remove and the mask is created.

All Rights Reserved © 2019 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019



Analysis

Finally the image is obtained.

VII. CONCLUSION

We propose the use of a forgery layer with an automatic pixel matching updating mechanism and achieve copy-move image forgery results. Our model can robustly handle blocks of any shape, size location, or distance from the image borders. Further, our performance does not deteriorate catastrophically as blocks increase in size. However, one limitation of our method is that it fails for some sparsely structured images.

REFERENCES

[1]. Fridrich.J, Soukal.D and Lukáš.J (2003) Detection of copy–move forgery in digital images, in Proc. Digit. Forensic Res. Workshop, Cleveland, OH, Aug.

[2]. Popescu A.C and Farid.H,(2004) Exposing digital forgeries by detecting duplicated image regions, Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515.

[3]. Luo.W, Huang.J, and Qiu.G, (2006) Robust detection of region-duplication forgery in digital image, in Proc. 18th Int. Conf. Pattern Recognit. (ICPR), Aug. pp. 746–749.

[4]. Li.G Wu.Q, D. Tu, and Sun.S, A(2007) sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD,in Proc. IEEE Int. Conf. Multimedia Expo, Jul. , pp. 1750–1753.

[5]. Mahdian.B and Saic.S(2007) Detection of copy–move forgery using a method based on blur moment invariants, Forensic Sci. Int., vol. 171, nos. 2–3, pp. 180–189,

[6]. Kang X.B and Wei S.M(2008) Identifying tampered regions using singular value decomposition in digital image forensics, in Proc. Int. Conf. Comput. Sci. Softw. Eng., Dec. , pp. 926–930.

[7]. Bayram.S SencarH.T and Memon.N,(2009)An efficient and robust method for detecting copy–move forgery, in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. , pp. 1053–1056.

[8]. J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang,(2009) Detection of image region duplication forgery using model with circle block, in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. , pp. 25–29.

[9]. Wang J.W, Liu G.J, Zhang.Z, DaiY.W, and Wang Z.Q,(2009) Fast and robust forensics for image region-duplication forgery, Acta Automat. Sinica, vol. 35, no. 12, pp. 1488–1495,

[10]. Lin H.J, Wang C.W, and Kao Y.T,(2009) Fast copy–move forgery detection,WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188–197,

[11]. Ryu S.J, Lee M.J, and Lee H.K (2010), Detection of copy-rotate-move forgery using Zernike moments, in Information Hiding. Berlin, Germany: Springer-Verlag, , pp. 51–65.

[12]. Ryu S.J, Kirchner, M. J, Lee, and . Lee.K(2013), Rotation invariant localization of duplicated image regions based on Zernike moments, IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1355–1370, Aug. .

[13]. Bravo-Solorio.S and Nandi.A,(2011) Exposing duplicated regions affected by reflection, rotation and scaling, in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May , pp. 1880–1883.

[14]. Huang.H, Guo.W, and Zhang.Y, (2008)Detection of copy–move forgery in digital images using SIFT algorithm, in Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA), Dec. , pp. 272–276.

[15]. Pan.X and Ly.S,(2010) Region duplication detection using image feature matching, IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857–867, Dec.

[16]. AmerinI.I, Ballan.L Caldelli.R, .IA. Del Bimbo, and Serra (2011), A SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep..

[17]. Bo.X, Junwen.W, Guangjie.L, and Yuewe.Di,(2011) Image copy–move forgery detection based on SURF,in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. , pp. 889–892.

All Rights Reserved © 2019 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 6, Issue 5, May 2019

All Rights Reserved © 2019 IJARTET