INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 498-503
RECEIVED : 23/02/2016. PUBLISHED : 3/03/2016 March 3, 2016

SEGMENTATION BASED ON IMAGE COPY MOVE FORGERY DETECTION BY USING IMAGE FEATURE MATCHING

Buvana Ranjani.M, Dept of Communication Systems Engg, Adhiyamann College Of Engineering, Hosur,
Mr.Poovendran.R, Asst.Prof, Dept of ECE, Adhiyamann College Of Engineering, Hosur.

Abstract:

In this paper, we propose a scheme to detect the copy-move forgery in an image, mainly by extracting the key points for comparison. The main difference to the traditional methods is that the proposed scheme first segments the test image into semantically independent patches prior to key point extraction. As a result, the copy-move regions can be detected by matching between these patches. The matching process consists of two stages. In the first stage, we find the suspicious pairs of patches that may contain copy-move forgery regions, and we roughly estimate an affine transform matrix. In the second stage, an Expectation-Maximization-based algorithm is designed to refine the estimated matrix and to confirm the existence of copy move forgery.

Key words – Maximization Based Algorithms, Forgery, Pairs of patch.

1. INTRODUCTION

The term digital image refers to processing of a two dimensional picture by a digital computer. In a broader context, it implies digital processing of any two dimensional data. A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory.

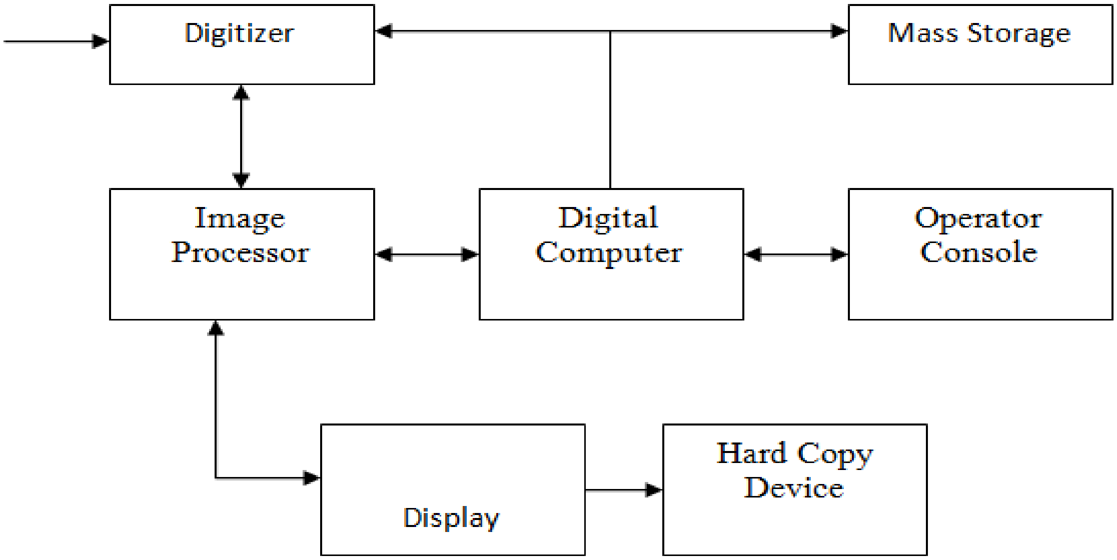


Fig.1.Block diagram of image processing system

This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display. The next step is the preprocessing step where the image is improved being fed as an input to the other processes. Preprocessing typically deals with enhancing, removing noise, isolating regions, etc. Segmentation partitions an image into its constituent parts or objects. The output of segmentation is usually raw pixel data, which consists of either the boundary of the region or the pixels in the region themselves. Representation is the process of transforming the raw pixel data into a form useful for subsequent processing by the computer. Description deals with extracting features that are basic in differentiating one class of objects from another. Recognition assigns a label to an object based on the information provided by its descriptors. Interpretation involves assigning meaning to an ensemble of recognized objects. The knowledge about a problem domain is incorporated into the knowledge base. The knowledge base guides the operation of each processing module and also controls the interaction between the modules. Not all modules need be necessarily present for a specific function. The composition of the image processing system depends on its application. The frame rate of the image processor is normally around 25 frames per second.

2. EXISTNG SYSTEM

In this paper, we adopt a practitioner’s view to copy-move forgery detection. If we need to build a system to perform CMFD independent of image attributes, which may be unknown, we created a realistic database of forgeries, accompanied by software that generates copy-move forgeries of varying complexity. We defined a set of what we believe are “common CMFD scenarios” and did exhaustive testing over their parameters. A competitive CMFD method should be able to cope with all these scenarios, as it is not known beforehand how the forger applies the forgery. We implemented 15 feature sets that have been proposed in the literature, and integrated them in a joint pipeline with different pre- and post processing methods. Key point-based methods have a clear advantage in terms of computational complexity, while the most precise detection results can be achieved using Zernike moments.

3. LITERRATURE SURVEY

A copy-move forgery is created by copying and pasting content within the same image, and potentially post processing it. In recent years, the detection of copy-move forgeries has become one of the most actively researched topics in blind image forensics. A considerable number of different algorithms have been proposed focusing on different types of post processed copies. 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. Located at the consumer-end of the Smart Grid, domestic energy monitoring and management systems aim to provide direct energy feedback whilst consumption occurs, so as to persuade users to achieve energy saving and efficiency. Image manipulation has become commonplace with growing easy access to powerful computing abilities. One of the most common types of image forgeries is the copy–paste forgery, wherein a region from an image is replaced with another region from the same image. Most prior approaches to finding identical regions suffer from their inability to detect the cloned region when it has been subjected to a geometric transformation. In this paper, we propose a novel technique based on transform-invariant features.

4. PROPOSED SYSTEM

We propose a straightforward yet effective replacement for the shift vectors that can expressly handle affine transformations. The core idea is to explicitly estimate the rotation and scaling parameters from a few blocks, expressed as an affine transformation matrix. Starting from an initial estimate, we apply region growing on block pairs with similar transformation parameters. Consider the i-th matched pair ~fi of feature vectors ~fi1, ~fi2, ~fi = (~fi1, ~fi2). In order to determine the rotation and translation between block pairs, we need to examine the coordinates of the block centers. Let C(~fij) denote the coordinates (in row vector form) of the block center from where ~fij was extracted,

$$\vec{p}_i = C(\vec{f}_{i1}), \qquad \vec{q}_i = C(\vec{f}_{i2}).$$

This is due to the use of a greedy strategy in the selection of suitable neighbors for the initial hypothesis. Within a local region, we pick two candidates that have been mapped into the same region.

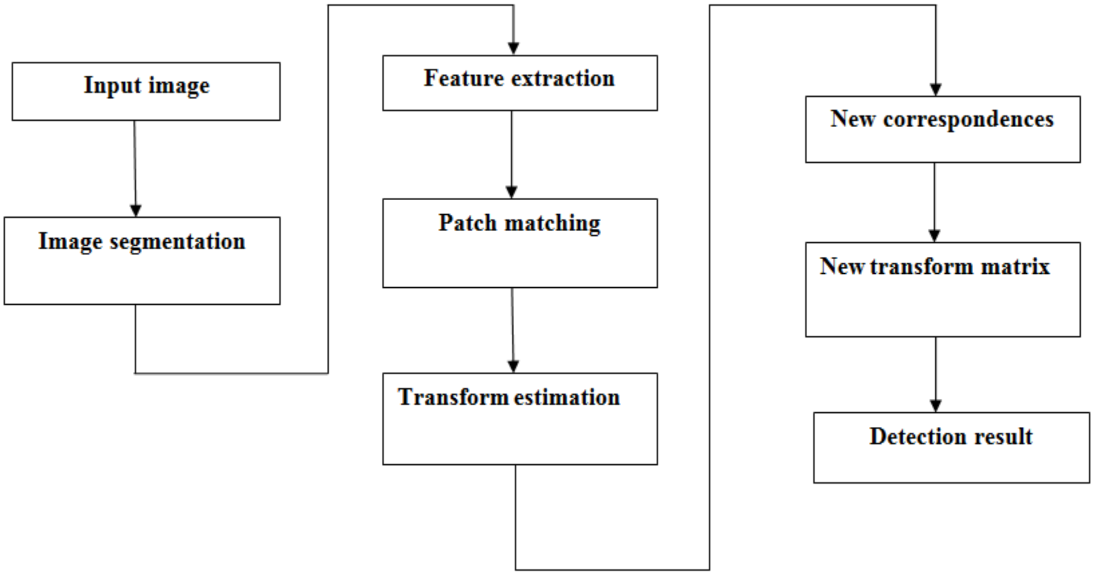


Fig.2.Block diagram of proposed system

Though this might be questionable from a theoretical viewpoint, we found the results to be sufficiently good in practice. Thus, the complexity mainly consists of: a) an iteration over all blocks and b) a per-block neighborhood search for suitable pairs. More precisely, let NB be the total number of blocks in the image, NCB the number of copied blocks and N the neighborhood size. Then the worst-case runtime is O (NBNCBN). In practice, it is reasonable to assume that NCB _ NB. Thus, the complexity is mainly influenced by the number of blocks in the image. When timing our code, we noticed that our unoptimized implementation of SATS takes at most as long as feature extraction and matching. Thus, it at most doubles the processing time for a particular image.

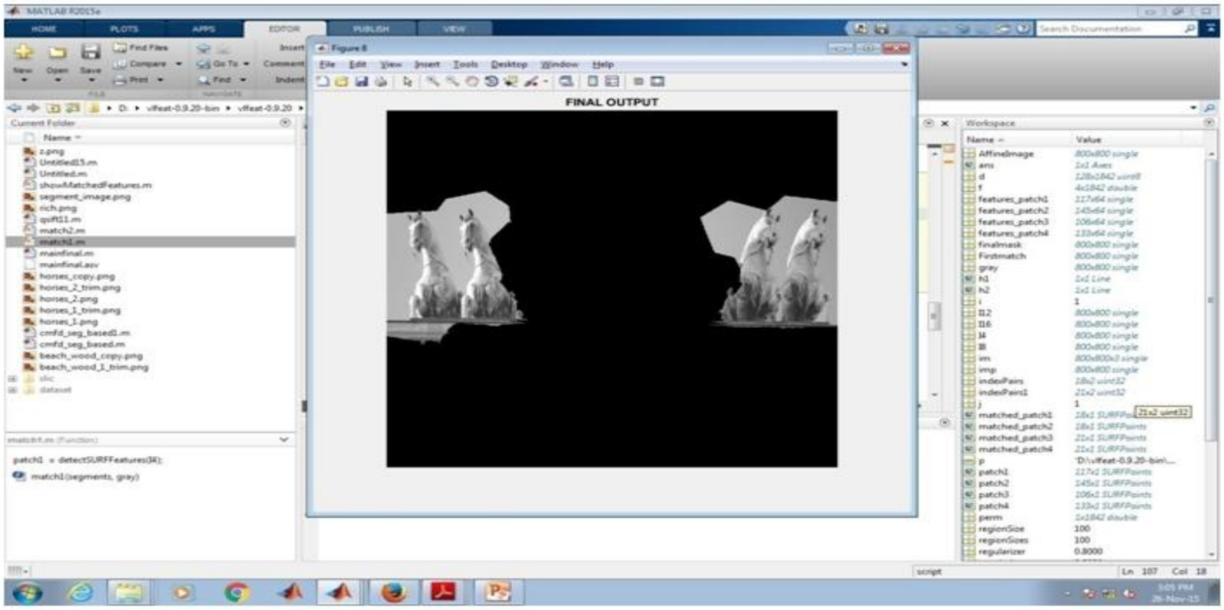
5. RGB COLOUR IMAGE

The RGB color model is an additive color model in which red, green, and blue light are added together in various ways to reproduce a broad array of colors. The name of the model comes from the initials of the three additive primary colors, red, green, and blue. The main purpose of the RGB color model is for the sensing, representation, and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography. Before the electronic age, the RGB color model already had a solid theory behind it, based in human perception of colors. RGB is a device-dependent color model: different devices detect or reproduce a given RGB value differently, since the color elements (such as phosphors or dyes) and their response to the individual R, G, and B levels vary from manufacturer to manufacturer, or even in the same device over time.

Fig.3. Example of RGB colour image

Thus an RGB value does not define the same color across devices without some kind of color management. Typical RGB input devices are color TV and video cameras, image scanners, and digital cameras. Typical RGB output devices are TV sets of various technologies (CRT, LCD, plasma, etc.), computer and mobile phone displays, video projectors, multicolor LED displays, and large screens such as JumboTron. Color printers, on the other hand, are not RGB devices, but subtractive color devices (typically CMYK color model).

6. RESULT ANALYSIS



D: ▸ vlfeat-0.9.20-bin ▸ vlfeat-0.9.20 ▸

Name
z.png
Untitled15.m
Untitled.m
showMatchedFeatures.m
segment_image.png
rich.png
qsift11.m
match2.m
match1.m
mainfinal.m
mainfinal.asv
horses_copy.png
horses_2_trim.png
horses_2.png
horses_1_trim.png
horses_1.png
cmfd_seg_based1.m
cmfd_seg_based.m
beach_wood_copy.png
beach_wood_1_trim.png
slic
dataset

match1.m (Function)

```
patch1 = detectSURFFeatures(I4);
match1(segments, gray)
```

Name	Value
AffineImage	800x800 single
ans	1x1 Axes
d	128x1842 uint8
f	4x1842 double
features_patch1	117x64 single
features_patch2	145x64 single
features_patch3	106x64 single
features_patch4	133x64 single
finalmask	800x800 single
Firstmatch	800x800 single
gray	800x800 single
h1	1x1 Line
h2	1x1 Line
i	1
I12	800x800 single
I16	800x800 single
I4	800x800 single
I8	800x800 single
im	800x800x3 single
imp	800x800 single
indexPairs	18x2 uint32
indexPairs1	21x2 uint32
j	1
matched_patch1	18x1 SURFPoi… 21x2 uint32
matched_patch2	18x1 SURFPoints
matched_patch3	21x1 SURFPoints
matched_patch4	21x1 SURFPoints
p	'D:\vlfeat-0.9.20-bin\...
patch1	117x1 SURFPoints
patch2	145x1 SURFPoints
patch3	106x1 SURFPoints
patch4	133x1 SURFPoints
perm	1x1842 double
regionSize	100
regionSizes	100
regularizer	0.8000

Fig.4. Final Output Image

Matlab is a program that was originally designed to simplify the implementation of numerical linear algebra routines.It has since grown into something much bigger, and it is used to implement numerical algorithms for a wide range of applications. The basic language used is very similar to standard linear algebra notation, but there are a few extensions that will likely cause you some problems at first.

CONCLUSION

This paper presented a CMFD scheme based on image segmentation. Although the CMF regions are detected mainly by comparing the keypoints extracted in the image, we cannot simply classify the proposed scheme as a keypoint-based one. Considering the CMF regions usually have certain meaning, we propose to segment the image into semantically independent patches, such that the CMFD problem can be solved by partial matching among these segmented patches.

REFERENCES

[1] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, “An evaluation of popular copy-move forgery detection approaches,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[2] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, “Detection of copy-move forgery in digital images,” in Proc. Digit. Forensic Res. Workshop, 2003.

[3] W. Luo, J. Huang, and G. Qiu, “Robust detection of regionduplication forgery in digital image,” in Proc. 18th Int. Conf. Pattern Recognit. (ICPR), vol. 4. 2006, pp. 746–749.

[4] S. Bayram, H. T. Sencar, and N. Memon, “An efficient and robust method for detecting copy-move forgery,” in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Washington, DC, USA, Apr. 2009, pp. 1053–1056.

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

[6] M. Ghorbani, M. Firouzmand, and A. Faraahi, “DWT-DCT (QCD) based copy-move image forgery detection,” in Proc. 18th Int. Conf. Syst., Signals Image Process. (IWSSIP), Jun. 2011, pp. 1–4.

[7] S. Khan and A. Kulkarni, “Detection of copy-move forgery using multiresolution characteristic of discrete wavelet transform,” in Proc. Int. Conf. Workshop Emerg. Trends Technol. (ICWET), New York, NY, USA, 2011, pp. 127–131.

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

[9] V. Christlein, C. Riess, and E. Angelopoulou, “On rotation invariance in copy-move forgery detection,” in Proc. IEEE Workshop Int. Inf. Forensics Secur. (WIFS), Dec. 2010, pp. 1–6.

[10] H. Huang, W. Guo, and Y. Zhang, “Detection of copy-move forgery in digital images using SIFT algorithm,” in Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA), vol. 2. Dec. 2008, pp. 272–276.