5th SASTech
Iran | Mashhad
May 12 - 17 | 2011
5th Symposium on Advances in Science & Technology

A Survey of three digital image forgery detection methods Based on image processing techniques

Mohammad V. Malakooti [1], Ahmad Pahlavan Tafti [2]
[1]Islamic Azad University, Dubai, UAE; [2] Islamic Azad University, Dubai, UAE
Malakooti@iau.ae, Ahmad.pahlavantafti@yahoo.com

Paper Reference Number: **0101-663**
Name of the Presenter: **Mohammad V. Malakooti**

Abstract

Digital image processing and machine vision are the most practical technologies which are mixing with different sciences like medicine, engineering and mathematics. Digital image processing has a precious role in designing and implementing intelligent systems, medical engineering, traffic and transportation, medical recognition, data centres, airports and military security.

A Digital image is a set of several physical and logical features that will help us to extract operational concepts from it, where we have good processing models.

Authority and validity of the digital images is one of the critical challenges for governmental organizations and departments. Nowadays, it is possible to add or remove important features from a digital image without leaving any obvious traces of tampering due to availability of powerful image processing and editing software like Photoshop.

We review three methods proposed to achieve forgery detection in digital images. In this paper we investigate on the performance, robustness and time complexity of these methods. All of these methods are demonstrated on several forged and non forged digital images. Compromising of these approaches is addressed at the end of this paper.

Key words: Digital image processing, forgery image detection.

1. Introduction

Images are playing a great role in human understanding. Human is not able to see and understand electromagnetic spectrums but digital equipments like cameras could capture all these. Actually, there is no border between digital image processing and machine vision. Having a good model in this aspect is performing a well calculating process, which are categorized in low level, moderate level and high level processes [10].

Low level processes consist of different parts such as noise decreasing, contrast improvement and changing transparency. It is the first operation should perform on a digital images and prepared images for the next steps. Moderate level processes divided to digital image operations like segmentation and quantization and last processes are highest processes that make a sense to feel a behavior from an object like happiness or sadness.

Understanding the authenticity and validity of a digital image is always a problem and challenge for organizations especially who are working on e-forms and e-documents. Nowadays, there are several powerful tools for editing digital images, therefore it is possible to someone use these tools to change contains of digital images. A tampered image known as a forged image.

There are several ways to detecting forgery digital images, but in this paper we just talk about three of them. The most famous and operational ways are cloning, resampling and statistical techniques. Each of these ways is able to find forgery digital images according to digital image's features, correlations and statistical information. Robustness, time complexity, and memory usage of these types are different, this happens because the digital images are different too. Some of them contain text and signature, stamp or table but others may have personal images or objects. So it is completely clear that these digital images are different in features and also qualification.

In this paper, we investigate on the performance and robustness of these methods. The reminder of this paper arranged as follows. Three different methods of detecting the forgery in digital images are described in the next section. We have tested all of these models on the Mashhad Customs clearance datasets.

Evaluating and comparing of these methods and their results are shown in section 4. Conclusion is addressed in section 5.

2. Three techniques for forgery digital images detection

The digital information revolution and issues concerned with multimedia security have also generated several approaches to tampering detection. Generally, these approaches could be divided into active and passive approaches [11]. The area of active methods simply can be divided into the data hiding approaches. By data hiding we refer to methods embedding secondary data into the image [12], [13]**.** Active approaches assume an inserting of a digital data at the source side (e.g., Scanner) and verifying the mark integrity at the detection side [1].

Passive methods are mostly based on the fact that forgeries can bring into the image specific detectable changes [7]. Passive techniques for image forensics operate in the absence of any data or signature. 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 [2]. Methods which are described in the following detect statistical anomalies introduced at the pixel level. You can be seen the one type of image forgery in Fig.1.

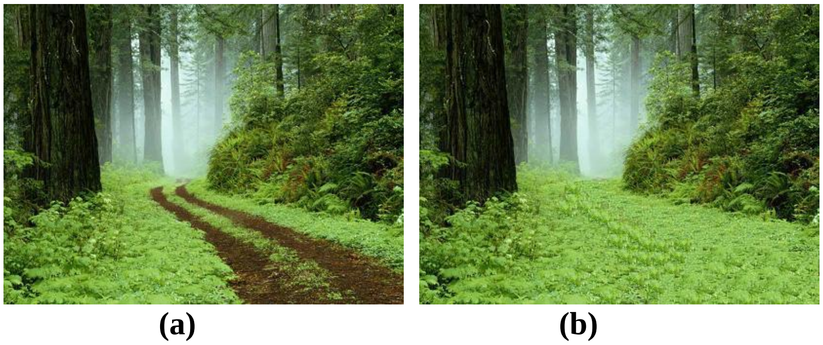

Fig 1: digital image forgery, (a) original image, (b) forged image.

2.1. Cloning

There are a number of possible forgeries in digital images. One of the most common image forgeries is copy and paste some parts of the image to disappearing an object in the image. This type of forgery is known as the cloning and it can be difficult to detect cloning visually.

Since the cloned regions can be of any shape and location, it is computationally impossible to search all possible image locations and sizes. Two computationally efficient algorithms have been developed to detect cloned image regions [2], [11]. The authors in [2] first apply a block discrete cosine transform (DCT). Duplicated regions are detected by lexicographically sorting the DCT block coefficients and grouping similar blocks with the same spatial offset in the image.

2.2. Resampling

To create a composite image, it is necessary to resize, rotate, or stretch portions of an image. For example, when creating a composite of two people, one person may have to be resized to match the relative heights and widths. Many forgeries particularly embedded one part of an image to another image. This way is often called resampling. This process requires resampling the original image onto a new sampling lattice, introducing specific periodic correlations between neighboring pixels. Because these correlations are unlikely to occur naturally, their presence can be used to detect this specific manipulation [12]. All approaches in this method are described in [6], [5] and [9].

2.3. Statistical

Each digital image has two types of properties. One of them is visual perception properties like contrast and lightness and another is the statistical properties. This method works on the specific statistical properties. The authors in [2], [3] and [4] exploit statistical regularities in natural images to detect various types of image manipulation. The authors in [8] compute first and higher-order statistics from wavelet decomposition. This decomposition splits the frequency space into multiple scale and orientation sub bands.

3. Methods Evaluation

In order to evaluate performance, robustness and time complexity of the proposed methods we perform several tests on a sample dataset. Our sample dataset is customs clearance documents in Mashhad customs. All codes are implemented with MATLAB R2009.

Our dataset contains one hundred of forged and also non forged digital images (600*800 pixels) in gray scale mode.

In Table 1, you can see the percentage of true and false detection of digital image forgery which are performed by these three methods. As you see, statistical method is the most robustness approach which we can use for digital image forgery detection.

Methods	True Alert (%)	False Alert (%)
Cloning	93	7
Resampling	82	18
Statistical	97	3

Table 1. The true and false alerts in detecting digital forgery on sample dataset.

To understand the time complexity of these approaches, consider the line chart shown in Fig. 2.

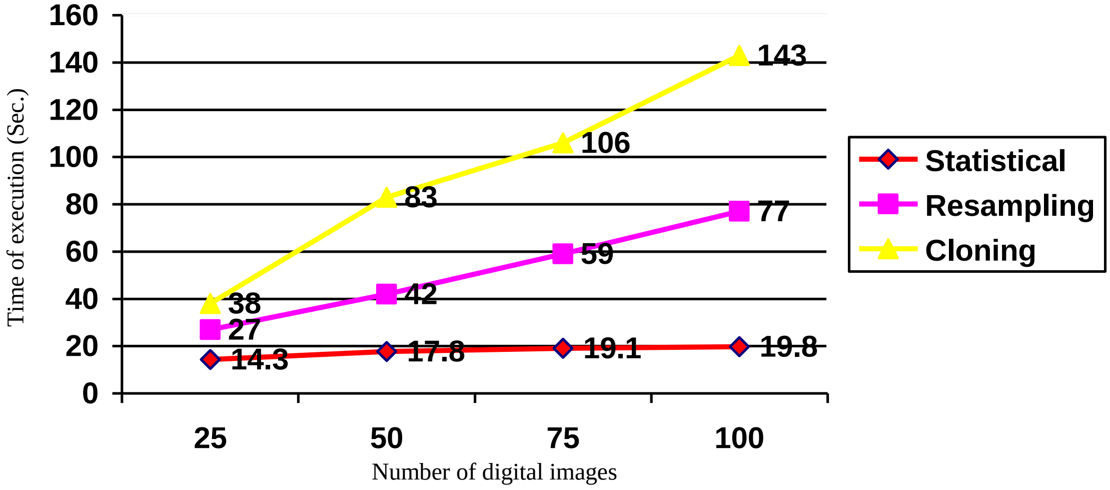

Fig 2: The line chart of time complexity for all of these three methods.

4. Results

To demonstrate these algorithms's ability and robustness to operate on digital image forgery detection, we used all of them in a same dataset and pointed to true and false alert of these methods

To test the performance of these three methods, we applied these to true and false alert shown in Table 1. The resulting estimate of time of execution is shown in Fig .2. When we compare the estimated line chart shown in Fig. 2 we find some difference between theses methods.

This chart shows how time of execution is changing by increasing number of digital images in three methods of forgery detection. In this figure, it can be seen runtime in statistical method has remained stable while time of execution has risen sharply in both resampling and cloning.

On the other hand, there are considerable differences in chart for time of execution. Statistical can process 50 images in 17.8 second whereas time of execution in resampling is 42 sec and 83 sec in cloning. Also in statistical variance of time for equal growth of images is fewer than resampling and cloning. It means, between 25 to 50 images, it is about 3.5 in statistical while it is 15 in resampling and 45 in cloning. Rate of alternations have increased in both of resampling and cloning as it is approximately stable with a little conversion.

5. Conclusions

In this paper, we presented a survey of three methods for digital image forgery detection. All of these methods considered as active methods. However, these are not all of active approaches to detecting the digital image forgery. The Statistical method is more robustness than cloning and resampling. Processing in cloning is more slowly than resampling and statistical. It means time of processing in the statistical method is faster than other methods.

References

[1] Arnold, M. & Schmucker, M. & Wolthusen, S.D. (2003). Techniques and Applications of Digital Watermarking and Content Protection, *Artech House, Inc*. Norwood, MA, USA.

[2] Avcibas, I. & Bayram, S. & Memon, N. & Sankur, B (2006). Image manipulation detection. *J. Electron. Imaging*. vol. 15, no. 4, p. 41102.

[3] Avcibas, I. & Bayram, S. & Memon, N. & Sankur, B. (2005). Image manipulation detection with binary similarity measures. *European Signal Processing Conf*. Turkey.

[4] Farid, H. & Lyu, S. (2003). Higher-order wavelet statistics and their application to digital forensics. *IEEE Workshop on Statistical Analysis in Computer Vision (in conjunction with CVPR)*. Madison, WI.

[5] Gallagher, A.C. (2005). Detection of linear and cubic interpolation in jpeg compressed images. *2nd Canadian Conf. Computer and Robot Vision, Victoria, British Columbia*. Canada, vol. 171, pp. 65–72.

[6] Kirchner, M. (2008). Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue. *ACM Multimedia and Security Workshop*. pp. 11–20.

[7] Lukas, J. (2000). Digital image authentication using image filtering techniques. *Proceedings of ALGORITMY 2000, Conference on Scientific Computing*. Podbanske, Slovakia, pp. 236–244.

[8] Farid, H. & Lyu, S. (2006). Steganalysis using higher-order image statistics. *IEEE Trans. Inform. Forensics Security*. vol. 1, no. 1, pp. 111–119.

[9] Prasad, S & Ramakrishnan, K. R. (2006). On resampling detection and its application to image tampering. *IEEE Int. Conf. Multimedia and Exposition*. Toronto, Canada, pp. 1325–1328.

[10] Boyle, R. & Hlavac, V. & Sonka, M. (2008). Image Processing, Analysis, and Machine Vision. *Thomson Learning*.

[11] Akansu, A.N. & Ramkumar, M. & Sencar, H.T. (2004). Data Hiding Fundamen- tals and Applications: Content Security in Digital Multimedia. *Academic Press, Inc.* Orlando, FL, USA.

[12] Wu, M. (2001). Multimedia data hiding, Ph.D. Thesis, A dissertation presented to the faculty of Princeton university in candidacy for the degree of doctor of philosophy.

[13] Liu, B. & Wu, M. (2002). Multimedia Data Hiding. *Springer-Verlag*. New York, NJ, USA.