International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

A Survey Paper on Revealing Image Forgery Using Image Manipulation Detection

Deepak B. Waghchaure[1], Ashish R. Gaikwad[2]

[1]Student, Master of Engineering, Department of Computer Engineering, Sir Visvesvaraya Institute of Technology, Chincholi, Sinner

[2]Student, Department of Civil Engineering, Sanjivani College of Engineering, Kopargaon

Abstract: ***There are different kinds of images are available from which Digital images are most widely used in the various fields like medical imaging, journalism, criminal and forensic investigation. There are different software's are available to make a duplicate image or which changes the original effect of images due to which the original contrast is get disturbed. Therefore it is necessary to create forensic techniques which are capable of detecting the tampering in image. In this paper, we present various techniques which detect global contrast enhancement and copy-paste forgery. This proposed technique of detection of contrast-enhanced image is based on contrast calculation. In copy-paste forgery detection, we used DCT based feature extraction method. The technique can efficiently detect the small, medium and large size regions in the forged image.***

Keywords: digital forensics; contrast enhancement; image forgery; image processing; copy-paste forgery

1. Introduction

Digital image authentication techniques broadly have two types i.e. active and passive. The active approach includes intrusive methods like watermarking and digital signature. With the increased importance of the digital images in various applications, where authenticity is of prime importance, it is necessary to verify the integrity and authenticity of digital images. It is also known as non-blind methods. The drawback of waterark approach is that atermarks need to be embedded in the image before distribution. Since the problem of image forensics is very broad, this paper focuses on forgery detection in digital images. This paper present efficient and reliable techniques for detecting globally and applied contrast enhancement, and copy-paste forgery in the digital image Forgery is the process of making, adapting, or imitating objects, statistics, or documents with the intent to deceive for the sake of altering the public perception, or to earn profit by selling the forged item. Copies, studio replicas, and reproductions are not considered forgeries, though they may later become forgeries through knowing and willful misrepresentations. Forging money or currency is more often called counterfeiting. But consumer goods may also be counterfeits if they are not manufactured or produced by the designated manufacturer or producer given on the label or flagged by the trademark symbol. When the object forged is a record or document it is often called a false document. Art forgery is the creating and selling of works of art which are falsely credited to other, usually more famous artists. Art forgery can be extremely lucrative, but modern dating and analysis techniques have made the identification of forged artwork much simpler. Today, almost everyone has a digital camera. Literally billions of digital images are taken. Some of these images are used for purposes other than family photo albums or Web site decoration.

With the rise in digital photography, manufacturers of graphic editing tools are quickly gathering momentum. The tools are becoming cheaper and easier to use—so easy in fact that anyone can use them to enhance their images. Editing or post-processing, if done properly, can greatly enhance the appearance of the picture, increase its impact to the viewer and better convey the artist's message. But at what point does a documentary photograph become a fictional work of art? While editing pictures is okay for most purposes, certain types of photographs should never be manipulated. Digital pictures are routinely handed to news editors as part of event coverage. Digital pictures are presented to courts as evidence. For news coverage, certain types of alterations or modifications (such as cropping, straightening verticals, adjusting colors and gamma, etc.) may or may not be acceptable. Images presented as court evidence must not be manipulated in any way; otherwise they lose credibility as acceptable evidence.

Today's powerful graphical editors and sophisticated image manipulation techniques make it extremely easy to modify original images in such a way that any alterations are impossible to detect by an untrained eye, and can even escape the scrutiny of experienced editors of reputable news media. Even the eye of a highly competent forensic expert can miss certain signs of a fake, potentially allowing forged (altered) images to be accepted as court evidence.

2. Related Works

G. Cao, Y. Zhao, R. Ni and X. Li, With the rapid development of digital media editing techniques, digital image manipulation becomes rather convenient and easy. While it benefits to legal image processing, malicious users might use such innocent manipulations to tamper digital photograph images. Currently, image forgeries are widespread on the Internet and other security-related applications such as surveillance and recognition that utilize images are therefore impacted. The event and scene information delivered in images might become no longer believable. In the applications such as law enforcement and news recording, it is also necessary to verify the originality and authenticity of digital images, and make clear the image manipulation history to get more information. To circumvent such a problem, digital forensic techniques have been proposed to blindly verify the integrity and authenticity of digital images [1], [2].

S. Bravo-Solorio, A. K. Nandi Some techniques, based on watermarks or digital signatures have been developed to verify the integrity of digital images. In practice, however, such approaches are limited to controlled environments with especially equipped cameras that generate the authentication information at the time of capturing [2]. This has motivated the study of passive forensic techniques aimed at identifying possible traces of tampering in digital images, in the absence of authentication information generated in advance. Such schemes focus on the detection of inconsistencies in the intrinsic statistics of the images, which can suggest, in some cases very strongly, that an image has been manipulated. In practice, given the plethora of possible manipulations an image may go through, forensic evidence will rely on a diverse set of methods, instead of a single algorithm

M. C. Stamm and K. J. R. Liu, when image processing operations are applied to digital images, they often leave behind distinct traces or intrinsic fingerprints. These intrinsic fingerprints are evidence of image manipulation and can be leveraged to determine which operations were used to modify an image. Digital forensic techniques have been proposed to identify several forms of image tampering such as double JPEG compression [1], [2] and image rotation and resizing [1]. Other techniques identify image forgeries using device specific fingerprints such as color filter array patterns [3] or noise features [4]. After manipulation has been identified, the next forensic task is to determine as much information as possible about the unaltered image and the operation used to modify it.

M. Stamm and K. R. Liu, Blind forensic methods, or methods that make no use of outside information about an image or its history, provide a solution to this problem. These methods operate under the premise that the only information available is the image of unknown authenticity itself [2]. Evidence of image alterations can be gathered by modeling intrinsic properties of an image, then using these properties to identify tampering. Similarly, a detection scheme can be designed by identifying traceable statistical

A. Global Contrast Enhancement Detection

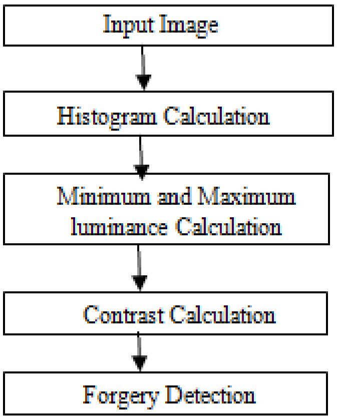

Figure 1: flowchart of global contrast enhancement detection algorithm

1: Calculate the histogram of input image.
2: Minimum and Maximum luminance calculation

artifacts left behind by an image altering operation. In order to determine if an image has undergone any form of alteration, the use of a wide variety of operations must be tested for. Existing image forensics work has dealt with the detection of resampling [3] [2], luminance nonlinearities [2], and the tracing of an image's compression history [4] [5]. In addition, methods have been proposed to detect the use of a tamper filter, as well as estimate its coefficients by exploiting properties of color filter array interpolation [6] [7]. While the parameterization of gamma correction has been studied in [2] and [8], a detection scheme is not fully developed and tested. Furthermore, no prior work has addressed the problem of blindly detecting more general contrast enhancement operations.

3. Existing Contrast Enhancement Impact

Histogram of the original image exhibits the smoothness; therefore it doesn't show gap artifacts. So, it is easy to detect the original images due to absence of gap artifacts in the gray level histogram of original image. It can be written as

$$h_{enhanced}(y) = \sum (h_{original}(x).I(m(x) = y))$$

4. Proposed Methodology

In previous methods, contrast enhancement is detected using the peak/gap artifacts that appear in the digital images. In case of post-processing operation such as JPEG compression, this work fails to detect the contrast enhancement in modified images. So, a new algorithm has been proposed to detect the contrast enhancement not only in compressed but also in JPEG compressed images.

In previous work, contrast enhancement is detected using the peak/gap artifacts that appear in the digital images. However, In case of post-processing operation such as JPEG compression, this work fails to detect the contrast enhancement in modified images. So, a new algorithm has been proposed to detect the contrast enhancement not only in uncompressed but also in JPEG compressed images.

3: Calculate Contrast = (Lmax - Lmin) / (Lmax + Lmin)
Where, Lmax = maximum luminance and
Lmin = minimum luminance
4: Forgery detection:
If (contrast! = 1) image is contrast enhanced
Else image is not contrast enhanced.
The contrast in the digital images which we are detecting here
is defined as:
Contrast = (Lmax - Lmin) / (Lmax + Lmin)

B. Copy-paste image forgery detection

There are two approaches of copy-paste image forgery.

1) Using single source image: In copy-paste forgery using single source image, some portion of image is copied and pasted on the another part same source image. This type of forgery basically used to cover the particular image portion.
2) Using two source images: In copy-paste forgery using two source images, a portion of one image is copied and

pasted on another image and then the contrast is adjusted to match the lighting conditions

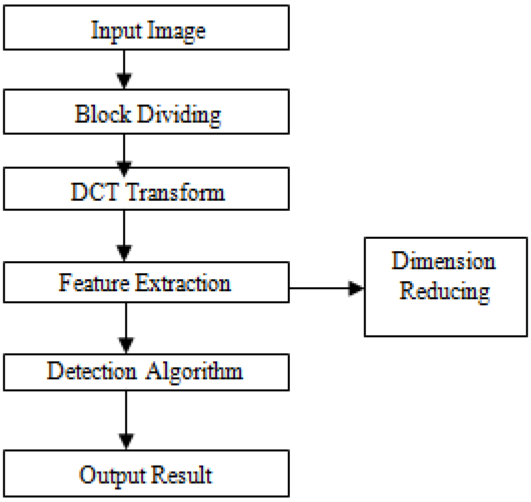

Figure 2: Flowchart of copy-paste forgery detection algorithm

5. Conclusion

This paper presents algorithms for the detection of global contrast enhancement and copy-paste forgery in digital images. The proposed contrast enhancement detection algorithm is robust against the post processing operation such as JPEG compression. So, the proposed algorithm overcomes the limitations of previous approaches. Also, an efficient algorithm for the detection of copy-paste image forgery is proposed. The algorithm can efficiently detect the large duplicate areas up to block size 64*64.

References

[1] Vincent Christlein,” An Evaluation of Popular Copy-Move Forgery Detection Approaches”, IEEE Transactions On Information Forensics And Security, 2011.

[2] S. Bayram, H.T. Sencar, N. Memon,” An efficient and robust method for detecting copy-move forgery”, in: IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Press, New York, 2009.

[3] Li Jing, and Chao Shao,” Image Copy-Move Forgery Detecting Based on Local Invariant Feature Journal Of Multimedia,Vol.7,No.1, February 2012.

[4] S. Bravo-Solorio, A. K. Nandi, “Exposing Duplicated Regions Affected by Reflection, Rotation and Scaling,” in International Conference on Acoustics, Speech and Signal Processing, May 2011

[5] G. Cao, Y. Zhao, R. Ni and X. Li, “Contrast Enhancement-Based Forensics in Digital Images,” IEEE Trans. Inf. Forensics Security, Mar. 2014.

[6] G. Cao, Y. Zhao, and R. Ni, “Forensic estimation of gamma correction in digital images,” in Proc. 17th IEEE Int. Conf. Image Process..Hong Kong, 2010, pp. 2097–2100.

Author Profile

Deepak Waghchaure received the B.E. degree in Computer Engineering from K.K.Wagh Enggineering College, Nashik in 2013. He is currently pursuing Master’s Degree in Computer.

Ashish Gaikwad is student in Sanjivani college of Engneering, Kopargon