National Journal of Advanced Research
ISSN: 2455-216X; Impact Factor: RJIF 5.12
Received: 25-11-2018; Accepted: 26-12-2018
www.allnationaljournal.com
Volume 5; Issue 1; January 2019; Page No. 28-29

Detection technique for the gif forgery image

Prakash Dangi[1], Neha Gopaliya[2], Aditya Narayan[3]
[1-3] Department CSE, Mitrc, Alwar, Rajasthan, India

Abstract
In the recent years, forgeries have a challenge in every digital image aspect. In this paper, we propose an algorithm for digital image forgery for joint photographic experts group (JPEG). The aim is to capture the GIF forged image using original image. Predominately existing work focus only JPEG image. Our target is to propose a generalised algorithm of forgery image that separates the original and forged image cue to contribution in digital image processing. This work surpasses all the literature work as a point of forgery in both types' images. At the end, the experimental setup results ensure that validate of the design approach. The robustness of algorithm of digital image forgery is tested on MATLAB R2015a (64bit) tool.

Keywords: forensics, forged image, Euclidean, compression, scaling, JPEG, GIF

Introduction
The digital image is 2D in x and y spatial plane. The intensity of the image at any point is determined by spatial coordinate [1]. In this regard, capture, modify, compression, and generation operations are performed by converting the image into digital numbers such as 0s and 1s known as bits. The digital image is composed of a finite number of pixels. The size of the standard image, 1024x1024 pixel and 256 type colours are required 3MB of space in the RAM memory [2, 3]. Moreover, colours type image is required more size in RAM memory. In the digital world, cameras are utilised for video and image capture. In contrast to bright light, the camera's videos and images have saturation level is high. Consequently, when the dark light is saturation level is low. The saturation level lies between high and low when the light level is maintained [4]. The image processing technique is highly used in such areas as biomedical, satellite, communication, electronics etc. In all these areas image features like compression, enhancement, and compression are an open area of research, but all these features challenging task is forgeries phenomena happen [5, 6]. In a more formal way, forgeries image can be categories into two parts such as analogue and digital [7]. In the type of analogue image the continuous signal treated, whereas digital type image has discontinuous signal treated. In fact, the digital image is popular nowadays in terms of quality of the image [8, 9]. The digital forgeries technique is a most used area of current research [10]. The digital type forgery is most active research field with many benefits and threats with the consideration of complexity in the objective.

Contribution
In this paper, we proposed the work for forged image for a GIF format. Our works only on few steps to capture the forgery image. Our proposed work are designed to handle GIF images the steps such as:

1. Compare
2. Marking
3. Extraction
4. Dark spot on forgery part

Each step has introduced as pseudocode for automatic verification to our target achieve. The pseudo code steps of this forgery are processed in MATLAB R2015a (64bit) tool. Where the outputs are evaluated using original and forged image.

Existing work on digital image forgeries
Existing research background on digital image forgeries is showed in this section which is essential to the readability of the proposed work. The challenging task on image forgeries is how to check that intellectual quality in the digital image from an authentic point of view. In most of the case, intellectual images assets are original demanded i.e unforged image. In digital world uncertainties about ethical, and validity issues in digital forgeries are challenging task. The need for prominent algorithm to identify the unforged digital image is more vital than ever. Less amount of article reported in existing literature on forgery capture with the standardised algorithm. The open research is how to recognised the fraud image on digital assets. In this way, visual image clarity is not altered for identifying the forged elements in the image. In 2010, E. Ardizzone *et al.* introduced forgeries capture using SIFT point matching. This forgeries capture algorithm is based on JPEG but is not for GIF image. Jessica Fridrich *et al.* introduce the digital image forgery by copy move attack. This methodology is based on exact match and robust match. Hwei-Jen lin *et al*. presented fast copy-move forgery detection [5]. Sevinc Bayram *et al.* presented a survey regarding copy-move forgery detection technique as well as matching duplication blocks and performance results table in the forged image

The proposed work
There is a two image required first: original image and second: forged image, i.e., two images are first converted into red-green- blue (RGB) to gray. However, the subtraction operation is performed for the extra and missing elements in the objective of unforged image. If there are no subtraction operation loop is reset and again process the subtraction operation. After the Marking of the connected components operation is performed. Next step is the extract the

component that large size; consequently, the extra part marked black.

Conclusions

Image forgery of the GIF image is challenging task in recent research. Based on the work the forgery GIF detection is presented in this paper. As an algorithm, the authenticity of the image is performed on MATLAB R2015a (64bit) simulation tool. Thus the problem of digital forgery is finally tracked in this work. Initially, in this work, we have shown a pseudo-code of various elements in original GIF forgery image. After the search approach by our proposed work, we capture both the original and forged GIF image. Therefore the robust technique is on time-based, which is few second.

References

1. Edoardo Ardizzone, Alessandro Bruno, Giuseppe Mazzola. Detecting multiple copies in tampered images. 17th IEEE International Conference on Image Processing (ICIP), 2010, 2117-2120.
2. Husrev Sencar T, Nasir Memon. Overview of state-of-the-art in digital image forensics. Algorithms, Architectures and Information Systems Security. 2008; 3:325-348.
3. Guohui Li, Qiong Wu, Dan Tu, Shaojie Sun. A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. IEEE International Conference on Multimedia and Expo, 2007, 1750-1753.
4. Hailing Huang, Weiqiang Guo, Yu Zhang. Detection of copy-move forgery in digital images using SIFT algorithm. IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application. 2008; 2:272-276.
5. Hwei-Jen Lin, Chun-Wei Wang, Yang-Ta Kao. Fast copy-move forgery detection. WSEAS Transactions on Signal Processing. 2009; 5(5):188-197.
6. Kuo-ming Hung, Ching-tang Hsieh, Kuan-ting Yeh. Multi-Purpose Watermarking Schemes for Color Halftone Image Based on Wavelet and Zernike Transform. In WSEAS Transaction on Computer. 2007.
7. Phen Lan Lin, Chung-Kai Hsieh, Po-Whei Huang. A hierarchical digital watermarking method for image tamper detection and recovery. Pattern recognition. 2005; 3812:2519-2529.
8. Alin Popescu C, Hany Farid. Exposing digital forgeries by detecting traces of resampling. IEEE Transactions on signal processing. 2005; 53(2):758-767.
9. Wei Zhou, Chandra Kambhamettu. Estimation of illuminant direction and intensity of multiple light sources. In European conference on computer vision Springer Berlin Heidelberg, 2002, 206-220.
10. Alin Popescu C, Hany arid F. Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing. 2005; 53(10):3948-3959.