IJournals International Journal of Social Relevance & Concern
ISSN No: 2347-9698 Volume 2 Issue 10, October-2014

Analysis of digital images for detection of tampering

Author: Preeti[1]; M.K. Mishra[2]; A.K. Gupta[3]; Chetan Sikka[4]; Afreen Tarannum[5]

Department of Forensic Science
Sam Higginbottom Institute of Agriculture, Technology & Sciences,
Deemed to be University, Allahabad, Uttar Pradesh,

E-mail: pmpreetimz@gmail.com[1]; munish_eureca@yahoo.com[2];

chetansikka24@gmail.com[4]

ABSTRACT

The increasing availability of low cost and sometimes easily available image editing software such as Photoshop, Corel Paint Shop, PhotoScape, Photo Plus, GIMP and Pixelmator have made the tampering of digital images even more easier and has become common practice. Tampered images are frequently found in criminal and civil cases. Tampered image generally found in case of fake evidence, social sites, porn sites etc. There are many images editing software which are used by forgers which affect the society and also court justice. The present study deals with 24 image samples, collected for analysis of digital images for detection of tampering. Out of 24 images 12 were original images and 12 tampered images which were edited by image editing software.

Analysis of image tampering was performed by using Belkasoft Forgery Detection Plugin. This work is focused on the software detects tampered images automatically, concise reporting, makes experts work easier, fast batch processing and supports about 3,000+ camera models. Altered, modified or re-saved images are detected with extreme reliability.

Keywords

Digital image, Tampering, Pixel, Forgery

1. INTRODUCTION

Images have always played an important role in forensic science and normally refer to photos or digitally stored images. An image can be defined as a 'visually recognizable pattern'. Or "An image is an optical representation of an object produced by light rays from the object being refracted or reflected by a lens or mirror." The most powerful and trust worthy media of expression now a days is photographs. These have been expected as evidence in varied field such as journalism, forensic investigations, military intelligences, scientific research and publications, crime detection and legal proceedings, investigation of insurance claims, medical imaging etc. [2].

Today, digital images have completely replaced the conventional photographs from every sphere of life but unfortunately, they seldom enjoy the credibility of their conventional counterparts. A digital image is a numeric representation (normally binary) of a two-dimensional image. It may be of vector or raster type depending if the image resolution is fixed [4] [7]. By itself, the term "digital image" usually refers to raster images or bitmapped images. All digital images have some individual signature components like

thumbnail, image compression, and resolution and Exif data.

The main multimedia forensics topic is image tampering detection that is assessing the authenticity of a digital image [1], [6]. Tampering is making false attachment to an image. Taken for granted if forger want to change the head of a person and fit another person's head then it is called as tampering. Modifying a digital image to change the meaning of what is represented in it can be crucial when used in a court of law where images are presented as basic evidence to influence the judgment. It is interesting, to establish that something has been manipulated, and to understand exactly what happened: if an object or a person has been covered, if a some part of the image has been cloned, if something has been copied from another image or if a combination of these processes has been carried out.

Image tampering is also known as image forgery. Image forgery is classified in to two categories: The image forgeries include images tampered by copying one area in an image and pasting it on to another area. It is called as Copy-Move Forgery. It is also known as cloning.

The forgeries is copying areas from one or more images and pasting on to an image being forged. It is called as Copy-Create Image Forgery [3].

The image processing community formally refers to this type of image as an image "composition," which is defined as the "digitally manipulated combination of at least two source images to produce an integrated result".

Digital images can be easily Manipulated and altered with the advent of low-cost and high-resolution digital cameras, and sophisticated editing software [5]. The increasing availability of low cost and sometimes easily available image editing software such as Photoshop, Corel Paint Shop, PhotoScape, Photo Plus, GIMP and Pixelmator have made the tampering of digital images even more easier and a common practice.

Photo shopping is a neologism for the digital editing of photos. The term originates from Adobe Photoshop, most commonly image editor used by professionals for this purpose ,many other image editing programs can be used . Tampered image is frequently found in criminal and civil cases. Tampered image generally found in case of fake evidence, social sites, porn sites etc.

Now a day's pressure are exerting on advertisers by governments, and are starting to ban photos that are too airbrushed and edited. The US is also moving in the direction of banning excessive photo manipulation where a Cover Girl model's ad, leading to a misleading representation of the product was banned due to its exaggerated effects.

2. METHODOLOGY

The image samples were collected by using digital camera memory card with write blocker. It does not allow change to a drive that contains image (evidence). After the analysis of original image some tampering has been done in the image using image editing software adobe Photoshop and analysed. Analysis of image tampering was performed by using Belkasoft Forgery Detection Plug-in software. Tampered images were detected on the basis of individual signature components thumbnail, compression, resolution and Exif. Thumbnail is reduced size versions of images used to help in recognizing and organizing them. Image compression is minimizing the size in bytes of a graphics file without degrading the quality of the image to an unacceptable level. Resolution of an image is the detail an image holds. Refers to the sharpness and clarity of an image. Exif (Exchangeable image file format) is a standard that specifies the formats. The probability of an image being forged or genuine is reported on a numeric scale of 1 to 100. Allows processing hundreds of images in a matter of minute. Belkasoft Forgery Detection. Plug-in supports about 3000+ camera models. After the analysis of original and tampered image the result of original image has

been compared with the result of tampered image and verified the difference between the signatures of both images.

3. RESULT AND DISCUSSSION

Table 1. Table shows result of the analysis of images by using Belkasoft :-

S.NO.	Signature components of Original Images	Signature Components of Tampered Images
Sample 1	Matched	Not Matched
Sample 2	Matched	Not Matched
Sample 3	Matched	Not Matched
Sample 4	Matched	Not Matched
Sample 5	Matched	Not Matched
Sample 6	Matched	Not Matched
Sample 7	Matched	Not Matched
Sample 8	Matched	Not Matched
Sample 9	Matched	Not Matched
Sample 10	Matched	Not Matched
Sample 11	Matched	Not Matched
Sample 12	Matched	Not Matched

4. DISCUSSION

Present studies carried out on were the concept validation and verification of software with particular respect to digital forensic tool.

The image was analysed for certain specific key words and results were reported under the page no.4. The analysed images shows the report which would help in the investigation of cases where the image was asked to be original or tampered for investigation purposes.

Under the study, it is observed that images can analyse, if original image was not available. This could be analysed by the use of Belkasoft forgery detection software on the basis of individual signature components or metadata. If signature components were matched with the record of 3000+ camera which is stored in belkasoft it shows image is not modified and if not matched shows modified image. The software is able to tell that the image was in fact modified in some graphic editing software, but it is unable to detect the exact location of foreign objects. This is a limiting factor for software and it needs to be considered for the on-going development of software.

5. SUMMARY AND CONCLUSION

Digital images are submitted as court evidence original or forged, altered or modified. There are many images editing software which is used by forger which affected the society and also court justice. Therefore, the focal point of this work is detection of altered, modified and forged images by using automatic tool Belkasoft forgery detection plug-in.

The forgery detection plug-in can reliably detect forged and tampered photos among the thousands of files available on a computer. The present study deals with 12 image samples, collected for analysis of digital images for detection of tampering. In the work 12 original and known tampered image sample were taken and analysed through the belkasoft forgery detection plug-in. After the analysis create an analysis report of original and tampered image sample which shows all individual signature components (thumbnail, compression, resolution, Exif tag) of original image were matched from the record of Belkasoft forgery detection plug-in and tampered images individual signature components were not matched. The probability of an image being forged or genuine is reported on a numeric scale of 1-100. The results of the work concluded that the Belkasoft forgery detection plug-in is a comprehensive software solution implementing algorithm based on statistical

analysis of information available in digital images. It detects tampered images automatically, concise reporting, makes expert work easier, fast batch processing and supports about 3,000+ camera models. Altered, modified and re-saved images are detected with extreme reliability.

The belkasoft forgery detection plug-in is able to tell that the image was in fact modified in some graphic editing software, but it is unable to detect the exact location of foreign objects. Our thanks to the experts who have contributed towards development of the template.

6. REFERENCES

[1] Farid, H. (2009) "A survey of image forgery detection", IEEE Signal Processing Magazine, vol. 2, pp. 16- 25.

[2] Mishra, M. and Adhikary, M. C. (2013) "Digital image tamper detection techniques- A comprehensive study", International Journal of Computer Science and Business Informatics, vol. 2, pp.1-12.

[3] Murali, S., Anami, B.S. and Chittapur, G. B. (2012) "Comparison and analysis of photo image forgery detection techniques", International Journal on Computational Sciences & Applications, vol. 2, pp.45- 55.

[4] Patel, P.P., Patel, J. and Shah, R. (2014) "3D image generation using interpolation and triangulation methods on ARM-9 processor based single board computer platform", The International Journal of Science and Technoledge, vol. 2, pp. 10-14.

[5] Popescu, A.C. and Farid, H. (2005) "Exposing digital forgeries by detecting traces of re-sampling", IEEE Trans. On Single Processing, vol.53, pp. 758-767.

[6] Sharma, S. and Tuli, P. (2012) "Study and analysis of image reconstruction techniques for fraud and tamper detection in authenticity verification", International Journal of Recent Technology and Engineering, vol. 1, pp. 145- 147.

[7] Yalamali, N. B. and Asuti, M. (2012) " An adaptive image watermarking algorithm based on neutral network", International Journal of Multidisciplinary Educational research, vol.1, pp. 484- 489.