ISSN: 2321-7782 (Online)
Volume 2, Issue 12, December 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

An Image Forgery Technique Having Undetectable Traces by Using Dither

Deepti Ojha[1]
Student M.Tech, (EIC)
AIET,
Lucknow U.P., India

Md.Sanawer Alam[2]
Asst. Prof., (EIC)
AIET
Lucknow, U.P., India

Abstract: ***Image forensic is a field in which the authenticity of an image can be verified along with the traces of image tampering can be detected without the knowledge of any pre-embedded or pre-extracted information. Due to the popularity of this field among researchers and numerous published papers in recent years has put considerable need for a new technique for image forgery, which cannot be detected by existing forensic methods. Due to easy manipulation on digital image along with challenges to detect the original one, a new field of image forensic has attracted many researchers. In this thesis, a new image forgery technique has been discussed.***

Keywords: Image Tampering, DCT, Dither, JPEG compression

I. INTRODUCTION

In early 90's era, it was almost impossible to manipulate digital media, but now with the advancement in the technologies it is not a tough task. The growing demand of digital photography has explored new work in the field of image forensic. Reasons to use the digital image are many; like digital camera that produce immediate images, along with the flexibility to the person for deciding to select the appropriate one without waiting for the development of the film. Also digital images can be stored easily. While considering the originality of the digital image, it is quite difficult for the researcher to decide the authenticity of the image. Due to easy manipulation on digital image along with challenges to detect the original one, a new field of image forensic has attracted many researchers. The most important one is that the existing techniques do not guarantee that new techniques may be designed which can be used to hide the traces of image manipulations.

By analyzing the existing forgery detection techniques, it has been observed that most of the forgery detection techniques are based on the pre processing history of the tampered image. If by any means these history can be hide, then detecting an image tampering would be difficult. The compression history of an image is the basic key of detecting tampering in an image. If a forged image is developed which has no traces of tampering, then detection of such type of tampered image will be almost impossible, because in digital world there is no original image itself.

Consider a situation that the forger already tried to remove the artifacts of compression or recompression. The forensic experts can easily find it with the help of existing techniques such as Quantizer estimation, jpeg detection [1][2].It is useful when image processing unit receives the compression details and quantization table used for processing and compression. Some of the existing techniques like detection of blocking signature, estimation of quantization table, allows to find the mismatches[3][4] and forgeries in JPEG blocks by finding the evidences of compression[5] .To solve the problems with the field of image forensics the researchers need to develop tools that are capable of fooling the existing methodologies[6]. Even though the existing techniques have many advantages they have some limitations too.

II. PROPOSED METHOD

The main drawback of existing techniques is that they do not report for the risk that new techniques may be designed and used to conceal the traces of manipulations. It calls into question the soundness of result of detection techniques representing the nonexistence of image tampering. As mentioned earlier it may be possible for an image forger to generate undetectable compression and other image forgeries. As a result, several existing techniques may contain unknown vulnerabilities [7][8].

Most of them are used to find the compression history such as JPEG detection, quantization table estimation [9]. JPEG compression history of an image deliver the information about the camera used to produce an image, and it can be used to discover forged areas within picture[10][11].Therefore it is used as evidence of image manipulation. When images go through JPEG compression it will create some quantization coefficients as proof of compression [12].

The main idea for this research came from the following observations:

Nowadays digital image are the most popular for sharing visual information. Image produced by the digital camera are instant. These images do not require film developing process. They are easy to store. They don't require physical space for storage. Within few seconds these images can be transferred with the help of electronic media for sharing information. In the case of digital image, authentication is not easy, because as compared with the conventional image editing a digital image is very simple. That is manipulating a digital image is very simple. Detection of image tampering is not an easy task. Image processing type of digital image may vary as per the available software.e.g. JPEG and bitmap. When digital images are used in bitmap format they need to be used without any information of past processing. In many cases the image that is used for processing have been already processed or compressed but there will not be any exclusive information about that. To know about the past processing information it is desirable to know the artifacts of image. Even though available forensic techniques are capable of finding the earlier processing information, a person with good knowledge in image processing can do undetectable manipulations.

Therefore forensic researchers need to examine the authenticity of images to find how much trust can be put on the available techniques. It is also desirable to find the drawbacks of these techniques.

For this purpose researchers have to develop both forensic and anti-forensic techniques to understand the weaknesses. As mentioned earlier most of the existing techniques are created for finding the processing history, especially the compression history. Even though the existing techniques have many advantages they have some limitations too. The main drawback of these techniques is that they do not report for the risk that new techniques may be designed and used to conceal the traces of manipulations. It calls into question the soundness of result of detection techniques representing the nonexistence of image tampering. As mentioned earlier it may be possible for an image forger to generate undetectable compression and other image forgeries.

As per the knowledge in the field of image forgery, little research has been done. With the help of the proposed technique, almost all forgery detection techniques can be fooled .Reason behind this is most of the forgery detection techniques are based on image compression history. Since this technique is able to hide traces of compression and filtering, there are no traces of processing history in the forged image.

The entire concept of the proposed method can be described as follows.

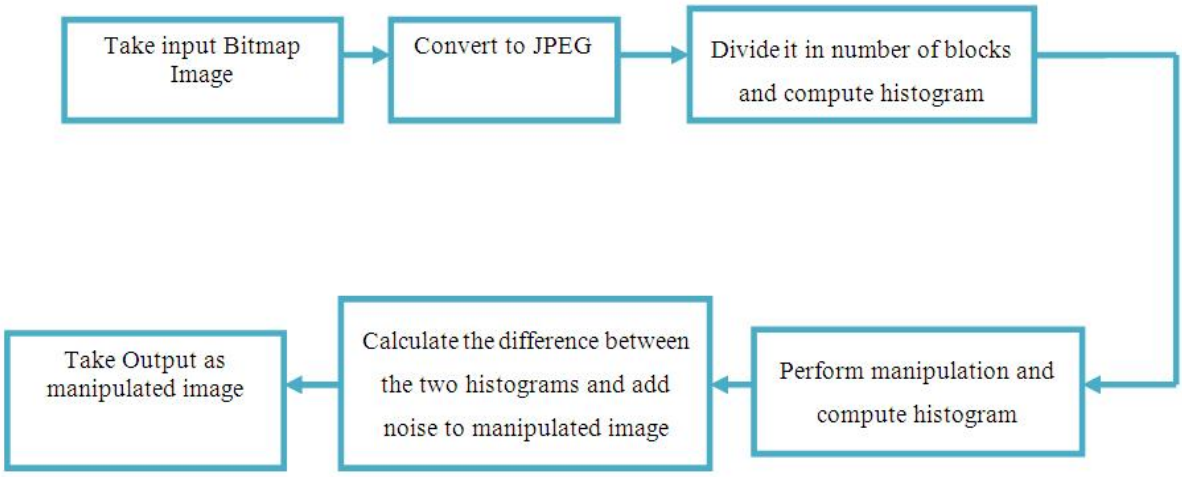

Figure 1: Block Diagram of Proposed Method

The image compression techniques are basically classified into two types namely lossy and lossless compression. In lossy image compression 2-D transformation techniques like discrete cosine transform (DCT) or discrete wavelet transforms (DWT). For conversion of bitmap image to JPEG, DCT is used in this method. After dividing the image into blocks, transform coefficients have been obtained, which is quantized further in the binary form. While reconstructing the image, the binary values are dequantized, which is not the inverse of quantization. Further IDCT has been performed for reconstructing the image. During image compression, some evidence of compression is left behind. There will be a uniform distribution among pixels for an unprocessed image. These distributions got disturbed at the time of compression, which act as an evidence of forgery. In the proposed technique, these deviations are calculated and further added to the forged image. For the other case that is when image was segmented, the above stated process is repeated for all segments. After that they are joined together[13]. The main drawback of existing techniques is that they do not account for the statistical values an image have. Therefore hiding statistical values of these traces will help forger to perform undetectable tampering[14]..

III. Result and Discussion

The proposed technique is applied to Lena image of size 256 KB. The results are discussed here. The Figure 2 shows the Lena image before and after applying the technique. The Figure 2(a) represents the original bitmap image taken as input. First we convert this image into jpeg image and then analyze the coefficients and find the values. The Figure 2 (b) represents the histogram of the original bitmap image. The Figure 2(c) represents the converted JPEG image and 2(d) its histogram. Figure 2 (e) is the reconstructed image and figure 2(f) is its histogram. Histogram of (c) and (e) are compared and the difference among each block of both images have been calculated.

Using the value calculate the noise D and which is added to the manipulated image so that the coefficient values will match with the estimated one. Then apply some quality improvement techniques to improve the quality if needed. Finally the modified image is obtained in figure 2(f). The image (f) shows the final output, and from that it is clear that there is no noticeable difference between the input image and the resulting image.

From the result it is very clear that just by observing the images, forgery cannot be detected. Since the forged image has no traces of forgery (filtering and compression), also the PSNR and size of both the images are exactly same. Hence forgery cannot be detected. Since there is no original image itself in digital media, the forged image will appear as the original image.

Figure: 2(a) Original bitmap image

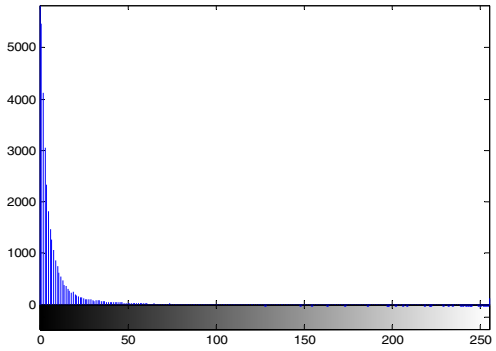

Figure: 2(b) Histogram of Original bitmap image

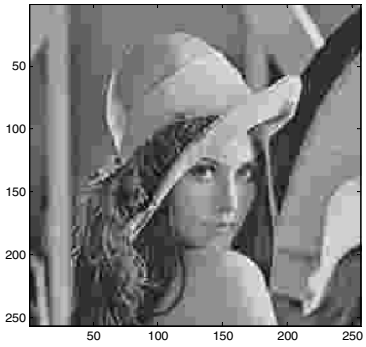

Figure: 2(c) JPEG lena image

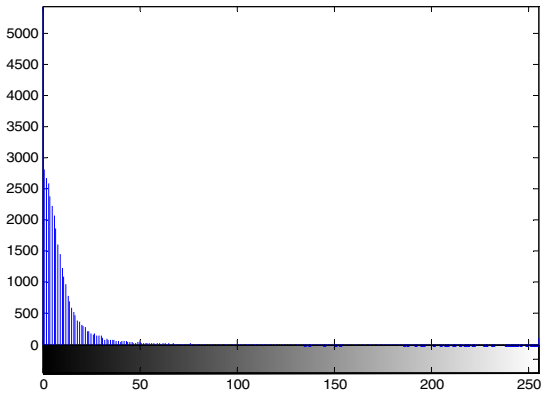

Figure: 2(d) Histogram of JPEG lena image

Figure: 2(e) Modified JPEG lena image

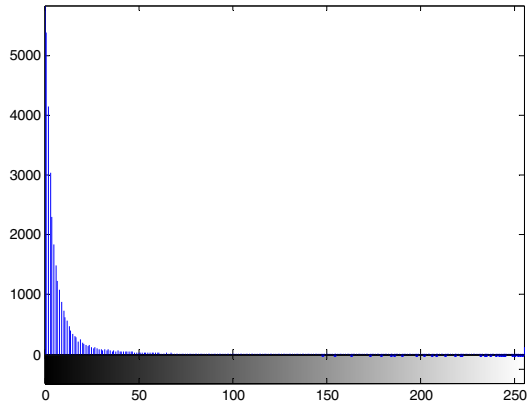

Figure: 2(f) Histogram of modified JPEG lena image

Figure: 2(g) Manipulated image

Table 1: Simulation Result

Image	Size	PSNR	MSE
Original lena image	256 KB	25.74	174.96
Modified lena image	256 KB	25.74	174.73

IV. CONCLUSION

The implemented forgery technique shows that the evidence of forgery can be hide, through which the compression history and filtering traces can be removed. These evidences are the basic key for forgery detection. By analyzing the distribution coefficients of DCT before compression and the transform coefficients of DCT after compression, the difference between these two can be find out. Further by adding these deviations to the forged image, compression traces can be removed. It has been found by seeing the result that the technique is a reliable one. The key feature of this technique is it is able to hide the evidences of compression. This work can be extended for hiding signature evidences produced while enhancing the image.

References

1. Avcibas, S. Bayram, N.Memon, M. Ramkumar, and B. Sankur,"A classifier design for detecting image manipulations," in Proc. IEEE Int. Conf. Image Process., Oct. 2004, vol. 4, pp. 2645–2648.
2. J. He, Z. Lin, L.Wang, and X. Tang, "Detecing doctored JPEG images via DCT coefficient analysis," in Proc. Eur. Conf. Computer Vision,May 2006, vol. 3593, pp. 423–435.
3. M. Chen, J. Fridrich, M. Goljan, and J. Luka˘s, "Determining image origin and integrity using sensor noise," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 74–90, Mar. 2008.
4. W. S. Lin, S. K. Tjoa, H. V. Zhao, and K . J. R. Liu, "Digital image source coder forensics via intrinsic fingerprints," IEEE Trans. Inf.Forensics Security, vol. 4, no. 3, 2009. , pp. 460–475, Sep.
5. Z. Fan and R. Eschbach, "JPEG decompression with reduced artifacts," in Proc. IS&T/SPIE Symposium. Electronic Imaging: Image and Video Compression, San Jose, CA, Feb. 1994.
6. Mathew C.Stamm and K.J.Ray Liu," Anti -Forensic of Digital Image Compression", IEEE Transaction on Information forensics And security, Vol.6, No.3, Septe mber2011.
7. R. Rosenholtz and A. Zakhor, "Iterative procedures for reduction of blocking effects in transform imag ge coding," IEEE Transsactions Circuits Syst.Video Technol., Mar. 1992. vol. 2, pp. 91–94
8. Z. Fan and F. Li, "Reducing artifacts in JPEG decompression by\ segmentation and smoothing," in Proc. IEEE Int. Conf. Image Processing,vol. II, 1996, pp. 17–20.
9. Weiqi Luo, Jiwu Huang and Guoping Analysis and Its Applications to Digital Image Forensics", IEEE Trans. Inf. Forensi no. 3, Sep. 2010.
10. M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," IEEE Trans Inf. Forensics Security, vol. 5, no. 3, pp. 492–506, Sep. 2010.
11. W. Pennebaker and J. Mitchell, JPEG: Still Image Data Compression Standard. New York: Van Nostrand Reinhold, 1993.
12. Luo, C.W. Chen, K. J. Parker, and T. S Huang, "Artifact reduction in low bit rate DCT-based image compression," IEEE Trans. Image Processing, vol. 5, pp. 1363–168, 1996.

.13. Mathew C.Stamm and K.J.Ray Liu," Anti Forensic of Digital Image Compression", IEEE Transaction on Information forensics And security, Vol.6, No.3, September 2011

14. Athira B.Kaimal, Dr.S.manimurugan,and J. Anitha," A modified anti-forensic technique for removing detectable traces from digital images," International Conference on Computer Communication and Informatics (ICCCI -2013), Jan. 04– 06, 2013, Coimbatore, INDIA

