IOSR Journal of Computer Engineering (IOSRJCE)
ISSN: 2278-0661 Volume 5, Issue 1 (Sep-Oct. 2012), PP 01-05
www.iosrjournals.org

A Tailored Anti-Forensic Approach for Bitmap Compression in Medical Images

Manimurugan.S[1], Athira B.Kaimal[2]
[1,2]*computer science and engineering, Karunya University,india*

Abstract: *Medical imaging is the technique and process used to create images of the human body for clinical purposes or medical science.Image processing has now become a significant component in almost all the areas. But storing medical images in a safe and sound way has become very complicated. Processing of such images should be carried out without knowledge of past processing on that image. Even though many image tampering detection techniques are available, the number of image forgeries is increasing. In this paper, a new approach is designed to prevent the medical image compression history. Then it also explains how this can be used to perform unnoticeable forgeries on the medical images. It can be done by the estimation, examination and alteration in the transform coefficients of image. The existing methods for identification of compression history are JPEG detection and Quantizer estimation. The JPEG detection is used to find whether the image has been previously compressed. But the proposed method indicates that proper addition of noise to an image's transform coefficients can adequately eliminate quantization artifacts which act as indicators of JPEG compression. Using the proposed technique the modified image will appear to have never been compressed. Therefore this technique can be used to cover the history of operations performed on the image and there by rendering several forms of image tampering.*

Keywords: *JPEG compression, Image history, Image coefficients, Digital forensics, Anti-forensics, medical imaging*

I. Introduction

Medical imaging is the technique and process used to create images of the human body (or parts and function thereof) for clinical purposes (medical procedures seeking to reveal, diagnose, or examine disease) or medical science (including the study of normal anatomy and physiology). Although imaging of removed organs and tissues can be performed for medical reasons, such procedures are not usually referred to as medical imaging, but rather are a part of pathology. Measurement and recording techniques which are not primarily designed to produce images, such as electroencephalography (EEG),electrocardiography (EKG),and others, but which produce data susceptible to be represented as maps (i.e., containing positional information), can be seen as forms of medical imaging.

Up until 2010, 5 billion medical imaging studies had been conducted worldwide. Radiation exposure from medical imaging in 2006 made up about 50% of total ionizing radiation exposure in the United States. In the clinical context, "invisible light" medical imaging is generally equated to radiology or "clinical imaging" and the medical practitioner responsible for interpreting (and sometimes acquiring) the images is a radiologist. "Visible light" medical imaging involves digital video or still pictures that can be seen without special equipment. Dermatology and wound care are two modalities that utilize visible light imagery. Diagnosticradiography designates the technical aspects of medical imaging and in particular the acquisition of medical images. The *radiographer* or *radiologic technologist* is usually responsible for acquiring medical images of diagnostic quality, although some radiological interventions are performed byradiologists. While radiology is an evaluation of anatomy, nuclear medicine provides functional assessment.As a field of scientific investigation, medical imaging constitutes a sub-discipline of biomedical engineering, medical physics or medicinedepending on the context: Research and development in the area of instrumentation, image acquisition (e.g. radiography), modeling and quantification are usually the preserve of biomedical engineering, medical physics, and computer science; Research into the application and interpretation of medical images is usually the preserve of radiology and the medical sub-discipline relevant to medical condition or area of medical science(neuroscience, cardiology, psychiatry, psychology, etc.) under investigation. Many of the techniques developed for medical imaging also havescientific and industrial applications.

Medical imaging is often perceived to designate the set of techniques that noninvasively produce images of the internal aspect of the body. In this restricted sense, medical imaging can be seen as the solution of mathematical inverse problems. This means that cause (the properties of living tissue) is inferred from effect (the observed signal). In the case of ultrasonography the probe consists of ultrasonic pressure waves and echoes inside the tissue show the internal structure. In the case of projection radiography, the probe is X-ray radiation which is absorbed at different rates in different tissue types such as bone, muscle and fat.[27]

In some situations, medical images are processed as bitmaps without any information of former processing. It typically happens when image data is used as a bitmap without other information. The image may have been already processed and compressed. But they may not be visually detectable. The images that are usually stored as raster as they contain so much complex information that trying to store them as vector would be unreasonably complex. If one wants to ensure that image is rendered it is enviable to realize the artifacts the image might have, i.e., it is desirable to know a bit of the image's "history." Techniques are available to detect manipulations of bitmap images and these make use of the transformation and other coefficient of images [1][21][23].. It will help to find the prior processing informations.But if a forger with good knowledge in the image processing and signal processing area can hide the evidence of compressions and other tampering. Since images have become an important part of visual communication it is important to examine how much we can trust on the available detection techniques and what all are the weaknesses .To examine the efficiency and to prevent the manipulations of raster bitmap images many techniques are developed by researchers. These techniques are designed to determine a bitmap images compression history. When the image processing units inherit images in raster bitmap format the processing is to be carried without knowledge of past operations that may compromise image quality (e.g., compression). To carry further processing, it is useful to not only know whether the image has been previously JPEG compressed, but to learn what quantization table was used. Consider the case, if one wants to remove JPEG artifacts or for JPEG re-compression, the existing techniques show it can be detected through JPEG detection and Quantizer estimation [1]. To prevent the image forgeries and to detect those researchers have developed a variety of techniques. They states that using the available techniques such as finding blocking signature[1], estimation of quantization table etc, we can find the evidence of JPEG compression [7]and thereby we can identify image forgeries as well as localized mismatches in JPEG block[4][5].

The extensive availability of photo editing software has made it easy to create visually believable digital image forgeries. To deal with this problem, there has been much recent work in the field of digital image forensics. There has been little work, however, in the field of anti-forensics, which seeks to develop a set of techniques designed to fool current forensic methodologies[22].JPEG compression history of an image can be used to provide evidence of image manipulation[24], deliver information about the camera used to produce an image, and discover forged areas within a picture [2].

The proper addition of noise to an image's discrete cosine transform coefficients can sufficiently remove quantization artifacts which act as indicators of JPEG compression while introducing an acceptable level of distortion [3][12][18]. Though many existing JPEG detection techniques are capable of detecting a variety of standard bitmap image manipulations, compression histories etc., they do not account for the possibility that new techniques may be designed and used to hide image manipulation evidences. This is particularly important because it calls into question the validity of results indicating the absence of image tampering. It may be possible for an image forger familiar with signal processing to secretly develop new techniques and use them to create undetectable compression and other image forgeries. As a result, several existing techniques may contain unknown vulnerabilities [14][15].The researchers believe that processing in raster bitmap images will reduce the quality and it can be used as visually identifiable evidence of tampering. But we can develop new techniques which are capable of fooling existing detection methods and capable of improving image quality [3]. Therefore they cannot find any evidence of compression as well as tampering in images[16][17].

II. Proposed Method

To the best of knowledge the prior work for identifying bitmap compression history is JPEG detection and quantization table estimation [1][8].In this paper a set of techniques capable of hiding the compression history and evidences of image manipulations are presented. Since most of the techniques involve analyzing the transform coefficients for the variations and blocking artifacts, this paper propose a new method for removing the detectable traces from images.[19][20] The proposed algorithm can be used to fool most of the existing techniques created for JPEG detection to identify bitmap image compression history. When images undergoes through JPEG compression it will leave some quantization coefficients as evidence [1] [6]. In this paper these are discussed first and then a method is proposed for hiding compression history in the bitmap images

If one want to ensure that the image is rendered, it is desirable to understand the artifacts that images have. It is also desirable to know a bit of image's history. Existing methods says that we can do this by detecting whether the image has ever been compressed using JPEG standard [1]. In this paper a feasible method for applying anti forensic techniques to hide the JPEG detection for identifying compression history is used. The proposed method can be used to hide the evidence of image compression by removing DCT coefficient fingerprints and by removing blocking artifacts of the image [2][8].The first step in the identification of the image's compression history is to identify whether the image has been compressed before or not. But the tailored anti forensic method can show an already compressed image as a never compressed image. Therefore it will not give any evidence of compression. It assumes that if there is no compression the pixel Differences across blocks should be similar to those within blocks. We find the differences using DCT coefficients. Let X represents the blocks of image. For applying our method we need to calculate the coefficients of each block before and after compression. First the image is divided into N number of blocks. For each block X (i, j) we compute the coefficients of blocks and that of pixels in each block. Consider two blocks. Let X1 be the first block and X2 be the second one.

$$X1(i,j)=\{a1,a2,a3,a4\} \qquad (1)$$

$$X2(i,j)=\{b1,b2,b3,b4\} \qquad (2)$$

where {a1,a2,a3,a4} and {b1,b2,b3,b4} are following two set of pixel values The first set represents the pixels inside block X1 and second represents the pixels inside block X2.We have to find the DCT coefficients of these two blocks and given pixels before and after compression. Let D1 represents the set of coefficients before performing compression and let D1' be the set of transform coefficients after transformation or compression. Find the difference between D1 and D1'which is represented as T.

$$T = \sum_{n} \left| D_1(n) - D_1^{'}(n) \right| \qquad (3)$$

When someone try to detect the history of compression this T value is used as the evidence since it shows the difference in coefficient values. Therefore if we are able to hide this difference means we can hide the history of compression and transformations. Using the proposed method we can do this. It is done by adding some noise called tailored dither to the images transform coefficients so that the transform coefficients will match the estimated one. After adding this noise we apply some quality improvement techniques so that the images visual quality of the image will not be affected. Then compression is performed. The final result will be a compressed or forged image with undetectable history of compression and tampering. The proposed technique is explained in the following algorithm

```
Input  :{ image I; stored in raster bitmap format}
Output :{ compressed/forged image with
                    Undetectable Traces}
              Divide image into two blocks
                   I<-X1+X2
                X1<-{a1 a2 a3 a4}
                X2<-{b1 b2 b3 b4}
                Find D1, D1'
                D1<-DCT of X1
                D1'<-DCT of X2
                Calculate T
              T = Σ |D1(n) - D1'(n)|
 Add T+D1' and
Apply quality improvement method
 Perform compression
```

III. Result And Discussion

The proposed approach can be used to hide the compression history and to remove JPEG blocking artifacts without affecting the visual quality. For this the tailored anti-forensic approach is applied to five images. Figure 1 is one of them. It shows the steps to be performed to implement the new technique. Fig1.1 show the original input Lena image and figure 1shows the same image before and after applying tailored anti-forensic technique. The image (a) represents the original image in bitmap format taken as input. First we analyze the coefficients and find the values then image (b) represents the same image after performing some manipulations. After that we are applying compression and analyze the values and find the difference. Using the value the tailored noise is calculated and which is added to the compressed image so that the values will match with the estimated one. Then we apply some quality improvement techniques to improve the quality. The image (d) shows the final output, and there is no noticeable difference between the input image and the resulting image. Similar way the same technique is applied to the other four images also and the results are obtained as shown. It is clear from the images that by just viewing the images nobody can find out any difference.from the original one. That is the images resulted from after applying the proposed technique contains no visual indicators of modification and compression. Since those who want to detect the modifications in the image will not have access to the original image the resulted image cannot be compared against the original one. The modified image will appear as unaltered image.From the resulting images no one can find any difference in the images. But we have to consider the case where forensic techniques are applied for detecting statistical values. As we know the forensic experts can analyze the transform coefficients by comparing the histograms of images. If any difference is found it will be declared as a forged one. Therefore this paper introduces a method to hide the difference between statistical coefficients of histograms of original image and manipulated one. It is capable of fooling forensic researchers. This is done by applying the algorithm explained in the section2 to the image after modification or compression. Since some tailored noise value is added to the modified image to match it with the estimated value there will not be much noticeable difference in the histogram coefficients. To examine the efficiency of the proposed method results are shown in the following figures. The figure 3 shows the histograms of DCT coefficients of uncompressed bitmap images and that of same images after compression and after applying the tailored technique. Analysis of transform coefficients distribution value of the images yields similar results. To verify that the proposed technique can hide the traces of image manipulations the following processing are done on the images.

Table 1. The accuracy of tailored anti-forensic technique on medical images

Input image	**Size of image before processing**	**Size of image after processing**	**PSNR**	**Error Rate**	**Correlation Coefficient**
1	43KB	43.1 KB	68.54	0.0091	0.0932
2	103KB	103.01KB	68.94	0.0083	0.998
3	30KB	30.002KB	68.99	0.0082	0.979
4	289KB	289.2 KB	70.20	0.0062	0.983
5	67KB	67.1 KB	69.32	0.0076	0.964

The medical images store in raster bitmap format are taken as inputs then they are converted in to gray scale images then the coefficient values are identified then the image is compressed using different quality factors. Then the traces of compression is removed by adding some tailored noise to the compressed image and the resulting images are tested using existing detection methods. If no evidence of compression is present then the image is considered as never compressed one. The proposed method is applied on five images and summarized The values indicate that there is not much difference between the values of original images and tampered images. Since we have added some noise to equalize the coefficients there is a slight difference in the size of image but it is negligible.

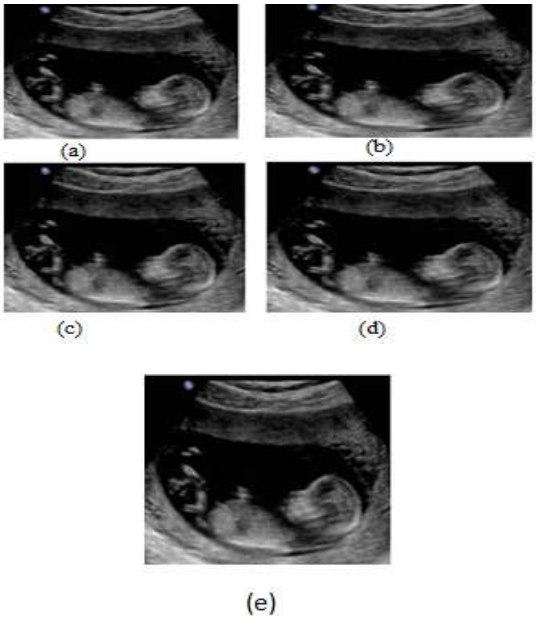

Fig.2 (a)image before compression (b)JPEG compressed image (c)applying tailored method(c)modified image after applying tailored method which appear as unaltered image (e)Original input image

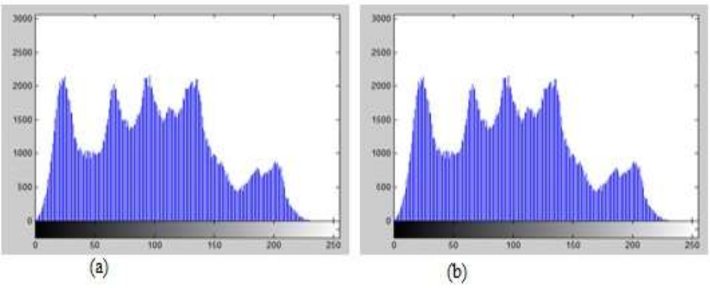

Fig.3.(a)Histogram of original medical image(b)Histogram of modified medical image after applying tailored method

IV. Conclusion

The contribution of this paper is a tailored anti-forensic technique which is capable of fooling forensic algorithms used to detect compression details and other manipulations on medical images stored in raster format images. Here a reliable method for hiding the compression history is presented. To do this first a generalized frame work is created for identifying and removing traces from images transform coefficients. According to this the traces of image manipulation can be removed by estimating the distribution of transform coefficients before compression then adding some noise to the compressed image so that the modified image's coefficient matches the distribution estimated. It is based on the analysis of transform coefficients of images. As the forgeries in medical images can cause unwanted problems in human life it is important to find such forgeries. This paper proposes a new method which challenges existing forensic algorithms.

V. Acknowledgement

We would like to express our gratitude to all those who gave us the possibility to complete this paper.

References

[1]. Z. Fan and R. de Queiroz, "Identification of bitmap compression history:JPEG detection and quantizer estimation,"*IEEE Trans.Image Process*,vol.12, no.2,pp.230–235,Feb. 2003.

[2]. M. Chen, J. Fridrich, M. Goljan, and J. Lukáˇs, "Determining image origin and integrity using sensor noise," *IEEE Trans. Inf. ForensicsSecurity*, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[3]. 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,September2011.

[4]. S. Ye, Q. N. Sun, and E.-C. Chang, "Detecting digital image forgeries by measuring nconsistencies of blocking artifact," in *Proc. IEEE Int.Conf. Multimedia Expo*, 2007, pp. 12–15.

[5]. J. He, Z. Lin, L.Wang, and X. Tang, "Detecting doctored JPEG images via DCT coefficient analysis," in *Proc. Eur. Conf. Computer Vision*,May 2006, vol. 3593, pp. 423–435

[6]. 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, pp. 460–475, Sep. 2009.

[7]. W. Pennebaker and J. Mitchell, *JPEG: Still Image Data Compression Standard*. New York: Van Nostrand Reinhold, 1993.

[8]. M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Undetectable image tampering through JPEG compression anti-forensics," in *Proc.IEEE Int. Conf. Image Process.*, Sep. 2010, pp. 2109–2112.

[9]. M. Chen, J. Fridrich, M. Goljan, and J. Lukáˇs, "Determining image origin and integrity using sensor noise," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[10]. J. Lukáˇs and J. Fridrich, "Estimation of primary quantization matrix in double compressed JPEG images," in *Proc. Digital Forensic Research Workshop*, Aug. 2003, pp. 5–8.

[11]. 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.

[12]. 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.

[13]. W. Pennebaker and J. Mitchell, *JPEG: Still Image Data Compression Standard*. New York: Van Nostrand Reinhold, 1993.

[14]. R. Rosenholtz and A. Zakhor, "Iterative procedures for reduction of blocking effects in transform image coding," *IEEE Trans. Circuits Syst.Video Technol.*, vol. 2, pp. 91–94, Mar. 1992.

[15]. Z. Fan and R. Eschbach, "JPEG decompression with reduced artifacts," in *Proc. IS&T/SPIE Symp. Electronic Imaging: Image and Video Compression*, San Jose, CA, Feb. 1994.

[16]. 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.

[17]. 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. 1363–1368, 1996.

[18]. Chou, M. Crouse, and K. Ramchandran, "A simple algorithm for removing blocking artifacts in block-transform coded images," *IEEE Signal Processing Lett.*, vol. 5, pp. 33–35, Feb. 1998.

[19]. Sir M. Kendall and A. Stuart, *The Advanced Theory of Statistics*. New York: Macmillan, 1977, vol. 2. Independent JPEG Group Library.. [Online]. Available:http://www.ijg.org.

[20]. Swaminathan,M.Wu, and K. J. R. Liu, "Digital image forensics via intrinsic fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 101–117, Mar. 2008.

[21]. Weiqi Luo, Jiwu Huang and Guoping Qiu," JPEG Error Analysis and Its Applications to Digital

[22]. Image Forensics", *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, Sep. 2010.

[23]. http://sig.umd.edu/events/

[24]. http://www.scribd.com

[25]. http://www.docstoc.com/docs/108996696/Advances-in-Digital-Image-Processing-and-Information- Technology

Ms.Athira B.Kaimal received the B.E. degree in computer science and engineering in 2011 from the Anna University, College SSCET.She is currently doing M.Tech Research in the area of Image Processing at the department of Computer Science and Engineering, Karunya Versity

Dr. S. Manimurugan completed his Bachelor's Degree from Anna University and he received his Master's Degree from Karunya University. He was highly commended for his work in Image Processing and Information Security, for which he was honored with a PhD from Anna University