www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 2 February 2015, Page No. 10539-10542

An Efficient Image Forgery Detection Method with Dempster Shefer's Theory for Detecting Jpeg Anti-Forensics

***K.Karthika*[1] *P.Damodharan*[2]**

ME Department Of CSE
Akshaya College Of Engineering & Technology
Kinathukadavu,Coimbatore
sendtokarthika@gmail.com

Associate Professor, Head Of the Department CSE
Akshaya College Of Engineering & Technology
Kinathukadavu,Coimbatore
damodharan@acetcbe.edu.in

ABSTRACT-With rapid development of high-quality cameras and powerful photo-editing tools significantly reduces the difficulty to make visually plausible fake images. The JPEG format is widely used as one of the most popular lossy image compression formats is used by various advanced digital cameras and image editor and processing software tools. Earlier work identified traces of the image JPEG compression history or JPEG anti-forensic processing with reasonable loss of image quality. This aims at removing from a given image the footprints in both the spatial and frequency domain left by JPEG compression. However, efficient forensic Undetectability not obtained. To deal with this problem the present work proposes different forgery detection algorithm such as Ststic image Format Analysis algorithm, lossy compression technique Effect and Place/Transfer Forgery. The result of this algorithm is combined by using Dempster-Shafer combiner which is based on the Dempster-Shafer theory as a framework within which the results of different tools are considered and taken decision. Experimental result of proposed system efficiently detects the Undetectability forgeries when and provides better result when compare with earlier methods.

Keywords: **Digital image forensics,place-transfer forgery,static image Format Analysis algorithm,lossy compression technique Effect.**

1.INTRODUCTION

Digital images are the major source of information in today's digital world. Due the easy way of acquisition and its storage they are the fastest means of information loading. Images can be used as an proof for any cases in the court . The images broadcasted in any television and in newspapers are accepted as the certificate for their trustfulness of their programs. Digital images are being used in many applications ranging from military to medical field to identify the diseases and from art piece to user photography. Therefore digital image forensics emerges as fast growing need of the society. Thus the images are required to be authenticated. Due to technology evolution and availability of low-expensive hardware and software tools it is very easy to make the changes in the digital images without leaving the visible traces of manipulation. It has become toughest to trace these operations. As the problem arises the integrity and authenticity of digital images is lost. This changes in image can be used for some risk purpose like to hide some important trace information from an image. Thus using modified images to convey invalid information. In order to identify the integrity of the images we need to detect any changes present in the image. Digital Image Forensic is that branch on study of science that deals with exposing the fake image manipulation.

2.PROPOSED SYSTEM

The Forgery detection algorithm with Dempster-Shafer theory is proposed for detection of JPEG anti forensic. Forgery detection algorithm such as JPEG Format Analysis algorithm, Double Quantization Effect and Place/Transfer Forgery. The result from these different tools is combined using Dempster-Shafer combiner to produce a better final classification. The Dempster-Shafer combiner is based on the Dempster-Shafer theory. It has been frequently applied to deal with uncertainty management and incomplete reasoning. According to the DS theory, a basic probability assignment can be associated to each tool which describes the subjective degree of confidence attributed to it. Experimental result of proposed system shows better results when compared with the existing one. This system wiil provide the Efficient tradeoff between the forensic Undetectability and the image visual quality is obtained and Sensitive to different properties of images and forgeries has been analysed. Reliability of the each individual forensic tools has been improved. Combination process can take advantage of the specificity of each method.

3. FORGERY CREATION PROCESS

3.1 TV-BASED DEBLOCKING

The first step is TV-based deblocking in the spatial domain. Besides the removal of JPEG blocking artifacts, another purpose of this step is to partly and plausibly fill gaps in the Discrete Cosine Transform histogram, so as to facilitate the following step of explicit histogram smoothing. Experimentally, it is necessary and beneficial to conduct this first-round deblocking, especially for a better histogram restoration in the high frequency subbands where all DCT coefficients are quantized to zero in the JPEG image.

For JPEG deblocking purposes, a variatiotnal approach is used to minimize a TV-based energy consisting of a TV term and a TV-based blocking measurement term.

The final constrained TV-based minimization problem is formulated as follows: where $\alpha > 0$ is a regularization parameter, balancing the two energy terms. It is easy to demonstrate that E(X) is a convex function (though not differentiable) and U is a convex set.

3.2 PERCEPTUAL DCT HISTOGRAM SMOOTHING

After JPEG image J has been processed using the TV-based deblocking method, the gaps in the Discrete Cosine Transform domain have been partly filled in the received image f ˆ_b. The partially recovered information in the Discrete Cosine Transform domain of fˆ_b will help us to build an adaptive local dithering signal model based on both the Laplacian distribution and the uniform distribution for a better goodness-of-fit.

3.3 SECOND-ROUND TV-BASED DEBLOCKING

In the perceptual Discrete Cosine Transform histogram smoothing, although we have tried to modify the Discrete Cosine Transform coefficients while minimizing the spatial-domain distortion, there must be some unnatural noise and blocking artifacts introduced in f ˆ_bq. Since the JPEG blocking artifacts presented in f ˆ_bq are not as serious as those in J , hence we lower the parameters α and t for a milder JPEG deblocking. We set $\alpha = 0.9$, and the step size t = 1/(k + 1) at the k-th iteration. As to the setting of the convex set U, here we set $\mu = 1.5$, which constrains that the processed Discrete Cosine Transform coefficient should stay within the same or the neighbouring quantization bins as its original value. Once a processed coefficient goes outside of the constrained range, the projection operator PU modifies its value back to a random value uniformly distributed in the original quantization bin. This can avoid strong Discrete Cosine Transform histogram shape modification by the TV-based deblocking and prevent the emergence of new Discrete Cosine Transform quantization artifacts.

3.4 DECALIBRATION

For fˆ_bqb all the existing detectors seems to be well fooled except the calibrated feature based detector. In fact the calibrated feature value has also been significantly decreased. However, for genuine, uncompressed images, this feature value is highly condensed in an interval of very small values. It is hard to further decrease this value by performing deblocking, when keeping the best visual quality.

The optimized energy function for decalibration purposes of minimization problem is formulated as: After decalibration the JPEG Forged image has been obtained.

4. FORGERY DETECTION TOOLS JPEG FORMAT ANALYSIS ALGORITHM

4.1 STATIC IMAGE FORMAT ANALYSIS ALGORITHM FOR JPEG IMAGE

The forged image is detected by using tool A called Joint photographic experts group Format Analysis algorithm. Joint photographic experts group is a de-facto standard in digital photographic images. Many of the digital cameras will produce Joint photographic experts group format .The Joint photographic experts group format is an endless source of data that can be used for the purposes of detecting forgery in the images. The Static Image Format Analysis algorithm uses the details stored in the many technical meta-tags available in the commencement of each Joint photographic experts group file. These labels contain information about quantization matrices, Huffman code tables, programming images by implementing less resolution for chroma information , and many other parameters as well as a opera mini version of the complete image. The content and sequence of those label, as well as which particular label is present , depending on the image itself and on the device that captured it or software that modified it. In addition to the system technical information, Joint photographic experts group labels contain important detail about the photo including shooting conditions and parameters. The fundamental analysis method checks the validity of Exchangeable image file format label in the first place in an shot to find discrepancies. This, for example, may contain checks for Exchangeable image file format label additional in post-processing by certain editing tools, checks for date of capturing vs. the date where the last change done, and so on. However, Exchangeable image file format labels can be easily forged; in fact that while we can treat existing Exchangeable image file format discrepancies as a positive sign of an image being altered, the fact that the labels are "in sequence" does not bring any meaningful information. Our solution makes an shot to find out discrepancies between the actual image and available Exchangeable image file format information, comparing the actual Exchangeable image file format label against tags that are typically used by a certain device (one that's mentioned as a capturing tool in the corresponding Exchangeable image file format label). We composed a wide-ranging database of Exchangeable image file format label produced by a broad range of digital cameras including many information about new models as soon as they become available.In addition to Exchangeable image file format analysis, we review quantization tables in all image channels. Most digital cameras feature a restricted set of quantization tables; therefore, we can find out discrepancies by comparing hash tables of the actual image against those expected to be produced by a certain camera. The following process is shown in the figure 4.1.1

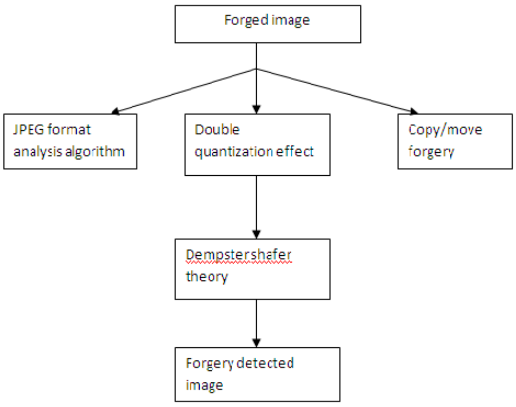

Figure 4.1.1

System flow diagram

4.2 LOSSY COMPRESSION TECHNIQUE EFFECT

Quantization, process is a lossy compression method is done by compressing a set of values to a single quantum value. When the no.of discrete symbols in a given stream is decreased, the stream becomes more easy compressible form. The forged image is detected by using tool B called lossy compression Effect algorithm. This algorithm is based on certain quantization artifacts appearing when applying Joint photographic experts group compression more than once. If a Joint photographic experts group file was used for any purpose the certain compression artifacts will unavoidably appear. In order to determine the lossy compression effect, the algorithm creates set of histograms like 192 histograms containing discrete cosine transform values. Certain quantization effects will only appear on these histograms if an image was saved in Joint photographic experts group format more than once. If the effect is exposed, we can definitely tell the image was modified(or at least saved by a graphic editor) at least once.

4.3 PLACE/TRANSFER FORGERY

The forged image is detected by using tool C called place/transfer Forgery detector. A very common practice of faking images is transplanting parts of the identical image one side to another image. For example, an image editor may cover the existence of a particular object by "patch image" with a part of conditions cloned from that identical image, place or transfer in existence or operation at the current time objects around the image.

5.FORGERY DETECTION USING DEMPSTER-SHAFER THEORY

In this module the result from Tool A, Tool B and Tool C are given as input to dempster-shafer theory to identify the forged content image.The final output of the fusion procedure knows whether a given region of an image has been damaged with or not. For this ,we consider the two sets: the first one is T the union of all propositions in which at least one trace is identified, the second one is N the single proposition in which none of the traces is found .

The output of the fusion process therefore consists of two belief values Bel(T) and Bel(N) calculated over the BBA m_FIN.These outputs summarize the information provided by the available tools, without forcing a final decision. If a binary decision about image authenticity is required, an interpretation of these outputs has to be made; the most intuitive binarisation rule is to classify an image as tampered with when the belief for the presence of at least one trace is stronger than the belief for the total absence of traces, that is to say when Bel(T) >Bel(N).

6. PERFORMANCE EVALUATION

The proposed system can be compared by means of Sensitivity, specificity, accuracy were calculated.It is shown in the figure 6.1

Sensitivity=$\frac{TP}{TP+FP}$

Specificity = $\frac{TN}{TN+FN}$

Accuracy=$\frac{TN+TP}{TN+FN+TP+FP}$

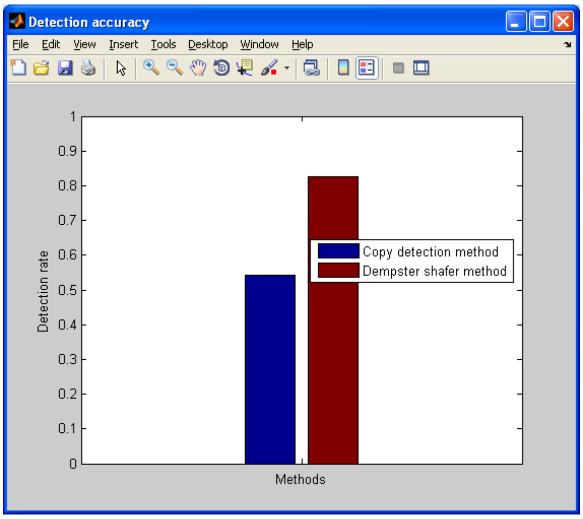

Figure 6.1 Detection Accuracy

Where True positive, False positive, True negative, and False negative represent the number of true positives, false positives, true negatives, and false negatives, respectively.

7.CONCLUSION AND FUTURE WORK

7.1 CONCLUSION

The existing method aims at removing from a given image the footprints left by Joint photographic experts group compression, in both the spatial domain and frequency domain. However, efficient forensic could not be easily obtained. To deal with this problem the present work proposes different forgery detection algorithm tools such as Joint photographic experts group Format Analysis algorithm, Double Quantization Effect and place/transfer Forgery. The result from these different tools is combined using Dempster-Shafer combiner to produce a better final classification. Efficient tradeoff between the forensic Undetectability and the image visual quality is obtained Sensitive to different properties of images and forgeries has been analyzed.

7.2 FUTURE WORK

Future research shall be devoted to the design of an optimal attack to the Joint photographic experts group image considering multiple detectors and the non-convex Structural similarity metric. We may get inspirations from existing work on optimal attack to a single, histogram-based forensic detector. We would like to further study the image statistics in the Discrete cosine transform domain for a better histogram restoration, and to compare our adaptive local dithering model with the recently proposed calibration-based non parametric Discrete cosine transform quantization noise estimation method.

8.REFERENCES

1.JPEG image steganalysis utilizing both intra block and inter block correlations, C. Chen and Y. Q. Shi ,2008.

2 . A variational approach to JPEG anti-forensics," .W. Fan, K. Wang, F. Cayre, and Z. Xiong, 2013.

3.Anti-forensics of double JPEG compression detection P. Sutthiwan and Y. Q. Shi ,2011,

4. Steganalysis by subtractive pixel adjacency matrix T. Pevny, P. Bas, and J. Fridrich, 2010.

5. Digital image authentication from JPEG headers, E. Kee, M. K. Johnson, and H. Farid, 2011.

6. Image forgery localization via block-grained analysis of JPEG artifacts, T. Bianchi and A. Piva, 2012.

7 . Detection of double-compression in JPEG images for applications in steganography, T. Pevny and J. Fridrich,. 2008.

8. Nonlinear Programming, D. Bertsekas, 1999.

9. UCID—An uncompressed colour image database G. Schaefer and M. Stich, 2004.

10. Biased reconstruction for JPEG decoding,"J. R. Price and M. Rabbani, 1999.

11. DCT quantization noise in compressed images,M. A. Robertson and R. L. Stevenson 2005.

12 .The Hungarian method for the assignment problem, H. W. Kuhn, 1955.

13. A universal technique to hide traces of histogram-based image manipulations ,M. Barni, M. Fontani, and B. Tondi, 2012.

14. JPEG anti-forensics using non-parametric DCT quantization noise estimation and natural image statistics ,W. Fan, K. Wang, F. Cayre, and Z. Xiong, 2013.

15. Using high-dimensional image models to perform highly undetectable steganography. T. Pevny, T. Filler, and P. Bas, 2010.