ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Image Forensics Analysis by Using DST, Fuzzy and Bayesian Approaches

D.Gokila Bharathi[1], G.Selvavinayagam[2]

PG-Scholar, Department of Information Technology, SNS College of Technology, Coimbatore[1]

AP/IT, Department of Information Technology, SNS College of Technology, Coimbatore[2]

ABSTRACT: A Forensic Image is often accompanied by a calculated Hash signature to validate that the image is an exact duplicate of the original. It is mainly focus on detection of artifacts introduced by single processing tool. Hence making it necessary for developing several for detection of artifacts. In this paper we introduce different theoretical frameworks, based on Dempster-Shafer's Theory of Evidence, Fuzzy Theory and Bayesian decision fusion respectively, to perform the fusion of heterogeneous, incomplete or conflicting outputs of forensic algorithms. These models are easily expandable to an arbitrary number of tools, do not require tools output to be probabilistic and take into account available information about tools reliability. To validate the proposed approaches, we carried out some experiments addressing a simple yet realistic scenario in which three forensic tools exploit different artifacts introduced by double JPEG compression to detect cut and paste tampering within a specified region of an image. The results we obtained are encouraging, especially when compared with the performance of a simple decision method based on the binary OR operator.

KEYWORDS**:** Dempster-Shafer, Fuzzy Theory, Bayesian decision fusion Image forensics, Image Tampering

I. INTRODUCTION

Dempster-Shafer's (DS) theory of evidence [8] is a framework for reasoning under uncertainty that allows the information in a more flexible way with respect to Bayesian theory. Reasoning in the Bayesian framework often urges to apply insufficient reasoning to assign a-priori probabilities, thus introducing extraneous assumptions. Dempster-Shafer's theory instead, abandons the classical probability frame and allows to reason without a-priori probabilities through a new formalism. Fuzzy sets theory was as an extension of the classic set theory [9], [10]. From this initial concept a multi-value fuzzy logic has been derived as an extension of Boolean logic. Fuzzy logic aims to imitate the highly adaptive behavior of human reasoning to incomplete, unreliable or partially true information. In a decision fusion approach,a verification system needs to fuse the partial decisions of the different individual modalities

II. TOOLS FORMALIZATION

One of simple and effective ideas for detection of JPEG block artifacts have been assumes that if there is no compression the pixel differences across blocks should be similar to those within blocks. If the image is JPEG-compressed, the differences across blocks should be different due to block artifacts assume the block grid is known. We then calculate the differences within a block and spanning across a block boundary.[1]

The different types of manipulations will lead to inconsistent blocking artifacts in the tampered region, which can therefore be used as evidence of tampering. The introduction of the blocking artifact characteristics matrix (BACM) which exhibits a symmetrical shape for the original JPEG images and that this symmetrical property will be altered by cropping and recompression operations. We have presented a method that exploits this property of the BACM for effectively detecting cropping and recompression operations in JPEG images. It is assumed as tool A.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The trained SVM is applied to decide whether the image is tampered .If it is tampered, and then the tampered region is also output. Our method has several advantages. First, it is capable of locating the tampered region automatically without the user to prescribe the suspicious region .[2]
To explain the DQ effect that results from double JPEG compression, we shall give a brief introduction of JPEG compression. The compression of JPEG images involves three basic steps:
(1) DCT: An image is first divided into DCT blocks. Each block is subtracted by 128 and transformed to the YUV colour space. Finally DCT is applied to each channel of the block.
(2) Quantization: the DCT coefficients are classified based on quantization step and rounded to the nearest integer.
(3) Entropy coding: lossless entropy coding of quantized DCT coefficients (e.g., Huffman coding)
This is assumed as a tool B[2]

The image, it is likely that the manipulated region will be altered after it has been inserted. Any such post-processing may disrupt the detection of JPEG ghosts. To test the sensitivity to
such post-processing, the tampered region was either blurred or sharpened, equalized after being inserted into the image[3] .The technique for detecting tampering in low quality JPEG images. This approach explicitly detects if part of an image was compressed at a lower quality than the saved JPEG quality of the entire image. Such a region is detected by simply re-saving the image at a multitude of JPEG qualities and detecting spatially localized local minima in the difference between the image and its JPEG compressed counterpart. Under many situations, these minima, termed JPEG ghosts, are highly salient and easily detected.

The technique is to detect the presence of non aligned double JPEG (NA-JPEG) compression. NA-JPEG compression is detected by training a classifier on a set of features, our approach relies on a single yet powerful feature derived from the statistics of DCT coefficients, allowing us to apply a simple threshold detector.It is able to estimate both the grid shift and the quantization step of the DCT coefficient of the primary compression. Such information can be used to perform a more detailed analysis of a possibly forged image.[4].It is assumed as tool C.

The embedding technique would perform well when tested only on that method and might fail on all others. Steganalysis methods perform less accurately overall but provide acceptable performance in many cases. The goal is to secure communications from an eavesdropper to hide the very presence of the message itself from an observer[5].It is assumed as a tool D.

The first application is the new steganalyzer could be created by fusing a number of steganalysis techniques while at the same time improving the detection accuracy. The increasing number of features, the classifier becomes more susceptible to curse of dimensionality problem.

The steganalyst will have to select one or more techniques which will employ on a set of suspected stegoimages. Only one steganalysis technique is employed but with the help of fusion one could improve and expand the results, by including more steganalyzers. This form of information would be valuable in any forensic analysis of the stego images that intends to recover the hidden message[5].

The tampering detection process does not rely entirely on a single detector and hence can be robust in face of missing or unreliable detectors. A statistical fusion framework based on Discriminative Random Fields (DRF) to integrate multiple cues suitable for forgery detection such as double quantization artifacts and camera response function inconsistency. This detection results in individual cues are used as observation from which the DRF model parameters and the most likely node labels are inferred indicating whether a local block belongs to a tampered foreground or the authentic background.
Framework is effective and general - outperforming individual detectors over systematic evaluation and easily extensible to other detectors using different cues Applying Discriminative Random Field based methods to incorporate both local-block authenticity and inter-block inconsistency measures[6]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The feature selection techniques, the Independent Component Analysis (ICA), and the Canonical Correlation Analysis (CCA) for achieving a more discriminate subspace for extracting tamper signatures from quantization and noise residue features.

The evaluation of proposed fuzzy fusion technique along with different feature selection techniques for copy-move tampering emulated on low bandwidth Internet video sequences, show a significant improvement in tamper detection accuracy with fuzzy fusion.

The processing pipeline once the images or video is captured consists of several stages. First, the camera sensor (CCD) captures the natural light passing through the optical system. In digital cameras, every pixel is detected by a CCD detector, and then passed through different color filters called Color Filter Array (CFA)

Enhance the robustness of tamper detection methods. By examining different feature selection techniques, the Independent Component Analysis (ICA), and the canonical correlation analysis (CCA) for achieving a more discriminate subspace for extracting tamper signatures from quantization and noise residue features[7]

The original not being available, it is emulated through the blurred version of the test image. The blurring operation removes additive high-frequency disturbance due to certain types of image manipulations to create a version of the untampered image.These are extracted from the multiscale decomposition of the image.

The performance of classifiers with respect to selected controlled manipulations as well as to uncontrolled manipulations are analyzed. The tools for the image manipulation detection are treated under feature fusion and decision fusion scenarios.

Each feature category has its weak and strong points manipulation types, and it is best to select features from the general pool of all categories feature fusion .In the second set of experiments with multiple manipulations, it is best strategy was to use different types of classifiers experts one per manipulation to fuse their decisions[8]

The Dempster-Shafer theory of evidence is an important tool in granular computing and particularly useful in the task of multi-source information fusion. Central to its application in information fusion is the use of Dempster's rule for combining belief structures. Implicit in the use of Dempster's rule is the assumption that the belief structures are independent. In many cases this assumption does not necessarily hold.

The possibility of incomparability in approach can at times involve considerable computational complexity. There may be a possibility of incomparability .This problem may be reduced by the fact that the atomic belief structures may be simple and hence easy to compare. This approach made use of a weighted aggregation of the belief structures where the weights are related to the degree of dependence. While the use of the containment procedure for comparing the information contents of belief structures has been greatly extended it still can often result in incomparability between belief structures .Use the sequence that results in a fused value that provides the most information, least uncertainty [9]

A.Tool Compatibility

Suppose we have three tools (TooIA, TooIB, TooIC) and suppose that ideally only some combinations of their outputs can be expected; for example, itmay be that the presence of the trace detectable by ToolA implies the absence of the trace detectable by ToolB and TooIC, so, at least ideally, the three tools should never detect tampering simultaneously.

All of these tools aim to check if a certain region of the image has been substituted with one cropped from another image, before performing a last JPEG re-compression of the resulting image with quality factor QF2. In particular, ToolA checks if the region has been cropped, without preserving JPEG grid alignment, from another JPEG image, that was already compressed with quality QF 1; ToolB reveals both if the region has been cropped from an uncompressed image or from a JPEG compressed image (quality QF1) but without preserving grid alignment; Toole checks if the region has been cropped from a JPEG compressed image (quality QF1) and pasted preserving JPEG grid alignment.

B.Experimental setup:

We conducted our experiments on a dataset of 1600 JPEG compressed images by checking integrity of a 256 x 256 region located in the center of each image. Among these 1600 images, 800 are kept unmodified and 800 are used to simulate 4 different classes of cut & paste tampering. Each class has been designed so that only a single tool (or a pair of tools) is able to detect the presence of the manipulation2. Depending on alignment or misalignment of 88 grids of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

first and latter JPEG compression and on their respective quality factors, a specific tool may or may not be able to detect a manipulation (see table I for a brief description of each tampering procedure). According to the principles underlying each tool and to a preliminary experimental analysis we carried out on them. According to the assumptions made in each tool has to output a value of detection in [0,1], where values near 1 indicate a high confidence about the analyzed region being tampered. For TA, this value is obtained using the approach to get a probabilistic output from the SVM (training has been performed on a separated dataset); for TB, the detection is taken as the median (over the suspected region) of the probability map for TC, the value of the KS statistics is directly used. The main advantage of the Bayesian approach is that it leads to the optimal classifier, in the sense that it implements the lowest Bayes risk. There are however a number of problems with this approach. The most important problem is that the probability density functions (pdfs) have to be estimated correctly. This usually implies the selection of the structure (class of functions) for the approximator and the optimization of the free parameters to bestfit the pdf. This optimization is performed on a training set. The plasticity of the approximator has to be chosen carefully. For highly plastic approximators, quite general pdfs may be approached, but an important (often impossible to obtain) number of samples is needed for performing the training. Furthermore, the training set should be representative (which in general does not correspond to the equal a priori probability hypothesis) and over-training has to be avoided to reach good generalization. The final evaluation is by calculating DST, Fuzzy Theory and Bayesian decision fusion.

REFERENCES.

[1] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in Proc. ICASSP 2007, Apr.2007, vol. 2, pp. II-217–II-220.

[2] Z. C. Lin, J. F. He, X. Tang, and C. K. Tang, "Fast, automatic and finegrained
tampered JPEG image detection via DCT coefficient analysis," Pattern Recognit., vol. 42, no. 11, pp. 2492–2501, Nov. 2009.

[3] H. Farid, "Exposing digital forgeries from JPEG ghosts," IEEE Trans.Inf. Forensics Security, vol. 4, no. 1, pp. 154–160, Mar. 2009.

[4] T. Bianchi and A. Piva, "Detection of non-aligned double JPEG compression with estimation of primary compression parameters," in Proc. 2011 18th IEEE Int. Conf. Image Processing (ICIP), Sep. 2011, pp.
1929–1932

[5] M. Kharrazi, H. T. Sencar, and N. D. Memon, "Improving steganalysis by fusion techniques: A case study with image steganography," Trans.Data Hiding Multimedia Security, vol. 4300, pp. 123–137, 2006.

[6] Y.-F. Hsu and S.-F. Chang, "Statistical fusion of multiple cues for image tampering detection," in Proc. 42nd Asilomar Conf. Signals, Systems and Computers, 2008, Oct. 2008, pp. 1386–1390.

[7] G. Chetty and M. Singh, "Nonintrusive image tamper detection based on fuzzy fusion," in Proc. IJCSNS, Sep. 2010, vol. 10, no. 9, pp. 86–90.

[8] S. Bayram, I.Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electron. Imag., vol. 15, no. 4, pp. 041102–041102-17,2006.

[9] Ronald R. Yager "Aggregating Non-Independent Dempster-Shafer Belief Structures",Machine Intelligence Institute,(New Rochelle,)NY 10801

[10] M.Fontani, T. Bianchi, A. De Rosa, A. Piva, and M. Barni, "A Dempster-Shafer framework for decision fusion in image forensics,"in Proc. 2011 IEEE Int. Workshop on Information Forensics and Security (WIFS), Dec. 29, 2011, pp. 1–6.