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 Dempster-Shafer Framework For Decision Fusion In Image Forensics

C.R.Lakshmi[1], Alex george[2],

PG Scholar, Member IEEE, SNS College of Engineering, Coimbatore, India[1]

Assistant Professor, Department of EEE, SNS College of Engineering, Coimbatore, India[2]

ABSTRACT: The Proposed work is based on a decision fusion strategy for image forensics is presented, based on Dempster-Shafer's Theory of Evidence. The goal is to automatically summarize the information provided by several image forensics tools, allowing both a binary and a soft interpretation of the global output produced. The proposed strategy is easily extendable to an arbitrary number of tools, it does not require that the output of the various tools be probabilistic and it takes into account available information about tools reliability. Comparison with logical disjunction and SVM based fusion shows an improvement in classification accuracy.

I. INTRODUCTION

In the last years many algorithm for detecting photographic tampering have been introduced. In particular, several schemes have been proposed to find traces left by different kinds of tampering. However, in many cases, tampering is obtained by applying a small set of processing tools hence a part of the available trace detectors will reveal the presence of tampering furthermore, it may happen that the positive answer of one algorithm inherently implies the negative answer of another because they search for mutually excluding traces. Finally, trace detectors often give uncertain if not wrong answers since their performance are far from ideal. For this reasons, taking a final decision about the authenticity of an image relying on the output of a set of forensic tools, is not a trivial task. This problem can be addressed in different ways as illustrated, for the steganalysis problem. There are basically three kinds of approaches to fusion. The first is to perform fusion at the feature level: each tool extracts some features from the data, and then a subset of these features is selected and used to train a global classifier. The second is to consider the output of tools (usually a scalar) as they are and fuse them (measurement level). The lat approach consists in fusing the output of the tools after they have been thresholded (abstract level).

Most of the existing works are based on the first approach. A problem with fusion at the feature level is the difficulty of handling cases involving a large number of features (curse of dimensionality) and the difficulty to define a general framework, since adhoc solutions are needed for different cases.

In order to get around the above problems, we chose to perform fusion at the measurement level. In fact, the choice delegates the responsibility of selecting features and training classifiers (or other decision methods) to each single tool, the keeping the fusion framework more general and easy to extend while avoiding to lose important information about tool response confidence, as would happen when fusion at the abstract level. Specifically, we present a fusion framework based on the Dempster- Shafer's "Theory of evidence" (DS theory) that focuses exclusively on the fusion at the measurement level.The proposed framework exploits knowledge about tool performances and about compatibility between various tool responses, and can be easily extended when new tools become available. It allows both a "soft" and a binary (tampered/non-tampered) interpretation of the fusion result, and can help in analyzing images for which taking a critical due to conflicting data. Note that a fusion approach involving DS Theory has already been proposed, however such as scheme applies fusion at feature level hence inheriting the general drawbacks of feature-level fusion, noticeably the lack of scalability and the need to retrain the whole system each time a new tool is added.

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

This paper is organized as follows: the Dempster-Shafer's framework is briefly introduced in sec. II; the proposed model is presented in sec. III, and its application to three well known tools ([1], [2] and [3]) along with experimental results is presented in sec. IV.

II. DEMPSTER-SHAFER FRAMEWORK

Dempster-Shafer's theory of evidence [9] is a framework for reasoning under uncertainty that allows the representation of ignorance and of available information in a more flexible way with respect to Bayes theory. When using classical probability theory for finding the probability of a certain event A, the additivity rule must be satisfied; so by saying that Pr(A) = pA one implicitly says that Pr($\bar{A}$) = 1-pA, thus committing information about the probability of event A to its complementary ($\bar{A}$).

Another consequence of the rule of additivity regards the representation of ignorance: complete ignorance about a dichotomic event A can be represented only by setting Pr(A) = Pr($\bar{A}$) = 0:5 (according to Laplace's principle of insufficient reasoning), but this probability distribution would also be used to model perfect knowledge about probability of each event being 0.5 (as for a fair coin tossing). Furthermore, reasoning in the Bayesian framework often urges to apply insufficient reasoning to assign a-priori probabilities, thus introducing extraneous assumptions. DS theory, instead, abandons the classical probability frame and allows to reason without a-priori probabilities through a new formalism.

A.Shafer's formalism

Let the frame $\Omega x = \{x1, x2, \ldots, xn\}$ define a finite set of mutually exclusive and exhaustive possible values of a variable x. We are interested in quantifying the belief for propositions of the form "the true value of x is in H", where $H \leq x$ .Each proposition is mapped onto a single subset and is assigned a basic belief mass through a Basic Belief Assignment.

Definition Let Ω be a frame. A function $m : 2^{\Omega} \rightarrow [0,1]$ is called a Basic Belief Assignment (BBA) if:

$$m(\Phi) = 0; \quad \sum_{A \leq} m(A) = 1 \quad ...(1)$$

where the summation is taken over every possible subset A of Ω. Each set S such that m(S) > 0 is called a focal element for m. Thus m(A) is the part of belief that supports exactly A but, due to the lack of further information, does not support any strict subset of A. Intuitively, if we want to obtain the total belief that a given BBA commits to A, we must add the mass of all proper subsets of A plus the mass of A itself, thus obtaining the Belief for the proposition A.

Definition A function $Bel : 2^{\Omega} \rightarrow [0,1]$ is a belief function over Ω if:

$$Bel(A) = \sum_{B \leq A} m(B)$$

Bel(A) summarizes all our reasons to believe in A. Relationships and interpretations of m(A), Bel(A) and other functions derived from these are well explored . Here we just notice that $Bel(A) + Bel(\bar{A}) \leq 1 \; \forall A \leq$ and 1 - (Bel(A) + Bel($\bar{A}$)) is the lack of information about A.

B. Combination Rule

We are interested in using the DS framework to perform data fusion. Dempster defined a combination rule that allows to combine several belief functions defined over the same frame.

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

Definition Let Bel1 and Bel2 be belief functions over the same frame ⍰ with BBAs m1 and m2. Let us also assume that K, defined below, is positive. Then for all non-empty A≤ the function m12 defined as:

$$m_{12}(A) = \frac{1}{1-K} \sum_{i,j:\ A_i \cap B_j = A} m_1(A_I)\, m_2(B_j) \quad ..(2)$$

where $K = \sum_{i,j:\ A_i \cap B_j = A} m_1(A_I)\, m_2(B_j)$, is a BBA function and is called the orthogonal sum of Bel1 and Bel2, denoted by Bel1 ⊕ Bel2.

This rule has many properties [11], in this work we are mainly interested in its associativity and commutativily. Note that K is a measure of the conflict between m1 and m2: the higher the K, the higher the conflict.

In definition (2) it is assumed that the two BBAs, m1 and m2, are defined over the same frame. Whenever we need to combine BBAs that are defined on different domains, we have to redefine them on the same target frame: this can be done using marginalization and vacuous extension. Let us call domain D the set of variables on which evidence is defined, and let denote a BBA on domain D with m^D.

Definition Let m^{D_1} be a BBA function defined on a domain D1, then its vacuous extension to D1 ∪D2, denoted with $m^{D_1 \uparrow (D_1 \cup D_2)}$, is defined as

$$m^{D_1 \uparrow (D_1 \cup D_2)}(C) = \begin{cases} m^{D_1(A)} \\ 0 \end{cases} \text{ if } C = A \times D_2$$

This allows to extend the frame of a BBA function without introducing extraneous assumptions (no new information is provided about variables that are not in D1).The inverse operation of vacuous extension is marginalization.

Definition Let mD be a BBA function defined on a domain D, its marginalization to the domain D0 ⊆ D, denoted with $m^{D \downarrow D0}$, is defined as

$$m^{D \downarrow D0}(A) = \sum_{B \downarrow A} m^D(B)$$

where the index of the summation denotes all sets B⊆ D such that the configurations in B reduce to those in A⊆ D0 by the elimination of variables in D that are not also in D0.

III. DST-BASED DATA FUSION IN IMAGE FORENSICS

In this section we present our framework for combining evidence coming from two or more tamper detection algorithms.

A.Assumptions

We consider a case in which we want to investigate the integrity of a known suspect region of an image. We assume that two or more tools are available that, given the suspect region, look for specific tampering traces whose presence reveals tampering. In some cases, we may know that two tools search for mutually-exclusive traces (so that if the first tool reveals a trace, the second one should not find its own); in some other cases, tools search for compatible traces. A single tool can never tell if the image is definitely unmodified: it can only indicate whether the image contains the trace it has looked for or not. We assume that each tool outputs a number in [0,1], where values near 1 indicate a high confidence about the analyzed

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

region being tampered; we also assume to have some information (possibly image dependent) about tools reliability (for instance such an information could derive from experimental evidence).

B. Formalization for one tool

For sake of clarity, we start by formalizing the proposed framework for one tool only, let us call it ToolA, which returns a value Aϵ [0, 1] and has a reliability R ϵ [0, 1]. We first consider the information coming from the detection value by introducing a variable Ta, with frame: $_{Ta}$= {ta, na} where ta is the event "image has undergone a tampering detectable using ToolA" and na is the event "image has not undergone a tampering detectable using ToolA". Information provided by ToolA can then be summarized with the following BBA over the frame $_{Ta}$

D. Tool compatibility

By now we have considered tool responses as if they were independent from each other. This allowed us to avoid conflicts between tools, obtaining an easily expandable fusion framework, however, as we noted in III-A, this is not always the case in real applications. Suppose we have three tools (ToolA, ToolB, ToolC) and suppose that ideally only some combinations of their outputs can be expected; for example, it may be that the presence of the trace detectable by ToolA implies the absence of the trace detectable by ToolB and ToolC, so, at least ideally, the three tools should never detect tampering simultaneously. This information can be easily incorporated within the DST model by using a BBA defined on the domain Ta×Tb×Tc, that has only one focal set, which contains the union of all events that are considered possible, while all other events have a null mass.

E. Final decision

We can now define the final output of the fusion procedure ,i.e. we want to know whether a given region of an image has been tampered with or not. To do so we consider the belief of two sets: the first one, T, is the union of all events in which at least one algorithm revealed a tampering, the second one, N, is the single event in which none of the tools detected a tampering (in the previous example it would be N = (na; nb; nc)). The output of the fusion process therefore consists of two belief values and a measure of the conflict detected during decision fusion; formally, the output is given by the triplet {Bel(T),Bel(N),K} where K is defined in sec. II-B. 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 binarization rule is to classify an image as tampered when Bel(T) > Bel(N), but we can also make a simple implementation of the "presumption of innocence" principle by requesting Bel(T) > Bel(N)+K. The Receiver Operating Curve can thus be obtained by classifying images according to Bel(T) > Bel(N) + K + þ and sampling þ in [-1,1]. Notice we did not need to introduce a-priori probabilities about an image being original or forged: in a Bayesian framework, this would have been harder to obtain.

IV. EXPERIMENTAL RESULTS

In order to validate the effectiveness of the proposed approach, we compared it with one of the approach proposed in [8], where image manipulations are detected by taking the logical disjunction (OR) of the outputs of single tools. Logical disjunction is indeed one of the simplest and most widely used methods for decision fusion, and is quite well-suited to the proposed case study1. On the other side, several methods have been proposed for decision fusion at feature level in image forensics [5] [6] [7] [10], but they are typically based on feature selection and are therefore not directly comparable to the method proposed in this work. In particular, in [10] DS Theory is employed in a decision fusion framework, but it is used to fuse features instead of tool responses: the actual decision is taken using a SVM, thus requiring an additional training step

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

which hinders one of the main advantages of the proposed method (namely, that each tool can be added without retraining the whole system). Nevertheless, because all cited methods end up using a classifier (usually a SVM) the best we can do for comparing our framework to them without exiting the measurement level is to train a SVM using the output of the single tools as input features, and see how the SVM performs in discriminating between tampered and original images.

A .Experiment setup

We choose to perform experiments by fusing outputs obtained from three algorithms for tampering detection, namely: the one from Luo et al.[1] (which we will call ToolA), the one from Lin et al.[2] (ToolB) and the one from Farid [3] (ToolC). 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 compressed with quality QF1; 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; ToolC checks if the region has been cropped from a JPEG compressed image (quality QF1) and pasted
preserving JPEG grid alignment. To be compliant with the assumptions in section III-A, each tool has to output a value in [0,1], where values near 1 indicate a high confidence about the analyzed region being tampered. For ToolA, this value is obtained using the approach in [12] to get a probabilistic output from the SVM (training is performed on a separated dataset); for ToolB, the detection is taken as the median (over the suspected region) of the probability map [2]; for ToolC, the value of the KS statistic is directly used [3], exploiting the fact that the DST framework does not require the input values to have a probabilistic meaning.

B. Results

We performed two different sets of experiments. In the first one, we built a test dataset of 1600 images, generated with exactly the same procedure used to build the training set, but using different images. We have 800 original images (that is, JPEG compressed once with QF in {40, 50,… 100} and 800 tampered images, 200 for each of the four classes. We run the three forensic tools and fuse their outputs on all of these

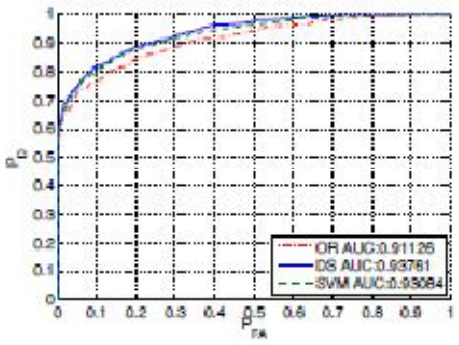

Fig:ROC for logical disjunction and SVM on the standard dataset.

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

V. CONCLUSION

In this paper we have addressed a central problem in image forensics, namely the fusion of information stemming from the application of several tamper detection tools. The fusion strategy we have developed is easily extendable to even a large number of tools. Other advantages derive from the adoption of a DST framework, since such a theory permits to cope with situations in which incomplete information is available about the a-priori tampering probabilities. Information about the dependence among the output of the single tools and their reliability can also be easily incorporated within the model. Experimental results are encouraging: the proposed model gives significantly better results than a fusion approach based on logical disjunction, and also outperforms SVM-based fusion (that presents the additional disadvantage of requiring a global training of the final SVM classifier, limiting the scalability of this approach). Future work will focus on validating the proposed scheme on larger datasets and assess its capacity to handle situations in which the output of more.

REFERENCES

[1] W. Luo, Z. Qu, J. Huang, and G. Qiu, "A novel method for detecting cropped and recompressed image block," in Proc. of ICASSP 2007, vol. 2, Apr 2007, 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 Recognition, vol. 42, no. 11, pp. 2492–2501, Nov. 2009.
[3] H. Farid, "Exposing digital forgeries from JPEG ghosts," IEEE T. on Information Forensics and Security, vol. 4, no. 1, pp. 154–160, 2009.
[4] M. Kharrazi, H. T. Sencar, and N. D. Memon, "Improving steganalysis by fusion techniques: A case study with image steganography," T. Data Hiding and Multimedia Security, vol. 4300, pp. 123–137, 2006.
[5] Y.-F. Hsu and S.-F. Chang, "Statistical Fusion of Multiple Cues for Image Tampering Detection," in Asilomar Conference on Signals, Systems, and Computers, 2008.
[6] G. Chetty and M. Singh, "Nonintrusive image tamper detection based on fuzzy fusion," IJCSNS, vol. 10, no. 9, pp. 86–90, Sep 2010.
[7] D. Hu, L. Wang, Y. Zhou, Y. Zhou, X. Jiang, and L. Ma, "D-S Evidence Theory based digital image trustworthiness evaluation model," in Proc. of MINES 2009, ser. MINES '09, vol. 1, 2009, pp. 85–89.
[8] S. Bayram, I. Avcibas, B. Sankur, and N. Memon, "Image manipulation detection," J. Electronic Imaging, vol. 15, no. 4, 2006.
[9] G. Shafer, A Mathematical Theory of Evidence. Princeton: Princeton University Press, 1976.
[10] P. Zhang and X. Kong, "Detecting image tampering using feature fusion," Proc. of ARES 2009, vol. 0, pp. 335–340, 2009.
[11] A. Benavoli, L. Chisci, B. Ristic, A. Farina, and A. Graziano, Reasoning under uncertainty: from Bayesian to Valuation Based Systems. ISBN: 978-8886658430, 2007.
[12] J. C. Platt, "Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods," in Advances in large margin classifiers. MIT Press, 1999, pp. 61–74. than three tools has to be fused.