IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 August 2022, accepted 6 September 2022, date of publication 14 September 2022,
date of current version 26 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3206543

SURVEY

A Comparative Study of Bayesian and Dempster-Shafer Fusion on Image Forgery Detection

ANH-THU PHAN-HO[1] **AND FLORENT RETRAINT**[2]
[1]CNRS, UMR 9189—CRIStAL, University of Lille, 59000 Lille, France
[2]ICD—LM2S, University of Technology of Troyes, 10300 Troyes, France

Corresponding author: Anh-Thu Phan-Ho (anhthuph88@gmail.com)

This work was supported by the ANR Project DEFACTO under Grant ANR-16-DEFA-0002.

ABSTRACT With the advent of digital imaging, it has become fairly easy to modify the content of an image in many different ways while leaving no obvious visual clue. This has further challenged many existing image forensic techniques. The techniques which perform well with one specific kind of forgeries still suffer from strong limitations when dealing with realistic tampered images. Therefore, an effective strategy for tampering detection and localization requires the application of fusion technique. Although there have been extensive researches on fusion technique on different fields, there has never been a systematic study about fusion technique in image forensic domain. In this paper, we provide a thorough review on the state-of-the-art of fusion methods applied in tampering image detection and localization domain. We then present a practical comparison of two popular fusion techniques: Bayesian and Dempster-Shafer theory (DST) based fusion. The comparison relies on two applications which leverage the two aforementioned fusion techniques. In the first case, aggregating the decision maps of two forensic approaches: Photo Response Non Uniformity (PRNU) and statistical features based approaches has improved the forgery detection performance on saturated and dark regions of images. In the second case, integrating the decision maps of the forensic approach using demosaicing artifacts and the forensic approach using SIFT descriptors and local color dissimilarity maps has enhanced the detection performance on both copy-moved and copy-pasted forgeries images. Experiments show that the DST based fusion performs better in the first case while the Markov Random Field (MRF) based fusion performs better in the second case. It can be concluded that each technique has its own advantages and the best choice depends on each situation and users' requirements.

INDEX TERMS Forgery localization, Dempster-Shafer theory, energy minimization, Bayesian fusion, photo response non-uniformity, decision fusion.

I. INTRODUCTION

Over past decades, the rapid growth and the advancement of powerful digital image processing tools has made it simpler and easier to forge an image while leaving no obvious visual clue. This has given rise in the number of forgery images in reality. In this context, image forgery has posed a serious impact on many areas, including: economics, politics or even criminal investigation. Therefore, verifying the authenticity of an image has become increasingly important. There has been accordingly increasing research in image forgery detection and localization. Generally speaking, there are two major approaches to study the trustworthiness of a candidate image: active approaches and passive approaches [1]. Active approaches usually involve designing various kinds of watermarks or perceptual hashes of the image content and embedding them into the digital image. At the verification stage, the former embedded watermarks or image hashes are extracted and compared to determine whether the original image has been tampered with [2], [3], [4]. In contrast to

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

active approaches, the passive approaches are more widely used as they do not rely on any prior information. They are mostly based on analyzing specific inherent clues or traces that left during the creation of forgery images. In this paper, we focus on forgery images detection based passive approaches. In [5], Farid divided image forgery operation into six different categories: compositing, morphing, retouching, enhancing, computer generating and painting. Among these categories, compositing operation, or alternatively image tampering, is one of the most popular technique to forge images as it is easier to process. In this paper, we mostly consider tampering image category. In a tampered image, there are the authentic parts and the tampered parts. If the tampered parts are copied within the original image, it is named copy-move tampering. If the tampered parts come from another image, it is named cut-paste tampering or splicing. These various forgery image operations would leave different traces during the creation process. Thus a single forensic detector would have difficulties giving good performance due to the following reasons. Firstly, each forensic method usually deals with a single type of manipulation or a single trace. It could then perform well with a specific forgery operation but much worse with others. For example, the copy-move detection methods relying on duplicated regions detection will fail to detect splicing images. Secondly, due to the advancement of information technology recently, most of tampering images are often the results of various processing tools. However, in blind forgery image detection approach, we do not have any prior information about which types of operation it has been undergone. Therefore, it would be better to construct a unified forensic detector system to be able to output a global answer about its authenticity. Thirdly, an individual forensic tool usually gives unreliable output as it only bases on a specific characteristic of a typical trace. Particularly, a single forensic detector is effective with a specific type of images. For example, the methods based on analysing device characteristics such as sensor pattern noise, Photo Response Non-Uniformity noise (PRNU) [6], [7], [8], color filter array (CFA) [9], [10] work well for RAW or TIFF images but worse for detecting JPEG forgery images with low quality compression. The algorithms based on exploiting the double quantization artifacts hidden among the DCT coefficients in forgery JPEG images to localize the tampered regions [11], [12], [13] fail in detecting forgery images which is processed in RAW and resave in JPEG. Methods based PRNU have high false detection rate on saturated and dark regions [14]. Some methods only detect tampered parts with large sizes while the others detect better with small sizes. Therefore, if we want to detect and localize the forgery image effectively, using a single forensic detector may not be efficient. In order to improve the robustness of the forgery image detection, it is necessary to use the fusion technique to merge information from different forensic tools. Fusion technique permits to either aggregate multiple cues from different forgery operations or integrate several decision output mappings of each single detector thus can exploit useful information from different sources. Hence fusion becomes a significant technique to improve the performance in forgery images detection and localization. However, how to select the different sources of information to be combined and which method to fuse to obtain a good performance in image forgery detection are not evident tasks. To the best of our knowledge, there has never had a systematic study before on the fusion technique applied in forgery image detection and localization. In this paper, we perform a review on information fusion in forgery image detection and localization. We hope to help students and researchers to have an overview about how to apply information fusion in forgery image detection. We then make a practical comparison of Bayesian and Dempster Shafer Theory fusion techniques applied in localizing forgery images.

This paper is an extension of [34] in which we present a systematic review on information fusion in forgery image detection and localization. We also propose a fusion framework to improve the forgery detection and localization by integrating the decision maps of the forensic algorithms which detect copy-paste and copy-move tampering. More importantly, a comparative study of two fusion techniques DST and Bayesian is presented. And finally, the experiment results are tested on more datasets comparing to [34].

The remainder of this paper is organized as follows. Section II gives a brief definition of information fusion and discussion on what and when to fuse. In Section III, we review fusion methods which have been applied in forgery image detection and localization. We then make a practical comparison of Bayesian and Dempster Shafer Theory fusion techniques applied in localizing forgery images in Section IV. Finally Section V concludes our work.

II. FUSION IN IMAGE FORGERY DETECTION

In this section, we first define what information fusion is, then discuss what source of information to be fused and when to fuse in forgery image detection and localization problem.

A. DEFINITION OF INFORMATION FUSION

There have been existed many definitions of data fusion. The authors in [15] gave a general definition of information fusion as "the science of combining measurements, signals, or observations from different sources to obtain a result that is in some sense better than what could have been achieved without this combination." Due to this advantages, fusion is a crucial topic in many scientific fields including sensors fusion, data fusion in internet of things [16], remote sensing [17], [18], [19], medical images fusion [20], [21], biometric fusion [22], fusion in steganalysis [23] and fusion in digital image forensics [24], [25], [26], [27].

B. INFORMATION SOURCE TO FUSE

1) **Multi-cue** An image is usually forged by using many different image processing tools, thus it leave various traces. For example, a spliced image can be created by cutting a region from an uncompressed or jpeg image and pasting into a jpeg host image and then resaving in

jpeg. This causes the double quantization traces [28], [29], [30], [31]. If the copied part in the spliced image comes from different camera, it leaves the camera sensor traces. The authors in [24] proposed a statistical fusion framework to integrate multiple cues suitable for forgery detection, such as double quantization artifacts and camera response function inconsistency.

2) **Multi-scale** To localize an image we use the sliding window manner. There is a tradeoff between choosing the size of the windows and the accuracy. If the size is too large, it cannot detect small forgery parts. If the size is too small, there may be not enough data for statistics analysis. The authors in [26] and [27] proposed to fuse multiple candidate tampering maps resulting from the analysis with different sizes of sliding windows to obtain a more reliable tampering map with better localization resolution.
3) **Multi-algorithm** In the jpeg forensics, forgery creation could leave different jpeg compression traces such as double quantization [28], non alignement jpeg grid [29] and ghost jpeg traces [30]. In [27] the authors proposed the Dempster Shafer Theory Fusion to exploit all available information from these traces to achieve a more reliable decision of the authenticity of an image. In [32], the authors combine the algorithm based PRNU and the one based CFA. The authors [33] integrated the tampering maps of statistical feature-based detector and copy-move forgery detector. In [34] the authors fused tampering maps obtained from PRNU and statistical feature-based detectors.

C. LEVELS OF FUSION

There are generally three stages in the forgery image detection and localization pipeline at which information can be fused, including feature-level fusion, score-level fusion and decision-level fusion.

1) **Feature-level fusion** involves training a single classifier in a concatenated feature space. Fusion at feature levels could improve the detection performance but becomes computationally demanding due to exponential growth of the dimensionalities of the training set.
2) **Score-level fusion** (or is also called measurement-level fusion [35]) is performed by aggregating the outputs of individual forensic detectors, which are trained separately. These scalar outputs could be classification score or probability.
3) **Decision-level fusion** is performed at the latest stage to merge binary results which are thresholded of each forensic detector. Fusion at this level is computationally efficient however it reduces some amount of detailed information at early levels such as features, scores.

III. FUSION METHODS

Despite the evident potential benefit of fusing information in forgery image detection and intensive research has been done, the knowledge of how to exploit the information, how to perform information fusion are still at very preliminary stages in digital image forensic field. In this sequel, we review several mathematical theories for fusing information applied in forgery image detection and localization problem.

There are two main categories of fusion methods in forgery image detection and localization problem due to its characteristics. Firstly, the decision outputs of forensic algorithms are usually unreliable and imprecise because of limited technical algorithm or particular characteristics of the considered images (e.g. type of compression or saturated regions). Therefore, the information sources to be fused such as traces and decision maps are often imprecise and uncertain. There are then approaches capable of representing specific aspects of imperfect data such as methods based on probability theory, Dempster-Shafer evidence theory and fuzzy set theory, etc. Secondly, the image forgery detection and localization can be seen as a classification problem in which it outputs the label (e.g. tampered or not tampered) or even a label probability of each pixel in the considered image. Hence methods of fusing multiple classifiers are also studied to improve the robustness in detecting and localizing forgery images. In the following, we discuss four fusion methods including rule-based fusion methods, probability-based methods, evidence reasoning methods, classification based methods.

A. RULE-BASED FUSION METHODS

The rule-based fusion method includes a variety of basic rules of combining such as linear weighted fusion (sum and product), MAX, MIN, AND, OR. In [36] and [37] the authors fuse the output maps of three forensic tools, based on sensor noise, machine-learning and block-matching, respectively. A decision fusion strategy is then implemented using the simple rule AND, based on suitable reliability indexes associated with the binary masks. In [38], the authors proposed to fuse three detectors which are PRNU based approach, Patch Match based approach and Near-Duplicate based approach. The tampering maps are merged with the AND operator, according to a confidence value obtained evaluating the maps on a training set of tampered images whose ground truth tampering mask is known.

B. PROBABILITY-BASED METHODS

Probability-based methods rely on the probability distribution which is defined based on the Kolmogorov axioms to express data uncertainty. Among those, Bayesian fusion which lies the Bayes estimator is one of the most powerful fusion methodologies, especially for the fusion of heterogeneous information sources. In fusion problem applied in detecting and localizing tampering images, we are usually interested in combining information such as traces, features, decision outputs, etc. of several quantities of interest $\boldsymbol{Z} = \{Z_1, \ldots, Z_n\}$. It is assumed that the information of each quantity of interest Z_i is $\boldsymbol{d_i} = \left(d_i^1, d_i^2, \ldots, d_i^K\right)$. In Bayesian fusion approach, it is of our interest to compute the quantity $P\left(\boldsymbol{Z} \mid \boldsymbol{d_1}, \ldots, \boldsymbol{d_n}\right)$. In the following, we discuss two approaches related to

Bayesian fusion methodology which can be applied in forgery image detection and localization problem.

1) THE CASE OF UNRELIABLE INFORMATION SOURCES

As aforementioned, the output of forensic tools are often affected by uncertainty and impreciseness. In the sequel, we consider an example to show that Bayesian fusion method is able to handle uncertainties. Assume that we want to fuse the decision output of two forensic tools $\mathbf{Z} = \{A, B\}$. The forensic tool A has the information $\boldsymbol{d}_1 = (\boldsymbol{t}_1, \boldsymbol{r}_1)$ where $\boldsymbol{t}_1$ is the tampering output map and $\boldsymbol{r}_1$ is the reliability of the output of tool A. Similarly, the information contribution of forensic tool B is $\boldsymbol{d}_2 = (\boldsymbol{t}_2, \boldsymbol{r}_2)$. In Baysian fusion approach, one has to compute the posterior distribution $P(\mathbf{Z} \mid \boldsymbol{d}_1, \boldsymbol{d}_2)$ using Bayes' theorem

$$\begin{aligned} P(\mathbf{Z} \mid \boldsymbol{d}_1, \boldsymbol{d}_2) &= \frac{P(\boldsymbol{d}_1 \mid \mathbf{Z}, \boldsymbol{d}_2)\, P(\boldsymbol{d}_2 \mid \mathbf{Z})\, P(\mathbf{Z})}{P(\boldsymbol{d}_1, \boldsymbol{d}_2)} \\ &= \frac{P(\boldsymbol{d}_1 \mid \mathbf{Z})\, P(\boldsymbol{d}_2 \mid \mathbf{Z})\, P(\mathbf{Z})}{P(\boldsymbol{d}_1, \boldsymbol{d}_2)} \\ &\propto P(\boldsymbol{d}_1 \mid \mathbf{Z})\, P(\boldsymbol{d}_2 \mid \mathbf{Z}) \end{aligned}$$

Here we ignore some constants such as $P(\boldsymbol{d}_1, \boldsymbol{d}_2)$ and $P(\mathbf{Z})$ which is assumed to follow the uniform distribution on $\mathbf{Z} = \{A, B\}$. We also assume that the information from each tool is conditionally independent given $\mathbf{Z}$, e.g. $P(\boldsymbol{d}_1 \mid \mathbf{Z}, \boldsymbol{d}_2) = P(\boldsymbol{d}_1 \mid \mathbf{Z})$. By modelling the distribution $P(\boldsymbol{d}_i \mid \mathbf{Z})$, we can then estimate the posterior distribution $P(\mathbf{Z} \mid \boldsymbol{d}_1, \boldsymbol{d}_2)$. For more detail, the reader can see the example that has been given in a similar form in [39].

2) RELATION TO AN OPTIMIZATION APPROACH TO INFORMATION FUSION

One of the goals of fusion problem is to find the optimal result via combining several available data. This is the reason why the Bayesian fusion problem resorts to Bayesian maximum a posteriori (MAP) estimation problem. For example, at decision-level fusion, the authors in [26], [27], and [33] aim at computing the optimal tampering map $\boldsymbol{x}$ given a set data $\boldsymbol{d}$ of candidte maps obtained from different forensic detectors or from various scales of sliding windows. The posterior and prior distributions are the basis for further calculations. In [26], [27], and [33], the authors modeled the prior with a Markov Random Field (MRF) and then represented it in terms of Gibbs potentials. By this transformation, Bayesian MAP estimation corresponds to energy minimization problem. In other words, the Bayesian fusion methodology is directly related to energy functional formalism. The authors in [24] also resolve the fusion problem to MAP estimation but they adopted the Discriminative Random Field (DRF) framework and thereby choosing the model for posterior distribution instead of the prior one. The logistic models are used for posterior probabilities.

C. EVIDENCE REASONING METHODS

Evidence reasoning methods include the method based Dempster-Shafer (DS) theory, which is a mathematical theory for modeling uncertain and combining evidence from different sources to arrive at a degree of belief. Different from Bayesian method, DS theory deals with measures of "belief" which may not obey the classical probability axioms to represent uncertain knowledge. It assigns mass function to represent distribution of belief thereby not requiring to specify the prior probability in advance. However, it does require mass values to be assigned in a meaningful way to the elements of the system.

In [27], the authors proposed a fusion framework based DS theory to combine the output of several forensic tools at measurement level thereby permitting to exploit as much information about the tool reliability and about the compatibility between the traces of tampering. More precisely, three combinations are carried out hierarchically in their framework including incorporation of the output of each forensic tool with its reliability, combination of different tools looking for the same tampering traces and combination of different traces. Each combination is merged by using Dempster's rule and Basic Belief Assignment (BBA) is redefined on the same frame using marginalization and vacuous extension before being combined. The final decision is then made by comparing the two belief values of two sets: T is the union of all propositions in which at least one trace is detected and N is the single proposition in which none of the traces is found. These belief values $Bel(T)$ and $Bel(N)$ are calculated over the BBA of the final mass function. A region is decided to be tampered when $Bel(T) > Bel(N)$.

In [40], the authors also proposed a fusion framework based DS theory, yet, they not only fuse output of different forensic tools but also integrate several background information into the framework such as tool-based information, trace-based information and semantic-based information. Taking into account these side information which influences the reliability of the forensic tools, the forensic performance is enhanced. Particularly, some local properties of the image such as saturated or textured regions affect accuracy of the forgery localization maps. Thus the values of output map are adjusted by mapping this local background information to a BBA on the frame of the considered trace by using the method proposed in [41]. Moreover, the global background affects the output map when the estimated statistical model of the tampered pixels and that of the original pixels are not well separated. They then model the global information by defining a new BBA. In addition, the compatibility relationships between traces are modeled as a BBA using Dempster's rule. Finally, the fused map is refined by exploiting the content of the analyzed image.

D. CLASSIFICATION BASED METHODS

Classification-based methods include fuzzy logic based on theory of fuzzy set and algorithms using machine learning such as K-Nearest Neighbor (KNN), Support Vector Machines (SVM) and Naive Bayes (NB), etc.

The image forgery detection and localization can be seen as a classification problem in which it outputs the label

TABLE 1. Fusion techinques and their applications.

Ref.	Fusion techniques	Applications
[36], [37]	Rule-based fusion	using AND rule to fuse the output maps of forensic tools.
[38]	Rule-based fusion	using AND rule to fuse the output maps of PRNU, Patch Match and Near-Duplicate based approaches.
[25], [26], [32]	Bayesian fusion	using MRF to model prior and resolve the fusion problem to MAP estimation.
[24]	Bayesian fusion	resolve the fusion problem to MAP estimation but adopted the Discriminative Random Field framework.
[27]	DST fusion	combine output maps to exploit information between traces of tampering.
[40]	DST fusion	combine background information such as tool, trace and semantic-based information.
[42]	Classification based fusion	classified tampered and not tampered pixels based on fuzzy integral.
[43] [35]	Classification based fusion	merge the outputs of several forensic tools in order to handle their uncertainty and impreciseness.
[44]	Classification based fusion	use the Sugneo and Choquet integrals to merge tool outcomes at the measurement level.
[45]	Classification based fusion	multiple classifier fusion.
[46]	Classification based fusion	using some combination rules including WMV, BKS and Naive Bayes Combiner, Product and Sum.
[49]	Classification based fusion	using BKS representation fusion to integrate two best approaches in the copy move detection.
[33]	Classification based fusion	integrated the tampering maps of SF-based detector and copy-move forgery detector.
[50], [51]	Classification based fusion	applying fusion in deep learning and CNN to localize forger images.

(e.g. tampered or not tampered) or even a label probability of each pixel in the considered image. In [42] Chetty and Singh classified tampered and not tampered pixels based on fuzzy integral. They first fuzzified features extracted from different forensic algorithms and then generated the membership functions and fuzzy integral. The input pixels are classified into a specific class if that class has the maximum output of fuzzy integral. In [35] and [43] Barni and Costanzo presented a fuzzy fusion system at measurement level to merge the outputs of several forensic tools in order to handle their uncertainty and impreciseness. They constructed the membership function from pairs (detection, reliability) provided by forensic algorithms and then used the if-then rules to compute the outcome. This outcome is then defuzzified by being compared with a threshold to obtain the final decision. Kuar and Gupta [44] proposed a fusion framework based on fuzzy integrals for passive-blind image tamper detection. Different from the work of Chetty and Singh, they used the Sugneo and Choquet integrals as the aggregation operators to merge tool outcomes at the measurement level.

As each detector has its own advantages and disadvantages, combination of different detectors is necessary to explore their complementary properties. A multiple classifier fusion [45] can be used to improve the robustness of forgery localization performance as it may generate more accurate classification than each of the individual classifiers. Classifier fusion is often based on combination rules like the product, sum, Weighted Majority Voting (WMV), Behavior Knowledge Space (BKS) and Naive Bayes Combiner (NB), etc.

In [46], the authors combined several forensic tools such as detector based on Block Artifact Grid introduced by JPEG compression [47], detector based on the double quantization effect introduced when the original and the tampered regions in images were coded at different compression ratios [30], [31], detector based on finding traces of resampling in the image [48] and detector based on PRNU [14]. The fusion decision is implemented using several combination rules including Weighted Majority Voting (WMV), Behavior Knowledge Space (BKS) and Naive Bayes Combiner (NB), Product and Sum. The authors in [25] compare the majority voting fusion, average fusion, supervised learning fusion and clustering analysis fusion using K-means with the fusion based energy minimization.

The traditional classifier fusion approaches did not consider the conditional and spatial dependence of tampered pixels with respect to their neighborhood pixels. The authors in [49] solve this problem by proposing the Behavior Knowledge Space representation fusion to integrate two best approaches in the copy move detection: block-based and points of interest detection methods.

The authors [33] integrated the tampering maps of statistical feature-based detector (M^{Fea}) and copy-move forgery detector (M^{PM}). They first projected the score of original and tampered pixels of the training forgery images on the $M^{Fea} - M^{PM}$ plane, then manually designed a decision curve with fewer parameters which is effective and faster comparing to linear and non-linear classifiers such as SVM. The experimental results show that this fusion strategy gives better performance than the fusion based DRF and fusion based supervised learning.

Recently, there have been several papers applying fusion in deep learning and CNN to localize forger images [50], [51]. In [50] Liu and Pun proposed a deep fusion network for splicing forgery localization. Particularly, the deep convolutional neural networks called Base-Net are first trained to extract forensic features including JPEG compression artifacts and noise discrepancy. Then the trained convolutional kernels from the Base-Nets are used to construct the fusion-net to fuse these forensic features.

Table 1 summarizes the fusion techniques and their applications.

IV. BAYESIAN AND DST FUSION AND APPLICATION

In this section, we compare the two dominate fusion techniques for multi-algorithms: Bayesian fusion and DST fusion at decision-level fusions. We study the Bayesian fusion as an optimization approach as mentioned in the subsection III-B2 which corresponds to energy minimization problem.

A. ENERGY MINIMIZATION BASED FUSION

Forgery localization problem can be seen as a labeling problem where we label 1 as a tampered pixel and 0 as an authentic pixel. Multi-algorithm fusion means to find the best labeling given decision maps of several forensic algorithms. The energy minimization based fusion tries to incorporate the knowledge from given data and the prior to look for the optimal labeling map. This framework is used in multi-scale fusion [25], [26]. Particularly, denote vector $\mathbf{t} \in \{0,1\}^N$ a tampering map of the image which is vectorized of size N. Denote vector $\mathbf{m}^{(k)} \in \{0,1\}^N$ be the tampering map of the forensic algorithm k^{th}. The optimal tampering map aggregating from K forensic algorithms is the one maximizing the posterior probability given a set of tampering maps $\mathbf{m}^{(k)}$:

$$\hat{\mathbf{t}} = \underset{\mathbf{t}\in\{0,1\}^N}{\arg\max} P\left(\mathbf{t} \mid \mathbf{m}^{(k)} : k = 1, \ldots, K\right) \tag{1}$$

Ignoring the constant term $P(\mathbf{m})$, the problem can be rewritten as:

$$\hat{\mathbf{t}} = \underset{\mathbf{t}\in\{0,1\}^N}{\arg\max} P\left(\mathbf{m}^{(k)} : k = 1, \ldots, K \mid \mathbf{t}\right) P(\mathbf{t}) \tag{2}$$

Assume the independence between m_i, we have

$$\hat{\mathbf{t}} = \underset{\mathbf{t}\in\{0,1\}^N}{\arg\max} \prod_{i=1}^{N} P\left(m_i^{(k)} : k = 1, \ldots, K \mid t_i\right) P(\mathbf{t}) \tag{3}$$

Assume the independence between methods, we have:

$$\hat{\mathbf{t}} = \underset{\mathbf{t}\in\{0,1\}^N}{\arg\max} \prod_{i=1}^{N} \prod_{k=1}^{K} P\left(m_i^{(k)} \mid t_i\right) P(\mathbf{t}) \tag{4}$$

The prior is usually assumed the smoothness of neighboring pixels and is then modeled with a Markov random field in which the decision at each pixel depends only on its direct neighborhood. It is noted that MRF formulation and Gibbs energy formulation are equivalent due to the Hammersely-Clifford theorem. Thus $P(\mathbf{t})$ is modeled as follows:

$$P(\mathbf{t}) = Z^{-1} e^{-U(\mathbf{t})} = Z^{-1} e^{-\sum_{c\in C} V_c(\mathbf{t})} \tag{5}$$

where Z is a normalizing constant, V_c is a clique which is defined as a subset of pixels such that any two distinct pixels are mutual neighbors. Then

$$\hat{\mathbf{t}} = \underset{\mathbf{t}\in\{0,1\}^N}{\arg\max} \prod_{i=1}^{N} \prod_{k=1}^{K} P\left(m_i^{(k)} \mid t_i\right) Z^{-1} e^{-\sum_{c\in C} V_c(\mathbf{t})} \tag{6}$$

Taking a negative logarithm of (6), the fusion problem can be solved by minimizing the following function:

$$\sum_{c\in C} V_c(\mathbf{t}) - \sum_{i=1}^{N} \sum_{k=1}^{K} \log P\left(m_i^{(k)} \mid t_i\right) \tag{7}$$

Similar to the work of [25], [6], [26], we use the Ising model [52] which considers single-element and two-element cliques.

Denote $E\left(m_i^{(k)}, t_i\right) = -\log P\left(m_i^{(k)} \mid t_i\right)$. The multi-algorithms fusion becomes minimizing the following energy function:

$$\sum_{i=1}^{N} \sum_{k=1}^{K} E\left(m_i^{(k)}, t_i\right) + \alpha \sum_{i=1}^{N} t_i + \beta \sum_{i=1}^{N} \sum_{j\in\mathcal{N}_i} \mid t_i - t_j \mid \tag{8}$$

where $\mathcal{N}_i$ contains top, bottom, left, right neighbor pixels of i. The parameter α controls the preference towards sparser tampering maps and the paraleter β controls the interaction strength of neighboring pixels.

We use the graph-cut based solver [53], [54] from UGM toolbox [55] to find the optimal tampering map. This approach uses a MRF to model the prior thus we call it interchangeably as MRF based fusion approach.

B. FUSION METHOD BASED DEMPSTER-SHAFER THEORY

1) ELEMENTS OF DEMPSTER-SHAFER THEORY

DST which is an effective theoretical framework for fusing and reasoning with uncertain and/or imprecise information was introduced by Dempster and Shafer [56], [57]. In this subsection, we briefly review its two main components: the degrees of belief representation and the Dempster's rule for combining such degrees of belief when they are based on independent sources. Let X be a variable taking values in a finite domain $\Omega = \{\omega_1, \ldots, \omega_n\}$, called the frame of discernment. Evidence about X may be represented by a mass function $m : 2^{\Omega} \rightarrow [0, 1]$ such that

$$\sum_{A\subseteq\Omega} m(A) = 1 \tag{9}$$

Each number $m(A)$ denotes a degree of belief attached to the hypothesis that $X \in A$. m is said to be normalized if $m(\emptyset) = 0$. This property will be assumed hereafter, unless otherwise specified. Corresponding to a mass function m, we can associate belief functions $Bel : 2^{\Omega} \rightarrow [0, 1]$ defined as follows

$$Bel(A) = \sum_{B\subseteq A} m(B) \tag{10}$$

Quantity $Bel(A)$ can be interpreted as the degree to which the evidence supports A.

In order to combine the evidence coming from multiple independent sources of information, we can use Dempster's combination rule to merge them. Let m_1 and m_2 be two mass functions derived from independent items of evidence. They can be fused to induce a new mass function m_{12} defined as

$$m_{12}(A) = \frac{1}{1-K} \sum_{B,C\subseteq\Omega, B\cap C=A} m_1(B)\, m_2(C) \tag{11}$$

where $K = \sum_{B,C\subseteq\Omega, B\cap C=\emptyset} m_1(B)\, m_2(C)$, $K < 1$ measures the degree of conflict between evidence m_1 and m_2. When $K = 1$, we define $m_{12}(A) = 0$.

In the following subsections, two applications using Bayesian and DST fusion are presented. In the first application, the decision maps of two forensic algorithms PRNU and Statistical Features (SF) based forgery detectors are integrated. The experiment is tested on our created dataset taken from three cameras Canon EOS-100D, Nikon D5200 and Panasonic DMC-GM1. In the second application, the decision maps of two forensic detectors for cut-paste and copy-move forgeries are aggregated. The experiment is tested on the public Realistic Tampering Dataset[1] created by Korus *et al.* [26].

C. APPLICATION I: FUSION TWO FORENSIC ALGORITHMS PRNU AND SF BASED FORGERY DETECTORS

To compare the performance of Bayesian and DST fusion, we consider to aggregate two image forgery detectors, one based on PRNU and the other based on SF.

1) PRNU-BASED FORGERY DETECTION

The PRNU which is a camera imaging sensor imperfection can be considered as a unique sensor pattern of each individual camera thereby being used for forgery detection. The idea is that the tampered regions could destroy or change position of the PRNU in the image. Therefore, by testing on which part of the image the PRNU is changed, one is able to reveal the tampered regions. We consider a simplified model of the image acquisition pipeline [58].

$$y = (1 + k)x + \eta \tag{12}$$

where y is a captured image, x is its idealized noise-free version, k is the camera PRNU, η is an additive noise term which accounts for all types of disturbances, and products between images, unless otherwise stated, are pixel-wise. The PRNU k can be estimated from N images obtained by the camera $y_1, \ldots, y_N$ using the maximum likelihood principle.

$$\hat{k} = \frac{\sum_{n=1}^{N} r_n y_n}{\sum_{n=1}^{N} y_n^2} \tag{13}$$

where $r_n = y_n - f(y_n)$ is the noise residual of the image y_n,f is a denoising filter. In the following, for the sake of simplicity, we assume that the estimation of the camera PRNU has no error, i.e., $\hat{k} = k$.

The PRNU of the image under test is compared with the reference PRNU in a sliding-window based manner. The forgery detection at each pixel $y_{i,j}$ is formulated as a binary hypothesis testing problem applied to a block B centered around the pixel $y_{i,j}$.

$$\begin{cases} H_0 : r_B = \eta_B \\ H_1 : r_B = z_B + \eta_B \end{cases} \tag{14}$$

where r_B, z_B and η_B are the restrictions of r, z, and η respectively, to the block B, $z = yk$ is the signal of interest (also called the reference PRNU). If the PRNU is absent in the block B (hypothesis H_0), its central pixel is labeled as being tampered. If the PRNU is present in B (hypothesis H_1), its central pixel is labeled as being genuine. The detection test is based on normalized correlation

$$\rho_{ij} = \text{corr}\,(r_B, z_B) \tag{15}$$

The probability density function (pdf) of ρ_{ij} under hypothesis H_0 is estimated by correlating the camera PRNU and the noise residuals coming from other cameras. The pdf of ρ_{ij} under hypothesis H_1 is heavily influenced by the block content. In deed, even in the genuine blocks, the correlation might be very low when these blocks are dark, saturated, or textured. The authors in [58] estimated a predictor based on local images features, such as texture, flatness and intensity, and then computed the expected value $\hat{\rho}_{ij}$ of the correlation under hypothesis H_1 hoping to reduce the false alarm in these cases.

The decision map M^{PRNU} is then defined as follows

$$M_{ij}^{PRNU} = \begin{cases} 0 & \rho_{ij} < \gamma_1 \text{ AND } \hat{\rho}_{ij} > \gamma_2 \\ 1 & \text{else} \end{cases} \tag{16}$$

where γ_1 is the threshold selected with a Neyman-Pearson approach to obtain the desired false acceptance rate (FAR), γ_2 is a threshold chosen heuristically to avoid labeling non-tampered ($M_{ij}^{PRNU} = 1$) pixels as tampered ($M_{ij}^{PRNU} = 0$).

2) SF-BASED FORGERY DETECTION

The SF based forgery detection is an approach in which we first extract some inherent features of image blocks that are likely to be modified when an image undergoes tampering and then use these features to proceed a two-class pristine/forged training procedure. It can be said that this is a universal approach in which we can detect many types of forgeries though the accuracy is not high. Among various statistical feature sets proposed in steganalysis, in this paper we adopt the statistical features named Spatial Color Rich Model (SCRM) [59] which work quite effectively in forgery detection [33]. SCRM is an extension of SRM. The SRM features from the R, G, and B channel are first added together and then concatenated three dimensional co-occurrences of residuals computed from all three color channels. These features are then used for training procedure. Based on a sliding-window manner, the training samples are extracted from tampered and pristine blocks of size 64 × 64 pixel with a step of 16-pixel and then fed into an ensemble classifier [60] with linear discriminant analysis base learners for identifying whether an image block is genuine or fake. The image under test I is divided into 64 × 64 pixel sliding windows with a step of 16-pixel. For each sliding window, the pre-trained ensemble classifier outputs a vote score $v \in \{-n_b, -n_b + 1, \ldots, n_b - 1, n_b\}$ where n_b is the number of base learners in the ensemble classifier. The decision map M^{SF} is computed as follows.

$$M_{i,j}^{SF} = \frac{1}{2n_b}\left(\frac{1}{K}\sum_{k=1}^{K} v_k + n_b\right) \tag{17}$$

where K is the number of blocks containing pixel $I_{i,j}$, and v_k is the vote score for the k^{th} block that contains $I_{i,j}$.

[1] http://pkorus.pl/downloads/dataset-realistic-tampering

3) DST BASED FUSION

The framework proposed in this subsection aims at fusing the evidence coming from the PRNU-based forgery detection and the SF-based forgery detection. We believe that aggregating the evidence from the SF-based approach will help to decrease the false alarm rate on the saturated and dark regions of images. The fusion procedure can be described as follows.

- Constructing mass functions m_1 and m_2 from the evidence of each approach: the PRNU-based forgery detection and the SF-based forgery detection.
- Using Dempster's combination rule to induce a fused mass function m_{12} from m_1 and m_2.
- Computing the belief function corresponding to the mass function m_{12}.
- Making final decision bases on the belief function.

What we are interested in this section is that whether the pixel $I_{i,j}$ in test image I is tampered or not tampered. We can model this scenario by defining a variable X with frame $\Omega = \{it, nt\}$ where it is the proposition "the pixel $I_{i,j}$ is tampered", and nt is the proposition "the pixel $I_{i,j}$ is not tampered". We want to quantify how much we are confident in these propositions.

The mass function m_1 and m_2 are respectively constructed from the decision maps of the PRNU-based forgery detection and the SF-based forgery detection.

$$m_1(X) = \begin{cases} t_1 & \text{for } X = \{it\} \\ n_1 & \text{for } X = \{nt\} \end{cases} \tag{18}$$

$$m_2(X) = \begin{cases} t_2 & \text{for } X = \{it\} \\ n_2 & \text{for } X = \{nt\} \end{cases} \tag{19}$$

where

$$\begin{aligned} t_1 &= M^{PRNU}_{i,j}, \quad n_1 = 1 - t_1 \\ t_2 &= M^{SF}_{i,j}, \quad n_2 = 1 - t_2 \end{aligned} \tag{20}$$

The degree of conflict K and the fused mass function m_{12} is computed as follows

$$K = t_1 n_2 + t_2 n_1 \tag{21}$$

$$\begin{aligned} m_{12}(\{it\}) &= \frac{t_1 t_2}{1-K} = \frac{t_1 t_2}{1 - t_1 n_2 - t_2 n_1} \\ m_{12}(\{nt\}) &= \frac{n_1 n_2}{1-K} = \frac{n_1 n_2}{1 - t_1 n_2 - t_2 n_1} \end{aligned} \tag{22}$$

The belief function in this case is equal to the fused mass function: $Bel(\{it\}) = m_{12}(\{it\})$ and $Bel(\{nt\}) = m_{12}(\{nt\})$. The quantity $Bel(\{it\})$ is the degree to which the evidence supports that the pixel $I_{i,j}$ is tampered. We then make a decision that a pixel is tampered if its degree of belief of tampering is greater than that of non tampering, i.e. $Bel(\{it\}) > Bel(\{nt\}) + \lambda$, where λ is a threshold chosen heuristically.

4) MRF BASED FUSION

Taking $\mathbf{m}^{(1)} = M^{PRNU}$ and $\mathbf{m}^{(2)} = M^{SF}$ where M^{PRNU} and M^{SF} are vectorized, and solving the optimal problem defined in eq. (8). We use the data term as in [26] and [27]:

$$E_\tau(m_i, t_i) = -\log \max(\Psi_{min}, \Psi_\tau(m_i, t_i)) \tag{23}$$

with $\Psi_{min} \in [0, 1]$ and

$$\Psi_\tau(m_i, t_i) = \begin{cases} 1 - \dfrac{m_i}{2\tau} & for\ t_i = 0 \\ 1 + \dfrac{m_i - 1}{2(1-\tau)} & for\ t_i = 1 \end{cases} \tag{24}$$

5) EXPERIMENTAL RESULTS

In this subsection, we will report some preliminary experiments to compare the performance of two fusion techniques. Our experiments were carried out on the dataset of the UTT which includes of images taken from three cameras, a Canon EOS-100D, a Nikon D5200 and a Panasonic DMC-GM1. The first row of Fig. 1 is some examples of realistic tampering images created by hand in modern photo-editing software in which their original images taken from the dataset of UTT. We first have estimated the PRNU of each camera over 100 images and then have extracted 25000 correlation samples over 25 images coming from other cameras and 25000 samples coming from the same camera to train the correlation predictor as proposed in [58].

We present in this section results only for one of the cameras, a Canon EOS-100D. For our experiments we used 200 tampered images and 200 pristine ones. The forgeries have been created with a copy-and-paste process and are all rectangular with size of 128 × 128. We evaluated the percentage of correctly detected forged pixels in the tampered images (P_D) and the percentage of falsely identified pixels in the pristine ones (P_{FA}), varying the relevant parameters of the algorithms that is, the γ_1, γ_2 in the PRNU-based forgery detection algorithm, and the threshold λ in the DST fusion and the parameter α, β in the Bayesian fusion.

In Fig. 1, we show the evaluation on several realistic tampered images (second row). The original images (first row) are taken from Canon EOS-100D camera and then are forged by inserting objects using the popular photo editing software GIMP. The third and fourth columns show the output maps of the SF and the PRNU based approaches. As can be seen, each individual approach has its own limitation. The PRNU based approach correctly detects the tampered regions but the false alarm rate is hard to avoid due to the saturated regions (see Fig. 2) and dark regions (see Fig. 3). In contrast, the SF based approach does not localize tampered regions with high accuracy but it does not have problem with saturated and dark regions. The integrated map fused from the PRNU and SF approaches in the fifth row shows a significant improvement of the DST fusion method. The last row are the decision maps integrated using MRF based fusion. We can see that, on these selected forgery images, MRF based fusion performs worse than DST based fusion did. It is worth mentioning that we did not apply any morphological operation in the fusion approach.

In Fig. 4 we show the ROCs (receiver operating characteristics) of the PRNU-based approach and of the fusion

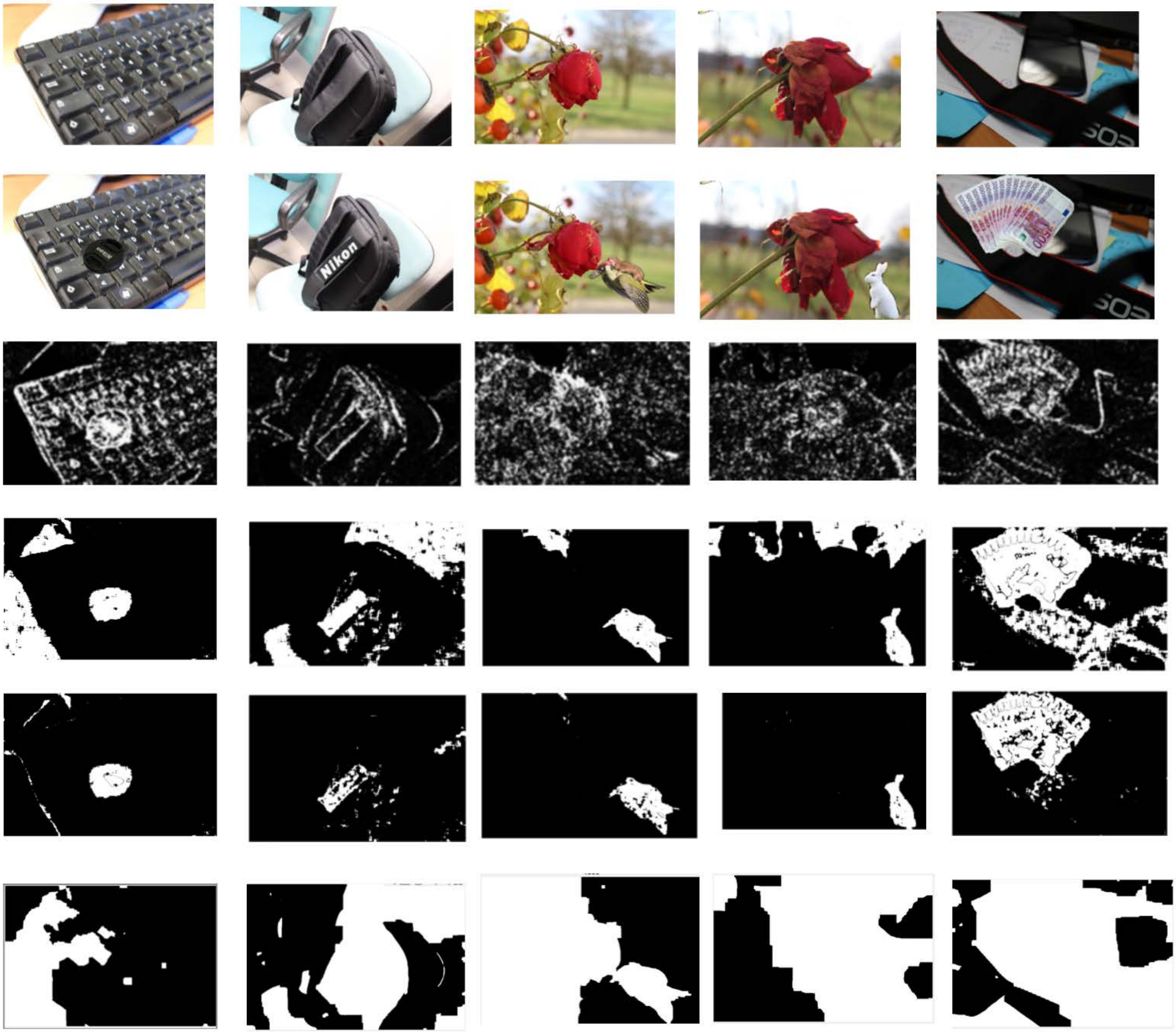

FIGURE 1. **Realistic examples of localizing tampering images. The first row are original images, the second row are tampered images, the third row are detection maps by SF-based approach, the fourth row are maps detected by PRNU-based approach, the fifth row are maps created by the DST based fusion and the last row are the decision maps integrated using MRF based fusion.**

approaches computed on the complete test set (200 forgery images and 200 genuine images). We can see in Fig. 4 that the performance of two fusion techniques are quite similar.

In Fig. 5 we show the ROC curves of the PRNU-based approach and of the DST and Bayesian fusion techniques computed on the 10 forgery images and 10 genuine images whose saturated and dark regions are considerable. We can see in Fig. 5 that the DST and Bayesian fusion approaches significantly outperform the single PRNU-based approach. The DST fusion has better performance comparing to the Bayesian fusion in the sense that with the probability of false alarm in the range [0.12, 0.4], the DST fusion technique gives greater detection probability.

It is noted that choosing what to fuse is also an art. It had better to analyze the strength and weakness of each algorithm before deciding to fuse them. As mentioned before, the weakness of PRNU algorithm is to make high false alarm rate on the saturated and the dark regions while the SF based detector does not. Therefore, integrating these two maps could enhance the detection performance. If we test on the dataset where there are not considerably saturated and dark regions, it is hard to see the significant improvement because the SF based algorithm does not have a chance of leveraging its advantage. This explains why the tested results on 200 images in general do not show much improvement comparing to the results on 10 images whose saturated and dark regions are considerable.

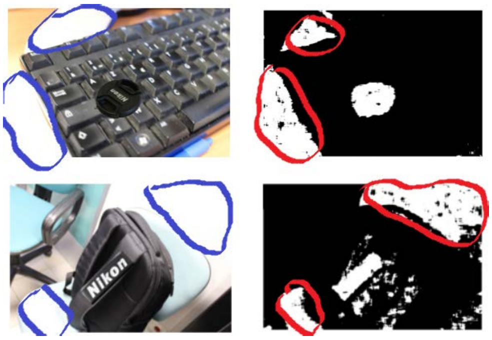

FIGURE 2. An example of falsely detected of PRNU based detector on saturated regions which are limited by blue curves.

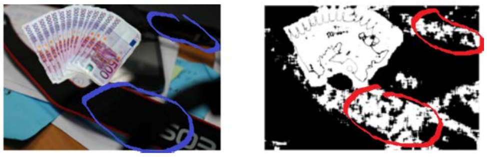

FIGURE 3. An example of falsely detected of PRNU based detector on dark regions which are limited by blue curves.

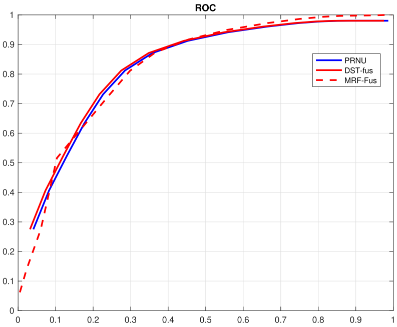

FIGURE 4. ROC for PRNU-based forgery detection algorithm and the DST and Bayesian fusion one on 200 images.

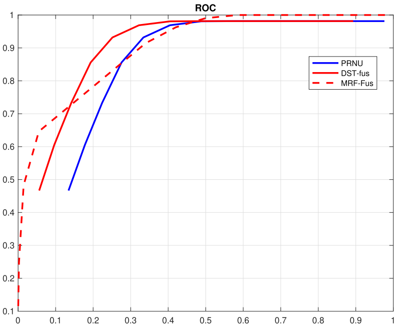

FIGURE 5. ROC for PRNU-based forgery detection algorithm and the DST and Bayesian fusion one on 10 images.

Beside that, we also use the F1-score to evaluate the detection performance [61]. F1-score is the harmonic mean of Precision (P) and Recall (R) which are computed from the confusion matrix of True Positive (TP), False Positive (FP),True Negative (TN) and False Negative (FN) as follows:

$$P = \frac{TP}{TP + FP} \text{ and } R = \frac{TP}{TP + FN} \tag{25}$$

$$F_1 = 2\frac{P \cdot R}{P + R} = \frac{2TP}{2TP + FN + FP} \tag{26}$$

The F1-score takes a high value when Precision and Recall are both important. The higher F1-score, the more efficient the algorithm is. Please see Table 2 for the meaning of the measure used in forgery localization performance.

TABLE 2. Measure to evaluate forgery localization performance.

TP	number of tampered pixels correctly localized
FN	number of unlocalized tampered pixels
FP	number of authentic pixels wrongly localized
TN	number of unlocalized authentic pixels
P	probability that localized pixels are tampered
R	probability that tampered pixels are localized

Table 3 shows the F1-score evaluated on the 10 forgery images and 10 genuine images whose saturated and dark regions are considerable. We can see that although the F1-score are low but it did show the significant improvement of the fusion. The F1-score of DST fusion is highest and 10 times greater than those of PRNU and SF based detectors.

TABLE 3. F_1-score on the dataset of UTT.

Method	F_1-score
PRNU based detector [58]	0.0056
SF based detector [59]	0.0057
DST based fusion of PRNU and SF	**0.0309**
MRF based fusion of PRNU and SF	0.0208

D. APPLICATION II: FUSION TWO FORENSIC ALGORITHMS DEMOSAICING ARTIFACTS AND COPY-MOVE BASED FORGERY DETECTORS

As mentioned in the introduction, the tampered parts of an image could either be copied within the original image, the so-called copy-move tampering, or come from another image, the so-called copy-paste tampering. The copy-move detection methods usually rely on duplicated regions detection thereby failing to detect copy-paste tampering images. On the other hand, algorithms aiming at detecting copy-paste tampering are limited to detect copy-move tampering images. Motivated from this idea, we come up with the idea integrating decision maps generated from algorithm detecting copy-paste and copy-move tampering to enhance performance. In the context of the project DEFACTO,[2] we find it necessary to combine the decision maps from different research teams [62], [63] to enhance the detection performance. In [62] Le *et al.* proposed to use demosaicing artifacts (also known as color filter array (CFA) interpolation) to detect tampered parts of images. Particularly, traces left by demosaicing are specific for different camera brands and/or models. The lack of these traces or their

[2] https://anr.fr/Project-ANR-16-DEFA-0002

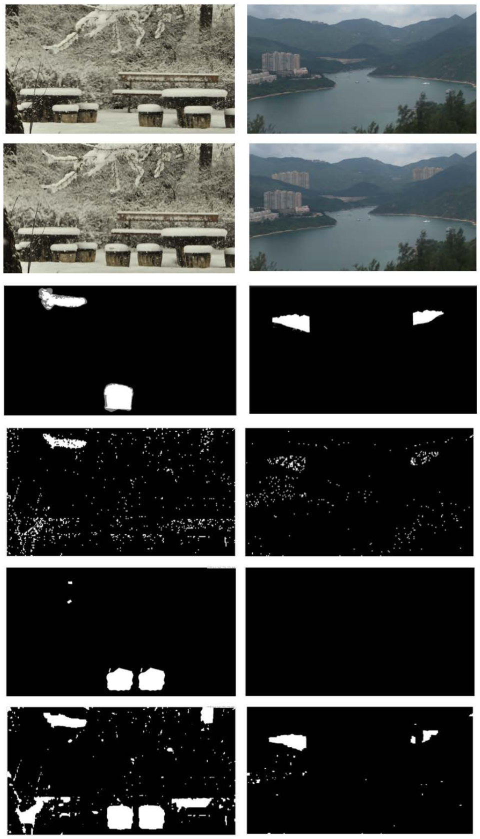

FIGURE 6. **Fusion of forensic algorithms improves detection performance by detecting both cut-paste and copy-move forgery regions. These two tampering images are chosen from the dataset of Korus [26]. The first rows are original images, the second row are tampered images, the third row are ground-truth images, the fourth row are maps detected by [62], the fifth row are maps detected by [63] and the last row are integrated maps based on MRF fusion.**

inconsistency for different image regions may indicate the presence of tampering. In [63] Mahfoudi *et al.* proposed to utilize the SIFT key-points and descriptors and then filter the result using a Local Dissimilarity Map to detect copy-move tampering. However, each of these algorithms has its own drawback. For example, we can see the first column in Fig. 6, the algorithm [62] could not detect the copy-move tampering and the algorithm [63] failed to detect the copy-paste in the image (see the fifth row in Fig. 6). Therefore it is a good idea to fuse these decision maps to improve the performance.

Let denote the decision maps generated from algorithm in [62] and [63] respectively M^{CP} (CP: copy-paste) and M^{CM} (CM: copy-move). The procedure to aggregate these decision maps based on DST and MRF fusion is totally similar to ones presented in Sub-section IV-C3 and Sub-section IV-C4.

More particularly, for the DST fusion, we only replace the maps in equation (20) as follows

$$\begin{aligned} t_1 &= M^{CP}_{i,j}, \quad n_1 = 1 - t_1 \\ t_2 &= M^{CM}_{i,j}, \quad n_2 = 1 - t_2 \end{aligned} \tag{27}$$

Similarly, for the MRF fusion, we take $\mathbf{m}^{(1)} = M^{CP}$ and $\mathbf{m}^{(2)} = M^{CM}$.

TABLE 4. ***F_1*-score on data Korus.**

Method	F_1-score
[62] Le et. al	0.2323
[63] Mahfoudi et.el	0.2948
DST fusion method [62] and [63]	0.0650
MRF fusion method [62] and [63]	**0.3912**

1) EXPERIMENTAL RESULTS

The experiment is tested on images containing both copy-move and copy-paste tampering chosen from the dataset generated by Korus *et al.* [26]. Such chosen images would leverage the performance of fusion algorithms because the individual algorithms in [63] and in [62] fail to detect copy-paste and copy-move tampering respectively (see Fig. 6) while the integrated of these two algorithms could detect both tampering operations.

The F1-score in Table 4 shows that the MRF based fusion gives the highest F1-score while the DST based fusion gives the lowest F1-score. Figure. 7 visually illustrates that the MRF based fusion algorithm gives better performance than the DST based fusion and individual algorithm [62], [63]. This significant improvement of the MRF based fusion is mainly based on the following reasons: First, the prior of the tampering map is modeled with a MRF thereby exploiting spatial dependencies of neighborhood pixels. This helps a lot to decrease the number of non-detected tampered pixels comparing to the algorithm [62]. For instance, comparing to the ground-truth images in the third column of Fig. 7, we see that the MRF fusion (the last column) is able to detect splicing pixels that the algorithm in [62] missed (the forth column). Second, the MRF fusion could integrate both copy-paste and copy-move tampering parts (see first column of Fig. 6 and first and last column of Fig. 7). Third, the DST based fusion in this context fails to improve the performance because the DST is limited to combine the conflict evidence. More specifically, we are considering to combine the decision maps of the algorithm [62] which could detect copy-paste tampering but not copy-move and those of [63] which could detect copy-move but not copy-paste tampering. Therefore, there are usually the conflict parts in these maps. That is the reason why the decision maps generated from DST fusion (the sixth column of Fig. 7) are usually all black.

E. DISCUSSION

In this subsection, we will discuss the differences and similarities between the DST and MRF fusion techniques and explain the advantages and disadvantages of each fusion technique in two considered experiments.

Both fusion techniques have a certain initial requirement. While the Bayesian technique requires the prior probabilities, the DST technique requires masses to be assigned in a meaningful way to the various states, including an undecided state. However, in this work we only consider two states that are tampered and not tampered. The implementation of DST fusion is quite simple comparing to the Bayesian fusion.

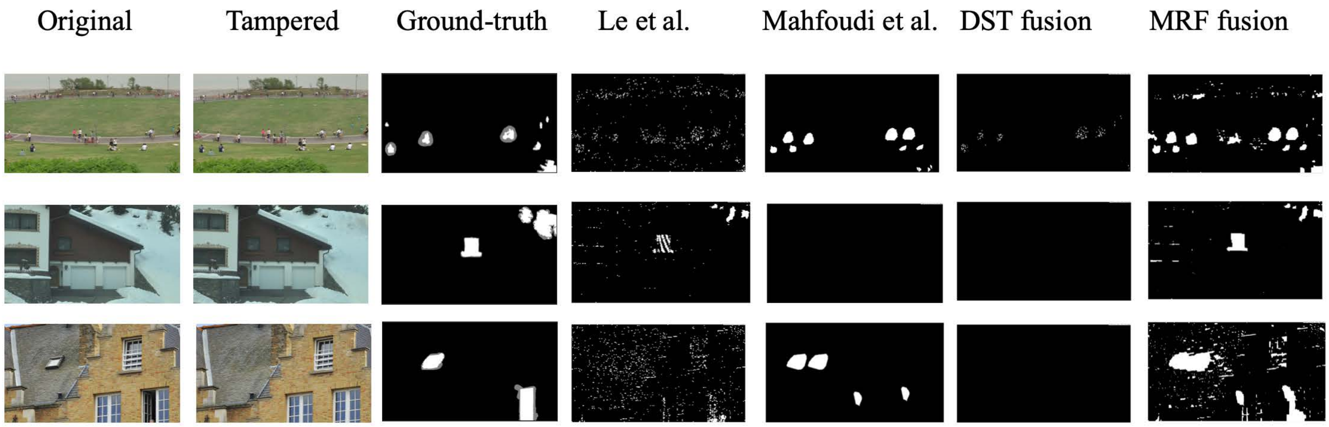

FIGURE 7. The decision maps of some images from the dataset of Korus [26].

In Bayesian fusion method we have to pay a cost for building the edge struct of Markov Random Field and the computing complexity for finding the optimization on the graph.

In the first experiment, on a particular dataset, DST method outperforms the Bayesian fusion method. In this case, the maps obtaining from two forensic algorithms usually have some common tampered parts and some conflicting parts (see Fig. 1). Those conflicting parts include false detection parts of the PRNU on the saturated regions and false detection parts of the SF based detector. The DST fusion technique succeeds in choosing the common parts and ignoring the conflicting parts thereby enhancing the performance. However, this is not the case of Bayesian fusion. From a Bayesian perspective, the Bayesian fusion needs more prior information about this conflict. In other words, the Bayesian fusion requires the knowledge about the reliability of the both forensic detectors, i.e., what is the probability that the forensic algorithm decides the given pixel is tampered. The readers can find more explanation about Bayesian approach to fuse conflicting information in [64]. Thus we think that it is possible that Bayesian fusion technique can be improved its performance if we are given more prior information about each tampering map [25], [26].

In the second experiment, the MRF based fusion gives considerable improvement comparing to the DST based fusion technique. It turns out that the strength of the DST based fusion method mentioned in the first experiment is its disadvantage in the second experiment. More particularly, the limitation in dealing with the conflict evidence prevents the DST based fusion from combining the copy-paste and copy-move tampering. The disadvantage of the MRF based fusion method in the first experiment is the strength for the second experiment. Exploiting the spatial dependencies of neighborhood pixels of MRF based fusion method has significantly enhanced the detection performance in the second context. Therefore, it could be said that the choice of the best fusion technique depends on the problem under consideration, on the properties and characteristics of each individual algorithm.

V. CONCLUSION

This paper has provided a systematic review on the state-of-the-art of fusion techniques applying in detecting and localizing forgery images domains. We then have proposed two effective fusion techniques, DST and Bayesian, to aggregate the tampering maps. Two fusion scenarios have been considered and experimental results have been tested on two different datasets. In the first scenario, the fusion method is applied to aggregate the decision maps of PRNU based approach and SF based approach. Preliminary experimental results have shown that DST fusion method outperforms the Bayesian fusion method on a particular dataset. This improvement is mainly due to the fact that the DST fusion method has significantly decreased the false positive rate on the saturated and dark regions which is one of the most challenging limitation of the PRNU based approach. In the second scenario, the fusion method is applied to integrate the decision maps of the algorithm based on demosaicing artifacts and the one based on SIFT key-points and descriptors. The experimental results have shown that MRF fusion has considerably performed better than the DST fusion. The ability to exploit the spatial dependencies of neighborhood pixels in the decision maps has leveraged the detection performance of MRF based fusion technique.

We have concluded that the final choice for a fusion framework depends on the scenarios, the properties of each individual forensic algorithm and requirements of the user.

In this paper, we have just considered the very basic setting and conditions on two fusion methods. As a topic for further research, we shall devote to analyzing more deeply on each fusion method. Particularly, the limitation of the traditional DST fusion when dealing with conflict evidence shall be studied further [65]. Moreover, we shall consider more advanced combination rules in DST fusion such as the transferable belief model (TBM) [66] and Dezert-Smarandache theory (DSmT) [67]. Various dataset and more prior information for Bayesian method will be provided to have a thorough comparison between these two methods.

REFERENCES

[1] H. Farid, "Image forgery detection," *IEEE Signal Process. Mag.*, vol. 26, no. 2, pp. 16–25, Mar. 2009.

[2] D. Kundur and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proc. IEEE*, vol. 87, no. 7, pp. 1167–1180, Jul. 1999.

[3] C. Rey and J.-L. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP J. Adv. Signal Process.*, vol. 2002, no. 6, pp. 613–621, Dec. 2002.

[4] M. Schneider and S.-F. Chang, "A robust content based digital signature for image authentication," in *Proc. 3rd IEEE Int. Conf. Image Process.*, Sep. 1996, pp. 227–230.

[5] H. Farid, "Creating and detecting doctored and virtual images: Implications to the child pornography prevention act," Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep., TR2004-518, 2004, p. 970, vol. 13.

[6] G. Chierchia, G. Poggi, C. Sansone, and L. Verdoliva, "A Bayesian-MRF approach for PRNU-based image forgery detection," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 554–567, Apr. 2014.

[7] G. Chierchia, G. Poggi, C. Sansone, and L. Verdoliva, "PRNU-based forgery detection with regularity constraints and global optimization," in *Proc. IEEE 15th Int. Workshop Multimedia Signal Process. (MMSP)*, Sep. 2013, pp. 236–241.

[8] X. Lin and C.-T. Li, "Refining PRNU-based detection of image forgeries," in *Proc. Digit. Media Ind. Academic Forum (DMIAF)*, Jul. 2016, pp. 222–226.

[9] C.-H. Choi, H.-Y. Lee, and H.-K. Lee, "Estimation of color modification in digital images by CFA pattern change," *Forensic Sci. Int.*, vol. 226, pp. 94–105, Mar. 2013.

[10] A. Singh, G. Singh, and K. Singh, "A Markov based image forgery detection approach by analyzing CFA artifacts," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 28949–28968, 2018.

[11] H. Nguyen, F. Retraint, F. Morain-Nicolier, and A. Delahaies, "An image forgery detection solution based on DCT coefficient analysis," in *Proc. 5th Int. Conf. Inf. Syst. Secur. Privacy*, 2019, pp. 487–494.

[12] T. Bianchi and A. Piva, "Image forgery localization via block-grained analysis of JPEG artifacts," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1003–1017, Jun. 2012.

[13] J. He, Z. Lin, L. Wang, and X. Tang, "Detecting doctored JPEG images via DCT coefficient analysis," in *Proc. Eur. Conf. Comput. Vis.* Cham, Switzerland: Springer, 2006, pp. 423–435.

[14] J. Lukáš, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," *Proc. SPIE*, vol. 6072, Feb. 2006, Art. no. 60720Y.

[15] M. Schmitt and X. X. Zhu, "Data fusion and remote sensing: An ever-growing relationship," *IEEE Geosci. Remote Sens. Mag.*, vol. 4, no. 4, pp. 6–23, Dec. 2016.

[16] W. Ding, X. Jing, Z. Yan, and L. T. Yang, "A survey on data fusion in Internet of Things: Towards secure and privacy-preserving fusion," *Inf. Fusion*, vol. 51, pp. 129–144, 2019.

[17] A. Ghulam, "Monitoring tropical forest degradation in betampona nature reserve, madagascar using multisource remote sensing data fusion," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 7, no. 12, pp. 4960–4971, Dec. 2014.

[18] S. Delalieux, P. J. Zarco-Tejada, L. Tits, M. Á. J. Bello, D. S. Intrigliolo, and B. Somers, "Unmixing-based fusion of hyperspatial and hyperspectral airborne imagery for early detection of vegetation stress," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 7, no. 6, pp. 2571–2582, Jun. 2014.

[19] M. Pedergnana, P. R. Marpu, M. D. Mura, J. A. Benediktsson, and L. Bruzzone, "Classification of remote sensing optical and LiDAR data using extended attribute profiles," *IEEE J. Sel. Topics Signal Process.*, vol. 6, no. 7, pp. 856–865, Nov. 2012.

[20] A. P. James and B. V. Dasarathy, "Medical image fusion: A survey of the state of the art," *Inf. Fusion*, vol. 19, pp. 4–19, Sep. 2014.

[21] M. Yin, X. Liu, Y. Liu, and X. Chen, "Medical image fusion with parameter-adaptive pulse coupled neural network in nonsubsampled shearlet transform domain," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 1, pp. 49–64, Jan. 2018.

[22] M. Singh, R. Singh, and A. Ross, "A comprehensive overview of biometric fusion," *Inf. Fusion*, vol. 52, pp. 187–205, Dec. 2019.

[23] M. Kharrazi, H. T. Sencar, and N. Memon, "Improving steganalysis by fusion techniques: A case study with image steganography," in *Transactions on Data Hiding and Multimedia Security I*. Cham, Switzerland: Springer, 2006, pp. 123–137.

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

[25] P. Korus and J. Huang, "Multi-scale fusion for improved localization of malicious tampering in digital images," *IEEE Trans. Image Process.*, vol. 25, no. 3, pp. 1312–1326, Mar. 2016.

[26] P. Korus and J. Huang, "Multi-scale analysis strategies in PRNU-based tampering localization," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 809–824, Apr. 2017.

[27] M. Fontani, T. Bianchi, A. D. Rosa, A. Piva, and M. Barni, "A framework for decision fusion in image forensics based on Dempster–Shafer theory of evidence," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 4, pp. 593–607, Apr. 2013.

[28] T. Bianchi, A. D. Rosa, and A. Piva, "Improved DCT coefficient analysis for forgery localization in JPEG images," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 2444–2447.

[29] T. Bianchi and A. Piva, "Analysis of non-aligned double JPEG artifacts for the localization of image forgeries," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, Nov. 2011, pp. 1–6.

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

[31] T. Bianchi, A. De Rosa, and A. Piva, "Improved DCT coefficient analysis for forgery localization in JPEG images," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2011, pp. 2444–2447.

[32] P. Korus and J. Huang, "Evaluation of random field models in multi-modal unsupervised tampering localization," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2016, pp. 1–6.

[33] H. Li, W. Luo, X. Qiu, and J. Huang, "Image forgery localization via integrating tampering possibility maps," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1240–1252, May 2017.

[34] A. T. P. Ho and F. Retraint, "Effective images splicing detection based on decision fusion," in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol. (ISSPIT)*, Dec. 2019, pp. 1–5.

[35] M. Barni and A. Costanzo, "Dealing with uncertainty in image forensics: A fuzzy approach," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2012, pp. 1753–1756.

[36] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery localization through the fusion of camera-based, feature-based and pixel-based techniques," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 5302–5306.

[37] D. Cozzolino, D. Gragnaniello, and L. Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2014, pp. 5297–5301.

[38] L. Gaborini, P. Bestagini, S. Milani, M. Tagliasacchi, and S. Tubaro, "Multi-clue image tampering localization," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2014, pp. 125–130.

[39] J. Sander and J. Beyerer, "Bayesian fusion: Modeling and application," in *Proc. Workshop Sensor Data Fusion: Trends, Solutions, Appl. (SDF)*, Oct. 2013, pp. 1–6.

[40] P. Ferrara, M. Fontani, T. Bianchi, A. D. Rosa, A. Piva, and M. Barni, "Unsupervised fusion for forgery localization exploiting background information," in *Proc. IEEE Int. Conf. Multimedia Expo. Workshops (ICMEW)*, Jun. 2015, pp. 1–6.

[41] M. Fontani, E. Argones-Rua, C. Troncoso, and M. Barni, "The watchful forensic analyst: Multi-clue information fusion with background knowledge," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Nov. 2013, pp. 120–125.

[42] G. Chetty and M. Singh, "Nonintrusive image tamper detection based on fuzzy fusion," *Int. J. Comput. Sci. Netw. Secur.*, vol. 10, no. 9, pp. 86–90, 2010.

[43] M. Barni and A. Costanzo, "A fuzzy approach to deal with uncertainty in image forensics," *Signal Process., Image Commun.*, vol. 27, no. 9, pp. 998–1010, 2012.

[44] M. Kaur and S. Gupta, "A fusion framework based on fuzzy integrals for passive-blind image tamper detection," *Cluster Comput.*, vol. 22, no. 5, pp. 11363–11378, 2017.

[45] L. I. Kuncheva, *Combining Pattern Classifiers: Methods Algorithms*. Hoboken, NJ, USA: Wiley, 2014.

[46] D. Cozzolino, F. Gargiulo, C. Sansone, and L. Verdoliva, "Multiple classifier systems for image forgery detection," in *Proc. Int. Conf. Image Anal. Process.* Cham, Switzerland: Springer, 2013, pp. 259–268.

[47] W. Li, Y. Yuan, and N. Yu, "Passive detection of doctored JPEG image via block artifact grid extraction," *Signal Process.*, vol. 89, no. 9, pp. 1821–1829, 2009.

[48] B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 529–538, Sep. 2008.

[49] A. Ferreira, S. C. Felipussi, C. Alfaro, P. Fonseca, J. E. Vargas-Munoz, J. A. dos Santos, and A. Rocha, "Behavior knowledge space-based fusion for copy–move forgery detection," *IEEE Trans. Image Process.*, vol. 25, no. 10, pp. 4729–4742, Oct. 2016.

[50] B. Liu and C.-M. Pun, "Deep fusion network for splicing forgery localization," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Sep. 2018, pp. 237–251.

[51] Y. Liu, Q. Guan, X. Zhao, and Y. Cao, "Image forgery localization based on multi-scale convolutional neural networks," in *Proc. 6th ACM Workshop Inf. Hiding Multimedia Secur.* New York, NY, USA: ACM, 2018, pp. 85–90.

[52] S. Z. Li, *Markov Random Field Modeling in Image Analysis*. Cham, Switzerland: Springer, 2009.

[53] Y. Boykov, O. Veksler, and R. Zabih, "Fast approximate energy minimization via graph cuts," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 11, pp. 1222–1239, Nov. 2001.

[54] Y. Boykov and V. Kolmogorov, "An experimental comparison of min-cut/max-flow algorithms for energy minimization in vision," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 26, no. 9, pp. 1124–1137, Sep. 2004.

[55] M. Schmidt. (2007). *UGM: A MATLAB Toolbox for Probabilistic Undirected Graphical Models*. [Online]. Available: http://www.cs.ubc.ca/~schmidtm/Software/UGM.html

[56] G. Shafer, *A Mathematical Theory of Evidence*, vol. 42. Princeton, NJ, USA: Princeton Univ. Press, 1976.

[57] A. P. Dempster, "Upper and lower probability inferences based on a sample from a finite univariate population," *Biometrika*, vol. 54, nos. 3–4, pp. 515–528, 1967.

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

[59] M. Goljan, J. Fridrich, and R. Cogranne, "Rich model for steganalysis of color images," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, Dec. 2014, pp. 185–190.

[60] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 432–444, Apr. 2012.

[61] O. M. Al-Qershi and B. E. Khoo, "Evaluation of copy-move forgery detection: Datasets and evaluation metrics," *Multimedia Tools Appl.*, vol. 77, no. 24, pp. 31807–31833, 2018.

[62] N. Le and F. Retraint, "An improved algorithm for digital image authentication and forgery localization using demosaicing artifacts," *IEEE Access*, vol. 7, pp. 125038–125053, 2019.

[63] G. Mahfoudi, F. Morain-Nicollier, F. Retraint, and M. Pic, "Copy and move forgery detection using SIFT and local color dissimilarity maps," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Nov. 2019, pp. 1–5.

[64] S. Maskell, "A Bayesian approach to fusing uncertain, imprecise and conflicting information," *Inf. Fusion*, vol. 9, no. 2, pp. 259–277, Apr. 2008.

[65] J. Chen, F. Ye, T. Jiang, and Y. Tian, "Conflicting information fusion based on an improved DS combination method," *Symmetry*, vol. 9, no. 11, p. 278, Nov. 2017.

[66] P. Smets and R. Kennes, "The transferable belief model," *Artif. Intell.*, vol. 66, no. 2, pp. 191–234, Feb. 1994.

[67] F. Smarandache and J. Dezert, *Advances and Applications of DSmT for Information Fusion: Collected Works*, vol. 14. Coimbatore, India: Infinite Study, 2015.

ANH-THU PHAN-HO received the M.Sc. degree in applied mathematics from the University of Orleans, France, in 2011, and the Ph.D. degree in image processing from the University of Technology and Sciences of Lille, France, in 2014. Since 2015, she has been working as a Postdoctoral Researcher at the GIPSA Laboratory, Grenoble, L3i Laboratory, LM2S, and CRIStAL Laboratory, University of Lille. Her research interests include statistical image processing, statistical detection theory and steganalysis, with a main application to digital image forensics.

FLORENT RETRAINT received the M.Sc. degree in applied mathematics and the Ph.D. degree in image processing from the National Institute of Applied Sciences, Lyon, France, in 1994 and 1998, respectively. He is currently a Full Professor with the University of Technology of Troyes. His research interests include image modeling, statistical image processing, hypothesis testing theory, and anomaly detection and localization, with a main application to digital image forensics.