Reliable and Fast Forgery Detection using FINE GRAINED approach

P.VENEELA
M.Tech Scholar (DECS), Department of Electronics and Communications Engineering, Chaitanya Institute of Science & Technology, India.

S.SRIVIDYA
Assistant Professor, Electronics & Communications Engineering, Chaitanya Institute of Science & Technology, India.

Abstract: **Forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime. A digital forensic investigation commonly consists of 3 stages: acquisition or imaging of exhibits, analysis, and reporting. Previously, it is able to detect tampered images at high accuracy based on some carefully designed mechanisms,localization of the tampered regions in a fake image still presents many challenges, especially when the type of tampering operation is unknown. Later on, necessary to integrate different forensic approaches in order to obtain better localization performance. However, several important issues have not been comprehensively studied, to improve/readjust proper forensic approaches, and to fuse the detection results of different forensic approaches to obtain good localization results. In this paper, we propose a framework to improve the performance of forgery localization via implementing tampering possibility maps along with fusion based technique. In the proposed framework, we first select and improve existing forensic approaches, i.e., copy-move forgery detector and statistical feature based approach, and then improve their results to obtain tampering possibility maps.**

***KeyTerms*— Digital Forensic; Forgery Localization; Statistical Feature; Copy-Move Detection;**

I. Introduction

The term digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.[1] With roots in the personal computing revolution of the late 1970s and early 1980s, the discipline evolved in a haphazard manner during the 1990s, and it was not until the early 21st century that national policies emerged.

Digital forensics investigations have a variety of applications. The most common is to support or refute a hypothesis before criminal or civil courts. Criminal cases involve the alleged breaking of laws that are defined by legislation and that are enforced by the police and prosecuted by the state, such as murder, theft and assault against the person. Civil cases on the other hand deal with protecting the rights and property of individuals but may also be concerned with contractual disputes between commercial entities where a form of digital forensics referred to as electronic discovery (ediscovery) may be involved.

Forensics may also feature in the private sector; such as during internal corporate investigations or intrusion investigation.

The technical aspect of an investigation is divided into several sub-branches, relating to the type of digital devices involved; computer forensics, network forensics, forensic data analysis and mobile device forensics. The typical forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.

In this paper, we propose an improved framework to deal with the problem of image forgery localization. The proposed framework first analyzes the input image using a statistical feature based detector and a copy-move forgery detector, respectively. The results of the two approaches are then converted into tampering possibility maps. By analyzing the properties of tampering possibility maps, we employ a simple yet very effective strategy to obtain the localization result. Compared with the existing methods [31], [32], the main contribution of this paper is to propose a fusion scheme based on tampering possibility maps. The main efforts in our work are as follows. Firstly, after analyzing the most popular tampering operations (splicing/erasing and copy-move) in real cases, we choose two forensic approaches and improve them for forgery localization. Although fewer forensic approaches are utilized compared to existing methods, we still significantly boost the overall performance. Secondly, unlike the existing methods that use binary maps, we convert the results of the adopted approaches into maps with continuous values ranging from 0 to 1, which indicate the tampering possibilities of the corresponding pixels. In this way, we can preserve more useful intermediate information of each approach and predict whether a pixel is pristine or fake more reliably. Compared to the binary maps, the tampering possibility maps are able to reduce the false positives and false negatives significantly based on our experiments. Finally and more importantly, the fusion method for

integrating tampering possibility maps is newly designed. By analyzing the properties of tampering possibility maps, we integrate the two tampering possibility maps with a carefully designed decision curve, which can more or less keep the advantages of both approaches and make them complement each other for forgery localization. The extensive experiments show that our framework can achieve the highest F1-score of 0.4925 in the IFS-TC Image Forensics Challenge.

II. Related Work

Cao et al [1] proposes a novel exact identification structure of demosaicing normality from various source pictures. This paper talks about the turn around arrangement of the demosaiced tests into a few classifications and afterward assessing the basic demosaicing recipes for every classification dependent on fractional second-request subsidiary connection models, which identify both the intra-channel and the cross-channel demosaicing relationship. An arrangement conspire called desire expansion turn around is utilized to iteratively resolve the uncertain demosaicing tomahawks so as to best uncover the understood gathering received by the hidden demosaicing calculation. The disadvantage of this strategy is that commotion variety discovery should be joined. Dirik and Memon [7] proposes an identification technique that uses the antiques created by the shading channel exhibit (CFA) handling in most computerized cameras. Here, two CFA highlights are extricated and methods are created dependent on these highlights. The strategies depend on figuring a solitary element and a straightforward edge based classifier. The restriction of the method proposed here is that this procedure is touchy to solid JPEG re-pressure and resizing. Mahdian and Saic proposed in [20], phony recognition strategies, where the picture commotion in textures are considered for the discovery of hints of altering. A division technique that distinguishes changes in clamor level is proposed here. A usually utilized device to cover the hints of altering is the expansion of locally irregular commotion to the changed picture areas. The commotion debasement is the primary purpose behind the disappointment of numerous dynamic or detached picture phony identification strategies. Normally, the measure of clamor is uniform over the whole true picture. Including locally arbitrary clamor may make irregularities in the picture's commotion. Hence, the altering can be found by the location of different commotion levels inan picture may connote. The strategy proposed in this paper is equipped for isolating a researched picture into different allotments with homogenous clamor levels. The nearby commotion estimation depends on tiling the high pass wavelet coefficients at the most noteworthy goals with non-covering squares. The clamor standard deviation of each square is evaluated utilizing the broadly utilized middle based strategy. The standard deviation of clamor is utilized as the homogeneity condition to fragment the explored picture into a few homogenous sub-districts. This strategy can be utilized as a valuable alongside other visually impaired falsification recognition undertakings, however the constraint is that the technique comes up short at whatever point the debasement of clamor is extremely little. Gallagher and Chen present an idea dependent on the demosaicing highlights. Instead of concentrating on the measurable contrasts between the picture surfaces, the component of pictures from advanced cameras are perceived to contain hints of resampling because of utilizing a shading channel cluster with demosaicing calculations. Here the estimation of the real demosaicing parameters isn't really considered; rather, discovery of the nearness of demosaicing is contemplated. The in camera handling (as opposed to the picture content) recognizes the computerized camera photos from COMPUTER designs. The nearness of demosaicing is an agenda being utilized in this identification calculation. The downside is that if a pernicious COMPUTER illustrator wishing to add a component of authenticity to her COMPUTER realistic pictures could basically embed a product module to reproduce the impact of shading channel cluster testing and afterward apply demosaicing. Here this calculation may fall flat, and hence this kind of calculation isn't a successful method to manage such assaults.

II. Forensic Approaches

Forgery localization usually employed several forensic approaches in their frameworks will describe and analyze as

A. Copy-move detection based approach. Copy-move detection tries to find the duplicate regions within an image. Many effective methods have been proposed previously, such as. The three works mentioned above used the image editing technique PatchMatch to find the similar patches, and then further determined the copy-move regions. As reported in their papers, copy- move detection made major contributions to the overall localization performance. However, copy-move detection cannot differentiate between the original regions from the copied regions, and thus always gives some ambiguous results. On the other hand, such methods are very specific. If there is no copy-move operation involved in the tampering procedure or the tampered region comes from another image, copy-move detection probably produces some inaccurate tampered regions and thus confuses the localization results.

B. Near-duplicate detection based approach, introduced an approach based on near-duplicate image analysis. For a testing image, the approach first finds its near-duplicate images in the database. After registering a pair of near-duplicate images, their differences are computed and those regions with large differences are regarded as tampered regions. Although it would suffer

ambiguity problems, such a method works well when some near-duplicate images for the testing images are available. However, such an ideal situation would seldom happen in practice, and thus the use of near-duplicate detection based approach is limited.

C. Sensor pattern noise based approach. As a reliable and unique fingerprint for a camera, sensor pattern noise can help to evaluate the integrity of an image taken by the same camera. By estimating the sensor pattern noise from the testing images, the tampered regions can be revealed by checking the compatibility of sensor pattern noise block by block. Although such a method can deal with many types of manipulations, its localization resolution1 is limited since it needs sufficient pixels for comparing the sensor pattern noise. Furthermore, for a given image in practice, it is hard to obtain the sensor pattern noise of its acquisition camera.

D. Statistical feature based approach. By adopting sliding- window strategy to extract forensic features from each image patch and feed them into a pre-trained classifier, it is possible to identify some tampered regions, such as patches from different image sources or with different processing histories. The statistical feature based approaches can be applied to any image under investigation. However, since it relies on machine learning techniques for training and testing, there would probably be some erroneous results. Thus, we should carefully select the features and the related parameters in order to control the error rates.

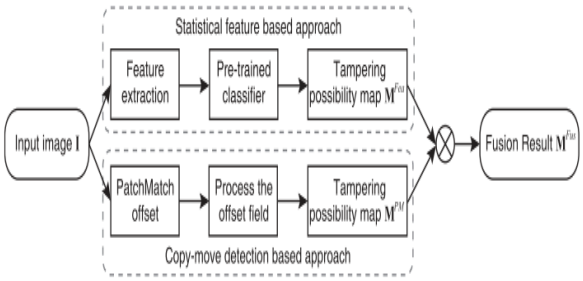

Fig. 1. Illustration of the proposed framework.

III. Design Scheme

First present the whole framework for forgery localization, and then introduce two improved forensic approaches used in the framework, respectively. Finally, we propose the fusion method for integrating the detection results of both approaches.

A. The Proposed Framework

The proposed forgery localization framework is illustrated in Fig. 1. This framework consists of the following two steps.

Step #1: Producing the possibility map for each forensic approach. In this step, we use two different forensic approaches, i.e., a statistical feature based approach and a copy-move detection based approach, to analyze the given image. The main reason for choosing the former approach is that some advanced steganalytic features can detect various image operations based on our previous work [7], and we expect that such features can achieve good performance in detecting image splicing/erasing operations, which are commonly used in image tampering. However, the statistical feature based approaches cannot perform well in detecting another popular used operation, copy-move. Thus, the copy-move detector is included as a complement. Please note that the methods based on sensor pattern noise and near duplicate analysis are not considered in the proposed framework due to their limitations described in Section II. In this work, we carefully improve the two selected approaches. What is more, unlike the existing methods, we produce a tampering possibility map for each approach, which is very helpful for the subsequent fusion step. Please refer to Section III-B and Section III-C for more details.

Step #2: Fusing the possibility maps to locate the tampering regions. In this step, we try to obtain the final localization result via combining the possibility maps obtained in the first step. Recently, some fusion methods have been proposed for forgery localization, such as. Unlike the exiting methods, in the proposed framework, we carefully analyze the distributions of the values within the tampering possibility maps for pristine and fake pixels, and design a decision curve to differentiate between pristine and fake pixels. Please refer to Section III-D for more details.

B. Statistical Feature Based Approach

Splicing and erasing some objects within an image are the most popular tampering operations in practice. Furthermore, some pre-operations such as scaling and rotation, and some post-operations such as boundary blurring, contrast/color adjustment, are applied to make the tampered regions more consistent with the whole image. All the operations involved in splicing and erasing would inevitably distort some inherent relationships among the adjacent pixels within a pristine image. Based on our analysis in previous work [1], some steganalytic features can effectively identify such manipulations. Thus, we try to use such features to locate tampered regions.

We decided to use the feature set named spatial and color rich model (SCRM) [6] in the proposed framework. SCRM is designed with an analogous mechanism as SRM. For a color image, it respectively extracts SRM features from the R, G, and B channel and adds them

together, and then concatenates them with another subset of features that consists of co-occurrence matrices computed on image residuals of the three color channels.

In the testing stage, the given images are also analyzed by a 64x64-pixel sliding-window with a step of 16-pixel. For each block, 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 lower the v is, the more likely the block is fake, and vice versa. We use a map M^{Fea}_v with the same size of the image I to record the mean of the vote scores assigned to each pixel, and then

$$\mathbf{M}_{i,j}^{Fea_v} = \frac{1}{2n_b}\left(\frac{1}{K}\sum_{k=1}^{K} v_k + n_b\right), \qquad (1)$$

normalize the map into the range 0, 1. Such procedures can be formulated as follows.

where K is the number of blocks containing Ii, j, and vk is the vote score for the kth block that contains Ii, j . Since the block size is 64 64 and the step is 16, K 16 for most pixels, while K is less for the pixels near the image boundaries. It is noted that MFeav indicates the possibility of that the pixel has been tampered with. For example, a pixel Ii, j with a lower value of MFeav is more likely to be fake.

In Fig. 2, we show some results of the statistical feature based approach. Fig. 2 (a) and (e) are two pristine images. We copied the fire extinguisher logo from (e) and pasted it into (a), obtaining a fake image as shown in (b). We just slightly modified the edges of the logo and kept its shape and brightness, so there are only some weak responses in the corresponding result (f). The result is reasonable because most pixels of the splicing region have not been modified. Since the logo looks quite unnatural in (b), we further adjusted its shape and brightness, as shown in (c). In this case, most tampered pixels exhibit strong responses (very low values) in the resulting map (g). For another example in (d), the logo on the dustbin, the switch and the electric wire in (a) are erased by filling the regions. The corresponding result is shown in (h). It can be clearly seen that the tampered regions within the resulting map contains low values. From these examples, we can observe that the feature based approach can effectively reveal the splicing and erasing tampered regions. Because the error rate of the trained classifier is 15%, there would naturally be some false positives such as the black region close to the left bottom corner in Fig. 2 (f)-(h). Fortunately, they may be identified as pristine ones again in the fusion step; thus, the false positives would be further eliminated in the final localization results.

Since the step of sliding-window is 16-pixel, there are mosaic artifacts appearing in the map M^{Fea}_v, which can easily be seen in Fig. 2 (f)-(h). Naturally, it is expected that the map for an image tends to be smoother, so we apply mean filtering with 64-pixel window for obtaining a smoothed map M^{Fea},

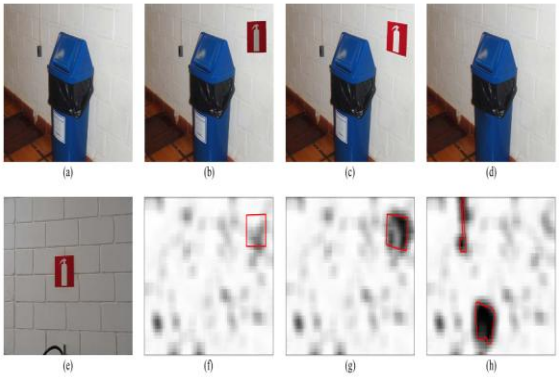

Fig. 2. Example results of the feature based approach. (a) and (e): pristine images. (b)-(d): fake images. (f)-(h): the corresponding results for (b)-(d).

$$\mathbf{M}_{i,j}^{Fea} = \frac{1}{64^2}\sum_{i'=-32}^{31}\sum_{j'=-32}^{31}\mathbf{M}_{i+i',j+j'}^{Fea_v}. \qquad (2)$$

Based on our experimental results in Section IV-A1, the above smoothing operation can indeed improve the forgery localization performance.

C. Copy-Move Detection Based Approach

Copy-move is another commonly used operation in image tampering. It copies one or more regions and then pastes them to the same image. Sometimes, post-operations are used to refine the tampered regions. Since the tampered regions come from an original untouched source, the inherent relationships among adjacent pixels within

1) Denote a 7 × 7 square image patch centered at pixel $I_{i,j}$ as $S_7(I_{i,j})$. For each $S_7(I_{i,j})$, we first use the PatchMatch algorithm to compute its four nearest neighbors $S_7(I_{pk,qk})$ within the same image, where k = 1, 2, 3, 4.

The numbers on the vertical bar indicate the probabilities of pixel occurrences. and |.| for a set means the number of its elements. In this way, the lower $M^{PM}_{i,j}$, the more likely that $I_{i,j}$ belongs to copy-moved regions.

The reason why we apply four nearest neighbours rather than only one as in the existing methods is that the PatchMatch algorithm involves a random initialization. If only one nearest neighbor is searched, the duplicate regions cannot be fully found in some cases, or there will be noisy results. Besides, more than one region may be copied from the same source in practice. Two examples

are shown in they can complement each other and better results can be obtained, as shown in the sixth column of Fig. 3. Due to the limitation of copy- move detection, we cannot differentiate between the source regions and the tampered regions. However, such a limitation could be overcome in some cases if the results of the feature based approach are combined. We show the results of the feature based approach in the right most column of Fig. 3. It is noted that the feature based approach produces many false decisions in these cases, implying that it cannot detect copy-move forgery effectively.

D. Fusion of Tampering Possibility Maps

In this subsection, we aim to define a fusion function $\Delta(M^{Fea}_{i,j}, M^{PM}_{i,j})$ to determine whether the test pixel $I_{i,j}$ in an image is pristine or fake. In the ideal case, the fusion function should output 1 for a pristine pixel and output 0 for a fake pixel.

To this end, by regarding the pixels belonging to the tampered regions as fake pixels and the rest as pristine ones, we select about 40 million fake pixels in the 442 training fake images of the IFS-TC Image Forensics Challenge corpus, and then randomly select the same number of pristine pixel in these images. Fig. 4 shows the normalized distributions of pristine pixels and fake pixels in the M^{Fea} -M^{PM} plane with a step of 0.02. In Typically, we can use some machine learning techniques to train a binary classifier (i.e., the fusion function) based on the training samples. However, it is not easy to do so in this problem due to the following reasons. First of all, by comparing the distributions between pristine and fake pixels in Fig. 4, it is expected that linear classifiers would not be suitable. If non-linear classifiers such as support vector machine (SVM) with Gaussian kernel are used, more parameters have to be tuned. Thus the training stage would be time-consuming due to the huge number of training samples. Second, even if a pre-trained non-linear classifier is available, the time spent on testing a single image is not acceptable since typically there are over 1 million pixels within an image. Therefore, a fast and effective method is needed. Based on the distributions shown in Fig. 4, we try to manually design a decision curve with fewer parameters, and work out the fusion function as follows.

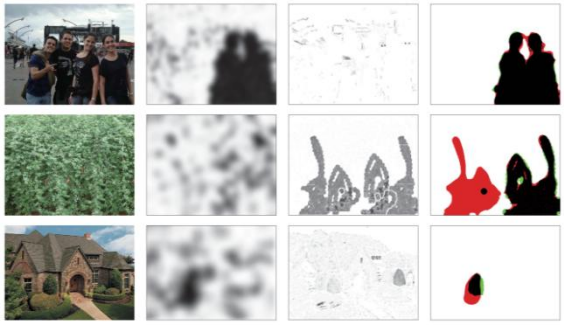

Fig. 3. Examples of fusion results. Column 1: input images. Column 2: the maps $\mathbf{M}^{Fea}$. Column 3: the maps $\mathbf{M}^{PM}$. Column 4: the fusion maps $\mathbf{M}^{Fus}$. In the fusion results, the pixels in black, white, red, and green indicate true positive, true negative, false positive, and false negative, respectively. Here positive means fake pixel, while negative means pristine pixel.

$$\Delta\left(\mathbf{M}^{Fea}_{i,j}, \mathbf{M}^{PM}_{i,j}\right) = \mathbb{1}\left(\left(\mathbf{M}^{Fea}_{i,j}\right)^{\lambda_1} \cdot \left(\mathbf{M}^{PM}_{i,j}\right)^{\lambda_2} \geq \tau\right), \quad (8)$$

where λ_1, λ_2 are parameters and $\tau \in (0, 1)$ is the threshold. $\mathbb{1}(\cdot)$ is an indicator function. The parameters λ_1 and λ_2 would respectively shift the levels of M^{Fea} and M^{PM} and thus determine the curvature of the decision curve, while τ determines the position of the decision curve.

Finally, we obtain λ_1=0.39, λ_2=4.26, and τ=0.48.

In this case, if we use the conventional fusion method, the region on the right with low values in MPM must be determined as fake. Fortunately, based on the proposed fusion strategy, we just detect the left region as fake, avoiding a larger number of false positives.

IV Experimental Results

In the experiments, we use the image corpus provided in the IFS-TC Image Forensics Challenge. The image corpus

TABLE I

F1 -Scores For Approaches Based On Statistical Features. The Value With An Asterisk " * " Denotes The Best

Detection Result

Method	F_1-score
Method in [31] (S3 feature, SVM)	0.1115
S3 feature, LDA ensemble	0.1737
Proposed (SCRM feature, LDA ensemble)	0.3458*
Proposed method without smoothing	0.3214

has 442 fake images for training and 700 fake images for testing, whose sizes vary from 640x480 to 4752x3168 (most images are 1024x768). The fake images are created with image editing software and cover various kinds of forgeries like splicing, erasing, copy-move, and so on. For the training images, their ground truth maps are available, while the ground truth maps for the testing images are not disclosed.

For a fair comparison, all of the results obtained for the testing images are submitted to the evaluation system of the challenge. According to the rules of the challenge, the forgery localization performance is evaluated with the F1-score as follows.

$$F_1 = 2 \cdot \frac{\text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} = \frac{2TP}{2TP + FN + FP}, \qquad (9)$$

where TP (true positive), FN (false negative), and FP (false positive) mean the number of detected fake pixels, undetected fake pixels, and wrongly detected pristine pixels, respectively.

A. Evaluation of Single Approach

In this subsection, we respectively evaluate the performance of the two approaches, and show that the proposed approaches can improve the performance of forgery localization compared with related approaches.

Furthermore, to validate the effectiveness of smoothing $\mathbf{M}^{Feav}$ described in Section III-B, the F1-score without smoothing is reported in the last row of Table I. It can be seen that the smoothing operation can improve F1-score by 2.44%.

TABLE II

F1 -Scores For Approaches Based On Copy-Move Detection. The Value With An Asterisk "*" Denotes The Best

Detection Result

Method	F_1-score
Method in [31]	0.3425
Method in [32]	0.2784
Method in [36]	0.1764
Proposed	0.3845*

2) Copy-Move Detection Based Approach: To evaluate the copy-move detection based approach, we obtain the binary map by thresholding $\mathbf{M}^{PM}$. After thresholding, we apply morphological operations to erase small regions and fill small holes. The use of morphological operations aims to obtain bet- ter performance, which has also been considered in previous works

Three related methods proposed are included for comparison. For the first two methods, the F_1-scores are reported in their papers. For the third method, we use the source code provided by the authors with default parameters to generate the results. Table II shows F_1-scores for testing images. From this table, it is observed that the proposed approach works the best, outperforming the second place (i.e., Method [31]) by 4% in terms of F_1-score.

A. Evaluation of the Whole Framework

The above subsection shows that the two proposed approaches outperform the corresponding related ones. In this subsection, we evaluate the performance of the whole proposed framework. Besides the two existing works the following six commonly used fusion methods are included to show the effectiveness of the proposed fusion method.

. OR *operator*. In this fusion method, a pixel is regarded as pristine if either of the two proposed approaches regards it as pristine.

. AND *operator*. In this fusion method, a pixel is regarded as pristine only if both proposed approaches regard it as pristine.

.

. *Discriminative random field (DRF).* Considering the forgery localization problem as a labeling problem,

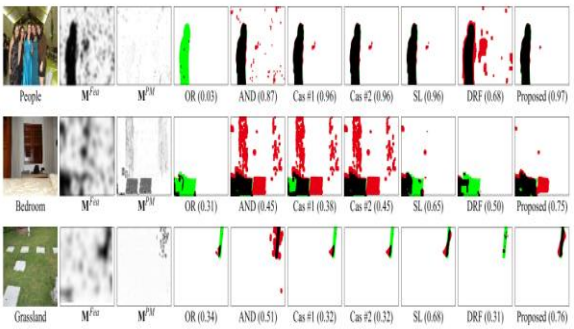

Fig. 4. Example fusion results for different methods. From the fourth to the right most column, the pixels in black, white, red, and green indicate true positive, true negative, false positive, and false negative, respectively.

Please note that the first four methods still need binary detection maps for fusion, while the latter two methods perform the fusion based on tampering possibility maps. Furthermore, the optimal parameters such as thresholds for the above methods are all obtained from the training data.

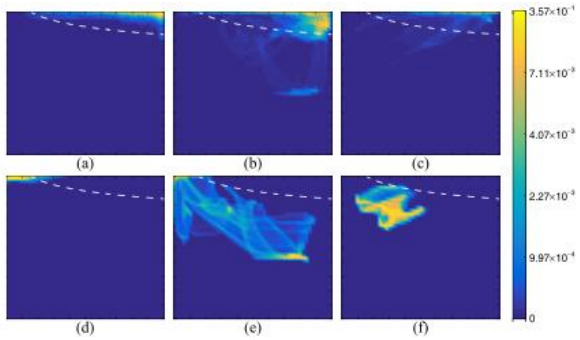

Fig. 5. The distributions of pristine and fake pixels in the MFea -MPM plane for the three examples in Fig. 6. (a)-(c): The distributions of pristine pixels in image "People", "Bedroom", and "Grassland", respectively. (d)-(f): The distributions of fake pixels in image "People", "Bedroom", and "Grassland", respectively. The white dashed curves indicate the designed decision curve.

To explain the superior performance of the proposed method, in Fig. 5 we show the distributions of pristine and fake pixels in the $\mathbf{M}^{Fea}$-$\mathbf{M}^{PM}$ plane for the three images "People", "Bedroom", and "Grassland", respectively. From Fig. 5, we can see that although the distributions are quite different due to different image contents, the pristine pixels are mainly located above the decision curve, and most fake pixels are located under the decision curve, which means that the proposed decision curve can effectively differentiate between the pristine and fake pixels in each single image. This can be demonstrated by the results in the right most column of Fig. 6, which are the most satisfactory results among all the evaluated methods. Although there are some false positives for the "Bedroom" example, it is noted that the proposed method has suppressed many false positives for the AND operator and cascade methods in the upper areas of the image. The reason is that the proposed method uses the tampering possibility map $\mathbf{M}^{PM}$, whose values in the upper areas are distinguishable from those in the bottom areas. It is also noted that the proposed method avoids many false negatives for the supervised learning based strategy, since we design the non- linear decision curve based on the distribution of elements within $\mathbf{M}^{Fea}$ and $\mathbf{M}^{PM}$, which is more suitable for classifying the pristine and fake pixels.

Table III shows the F_1-score evaluated on the testing images. Among the methods relying on binary maps (i.e., OR operator, AND operator, and the two cascade decision methods), the fusion based on the AND operator gives the best results.

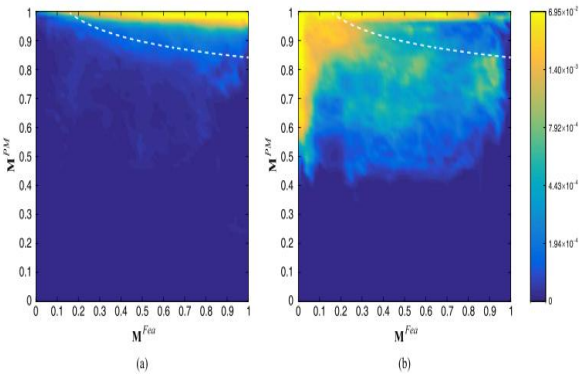

Fig. 6. The distributions of pristine pixels (a) and fake pixels (b) in the $\mathbf{M}^{Fea}$-$\mathbf{M}^{PM}$ plane for 50 images not belonging to the IFS-TC Image Forensics Challenge corpus. The white dashed curves indicate the designed decision curve. The numbers on the vertical bar indicate the probabilities of pixel occurrences.

TABLE III

F1 -Scores For Different Framework's Fusion Results. The Value With An Asterisk " * " Denotes The Best Detection Result

Method	F_1-score
Method in [31]	0.4072
Method in [32]	0.4533
OR	0.2684
AND	0.4447
Cascade #1	0.3658
Cascade #2	0.3700
Supervised learning	0.4007
DRF	0.1178
Proposed	0.4925*

Benefiting from the improvements of our two approaches, the F_1-score of the fusion method based on the AND operator becomes commensurate with that of the method. It is also noted that only the AND operator outperforms both of the single approaches among the fusion methods based on binary maps. For the two comparative methods based on tampering possibility maps (i.e., SL and DRF), the supervised learning method gives a barely satisfactory result, while the method based on DRF does not work well at all. The reason for the unsatisfactory result of DRF may be that its output localization map is highly dependent on the randomly initialized weights. Among all the methods, the proposed method achieves the highest F_1-score of 0.4925, and outperforms the best existing method by about 4%, implying a significant improvement in image forgery localization.

C. Discussion

In this subsection, we will discuss the generalization per- formance and shortcoming of the proposed method. Some potential ways for further improving the performance are presented as well.

1. Test on Other Images: Firstly, we would like to discuss the performance on other images not belonging to the IFS-TC Image Forensics Challenge corpus. To this end, we collected 50 fake images created by our colleagues and then applied the proposed method for locating the tampered regions. Please note that all of the parameters of our algorithms are set as those obtained from the training data of the IFS-TC Image Forensics Challenge corpus.

We show the distributions of pristine and fake pixels in the $\mathbf{M}^{Fea}$-$\mathbf{M}^{PM}$ plane for the 50 images in Fig. 8. Compared with Fig. 4, we can observe that: a) The distribution of the pristine pixels in the 50 testing images is very similar to that of the training images. They are always located at the upper right corner of the $\mathbf{M}^{Fea}$-$\mathbf{M}^{PM}$ plane. b) For the fake pixels, the corresponding distribution is somewhat different from that of the training data, since the performed tampering operations and their parameters for the testing and training images are usually not the same. c) Although the distributions of the fake pixels seem different, they are mainly located on the left side of the $\mathbf{M}^{Fea}$-$\mathbf{M}^{PM}$ plane. As a result, the decision curve can still effectively differentiate between the pristine and fake pixels.

Some examples of the localization results are shown in Fig. 9, from which we see that the tampered regions can be successfully detected. On average, the obtained F_1-score over the 50 testing images is 0.5361, meaning that the proposed method can achieve good performance on other images.

2. Shortcoming and Complementary Effects: Secondly, we would like to discuss one shortcoming of the copy-move detection based approach and the complementary effects of the two adopted forensic approaches.

Based on our experiments, the copy-move detection based approach can successfully reveal some slightly scaled and/or rotated copied objects. In order to show the robustness against scaling and rotation, we illustrate some examples in Fig.8, where the car near the center of each image is copied from the one at the left part of the image. We have respectively tested four different scaling factors and rotation angles. We observe that the copy-move detection algorithm can successfully identify the copied regions when the scaling is 5% or the rotation angle is less than 5, while it cannot effectively detect the copied regions when the scaling/rotation becomes stronger.

Although the copy-move detection based approach has such a shortcoming, it is interesting to observe that the strongly scaled and/or rotated objects would trigger higher responses in the map of the feature based approach, meaning that they can be detected by the feature based approach. By fusing their results, we can still locate the tampered regions as shown in the bottom row of Fig.8.

Fig. 7. Some examples for images not belonging to the IFS-TC Image Forensic Challenge corpus. Row 1: pristine images. Row 2: fake images (the tampered regions are highlighted with yellow curves). Row 3: localization results (F1-scores: 0.9298, 0.7562, 0.6679, 0.9612, 0.6777, 0.8508).

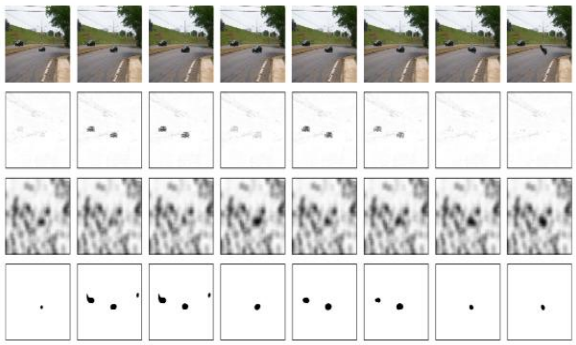

Fig. 8. The detection results for copy-moved forgeries with different scaling factors or rotation angles. The tampered region (copied object) is the cat near the center of the image. Column 1-4: the copied object is scaled with 0.8, 0.95, 1.05, and 1.2, respectively. Column 5-8: the copied object is rotated with 2°, 5°, 15°, and 45°, respectively. Row 1: the fake images. Row 2: results of copy-move detection based approach. Row 3: results of feature based approach. Row 4: fusion results (F1-scores: 0.3744, 0.4702, 0.4353, 0.5700, 0.5990, 0.6470, 0.4899, 0.4529).

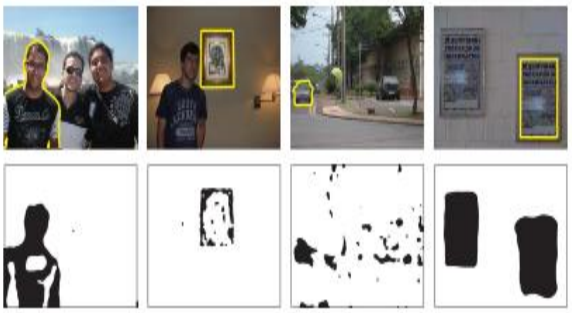

Fig.9. Some examples that can be further improved. Row 1: fake images (the tampered regions are highlighted with yellow curves). Row 2: the corresponding localization results of the proposed method.

3) Potential Ways for Improvement: Lastly, we will show some example results for the proposed framework to discuss some potential ways to further improve the localization performance.

Some simple methods may be effective for improving the above results. For instance, we can use some morphological operations to fill the holes and/or eliminate the small separated regions. However, it would not work well for some cases based on our experiments since the coves will never be filled and sometimes the holes are actually not the tampered regions, while the size of small separated regions is dependent on image contents. Furthermore, we can complement the fusion map with the help of some information based on image content and/or computer vision. For instance, we can segment the image into different semantic regions and compare the fusion map with the segmented regions. If most pixels within an image region or along the boundaries of a region are detected as fake in the fusion map, such a region is likely to be a tampered region. If some small regions are detected as fake stochastically, such regions may be declared as pristine. We may identify the tampered region in copy-move forgery by checking the consistency of illumination on the located regions. Furthermore, due to the complexity of tampering in practice, the localization results based on some fully-automatic frameworks may not be very convincing in some cases. Therefore, manual intervention is needed in practice after we obtain the localization results.

V. Conclusion

This method has addressed the issue successfully and is considerably faster than the existing method. It has detected forgery with good success rate in the image dataset. Also, it has shown robustness against Added Gaussian noise, JPEG compression and small amount of scaling and rotation. As an extension, focused main attention on the fine grained forgery localization problem. Here we have no prior knowledge about the tampered areas. We analyze artifacts left in the image by the interpolation process to reveal image forgery. In previous approaches for detecting forgeries either the area to be investigated has to be manually selected or also the automatic block processing but it results in poor detection performance. The results show that the proposed algorithm can be a valid tool for detecting and localizing forgeries in images acquired by Matlab.

References

[1] H.Farid,"Imageforgerydetection,"*IEEESignalProcess.Mag.*,vol.26, no. 2, pp. 16–25, Mar.2009.

[2] M. C. Stamm, M. Wu, and K. J. R. Liu, "Information forensics: An overview of the first decade," *IEEE Access*, vol. 1, pp. 167–200, May2013.

[3] J. Lukáš, J. Fridrich, and M. Goljan, "Detecting digital image forgeries using sensor pattern noise," *Proc. SPIE*, vol. 6072, p. 60720Y, Feb.2006.

[4] A. Swaminathan, M. Wu, and K. J. R. Liu, "Nonintrusive component forensics of visual sensors using output images," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 1, pp. 91–106, Mar.2007.

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

[6] W. Luo, Y. Wang, and J. Huang, "Detection of quantization artifacts and its applications to transform encoder identification," *IEEE Trans. Inf.ForensicsSecurity*,vol.5,no.4,pp.810–815,Dec.2010.

[7] Li, Y. Q. Shi, and J. Huang, "Detecting doubly compressed JPEG images by using mode based first digit features," in *Proc. IEEE 10th Workshop Multimedia Signal Process.*, Oct. 2008, pp.730–735.

[8] T. Bianchi and A. Piva, "Detection of nonaligned double JPEG com- pression based on integer periodicity maps," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 842–848,Apr. 2012.

[9] M. Stamm and K. J. R. Liu, "Blind forensics of contrast enhancement in digital images," in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2008, pp.3112–3115.

[10] G. Cao, Y. Zhao, R. Ni, and X. Li, "Contrast enhancement-based forensics in digital images," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 3, pp. 515–525,Mar. 2014.

