Abstract—In this work, we present a deep learning-based approach for image tampering localization fusion. This approach is designed to combine the outcomes of multiple image forensics algorithms and provides a fused tampering localization map, which requires no expert knowledge and is easier to interpret by end users. Our fusion framework includes a set of five individual tampering localization methods for splicing localization on JPEG images. The proposed deep learning fusion model is an adapted architecture, initially proposed for the image restoration task, that performs multiple operations in parallel, weighted by an attention mechanism to enable the selection of proper operations depending on the input signals. This weighting process can be very beneficial for cases where the input signal is very diverse, as in our case where the output signals of multiple image forensics algorithms are combined. Evaluation in three publicly available forensics datasets demonstrates that the performance of the proposed approach is competitive, outperforming the individual algorithms and providing a fused tampering localization map, that learns how to combine diverse input signals into a more accurate overall tampering localization visualization. Second, we present a fully automatic deep learning-based approach for tampering localization fusion. This approach for image tampering localization fusion is designed to combine the outcomes of multiple image forensics algorithms and provides a fused tampering localization map, which requires no expert knowledge and is easier to interpret by end users. Finally, the final output of our approach is easier to interpret and requires no additional specialized knowledge. This outcome can empower non-experts in image forensics, who are interested in image verification, e.g. fact-checkers and journalists, to actively contribute to image verification tasks.

The work presented in this paper is conducted in the context of the WeVerify project [8], which aims to build an open-source platform that engages communities and citizen journalists alongside newsroom and freelance journalists for collaborative and decentralized content verification, tracking, and debunking. For the content verification task, we build on the existing Image Verification Assistant [9], which is a tool that analyses the authenticity of images by visualizing the outcomes of various tampering localization approaches. For the purpose of WeVerify, we have extended this tool with new state-of-the-art algorithms but also by adding the presented fusion approach in order to enhance its usability by non-experts, including fact-checkers, journalists, and citizens.

In this work, we make the following contributions. First, we present a fully automatic deep learning-based approach that learns how to combine diverse input signals into a more accurate overall tampering localization visualization. Second, the final output of our approach is easier to interpret and requires no specialized knowledge by end users. Finally, the evaluation results show that the proposed fusion approach largely leads to better results compared to other approaches.

I. INTRODUCTION

Image forensics algorithms are crucial for determining the integrity of digital images. This is evident by the number of research efforts in the literature that deal with different types of digital manipulations and traces [1]. Designing algorithms for detecting and localizing a specific type of forgery has proven to be challenging, even when evaluating their performance on controlled datasets and settings [2]. The situation is even more difficult when dealing with online media. Images are manipulated multiple times with different tools and are then circulated over the Internet, further undergoing a variety of transformations (e.g., cropping, re-sizing, re-compression). Consequently, many methods suffer from low detection accuracy and localization robustness, presenting noisy outcomes and higher false-positive rates when applied to new datasets [2]. Due to these observations, many works posit that there is true benefit in acquiring different reports from independent algorithms and inspecting the multiple clues in tandem [3]–[6]. This is attributed to the fact that at least one or few of these diverse approaches are more likely to capture some tampering traces even after an image has undergone multiple transformations.

Although discovering manipulation traces is desirable, adding more forensics output visualizations increases the complexity of a media verification tool that presents the results, especially for non-expert users. The reason for this is that each algorithm has a different output that requires specific knowledge for proper interpretation. Consequently, this quickly becomes overwhelming for the non-expert. As a matter of fact, even forensics experts may provide wrong or contradicting interpretations of these visualizations [7].

In this paper, we aim to overcome these limitations, which often exclude non-expert users from the verification process of suspicious online images. The main objective is to develop a fully automatic fusion approach using deep learning, being able to leverage diverse forensics signals that are complementary to each other, so as to improve the robustness and reliability of the overall localization system. This final visualization retains the most important features of the individual algorithms and discards the noise. Additionally, another important objective is to communicate the tampering localization results to end users in a manner that is easier to interpret and requires no additional specialized knowledge. This outcome can empower non-experts in image forensics, who are interested in image verification, e.g. fact-checkers and journalists, to actively contribute to image verification tasks.
II. RELATED WORK

The field of media forensics has become increasingly popular in recent years [10]. Several fusion approaches have been proposed in the literature, aiming at combining diverse signals that improve the overall robustness of the forensics localization maps. The various approaches can be categorized based on the level at which fusion is performed and the manipulation traces that are taken into consideration. Frameworks proposed for feature-level fusion often suffer from drawbacks related to selecting and handling a large number of features [11], [12]. Additionally, authors in [3] present a framework that fuses the localization outputs of various forensics algorithms and further refines the result based on statistical features. The drawback of this method however is that it has hard-coded heuristics and assumptions about the input tampering localization algorithms.

Approaches based on measurement-level fusion are best suited for the tampering detection, and not localization, problem as they provide an overall result regarding forgeries being present or not [3], [5].

On the other hand, techniques proposed for pixel-level fusion usually involve utilizing probability output maps and a fusion model to refine the final output and improve the localization of the tampered region [6]. In recent years, deep learning shows great power in many research fields, and methods based on deep Convolutional Neural Networks (CNN) outperform traditional methods and achieve remarkable success in solving computer vision problems. For instance, the work in [13] presents a fusion architecture that outperforms traditional approaches. The difference of this approach is that it fuses features from different patches of the same image to produce the final localization map.

III. METHODOLOGY

The main objective of our work is to develop a fully automatic fusion approach, able to exploit diverse forensics signals from the Image Verification Assistant and generate a robust and easy-to-interpret visualization. The current version of Image Verification Assistant contains 11 forensics algorithms with corresponding outputs.

To simplify the training and evaluation of our fusion models, we select a subset of the forensics algorithms to be considered for fusion. Also, to provide a direct comparison with another fusion framework [4], we adopt their algorithm selection based on an evaluation of three publicly available datasets. These datasets are: (i) The First IFS-TC Image Forensics Challenge set [14], (ii) the synthetic dataset by Fontani et al. [3], and (iii) the real cases of the Wild Web dataset [15]. Based on the evaluation results, a set of five methods were selected as the building blocks of the fusion model:

- ADQ1 [16] and DCT [17] that both base their detection on analysis of the JPEG compression, in the transform domain;
- BLK [18] and CAGI [19] that base their detection on analysis of the JPEG compression in the spatial domain;
- Splicebuster [20], a noise-based detector selected as a complementary method due to its high reported performance and good interpretability of its produced outputs.

In this work, we adopt a deep learning-based fusion approach for the following reasons. First, we aspire to develop a fully automatic approach without the need for heuristic tuning or manual intervention, as for instance in the case of [4]. Second, the complex and diverse nature of the input signal calls for an effective approach to automatically extract the most important features, which deep learning excels at [21]. Finally, the availability of large-scale datasets, which are required by deep learning approaches makes the training of a deep learning-based model feasible.

For the fusion architecture, we initially consider two different deep learning architectures. The first model we adopt is U-Net [22]. U-Net is a convolutional neural network that was initially applied for semantic segmentation in a medical context in order to localize tumors in the lungs or brain, but nowadays, it has got a much broader application field. The main idea is to supplement a usual contracting network by successive layers, where pooling operations are replaced by up-sampling operators. Hence these layers increase the resolution of the output. A successive convolutional layer can then learn to assemble a precise output based on this information. One important feature in U-Net is that there are a large number of feature channels in the up-sampling part, which allow the network to propagate context information to higher resolution layers. Consequently, the expansive path is roughly symmetric to the contracting part and yields a U-shaped architecture. The network only uses the valid part of each convolution without any fully connected layers. The U-Net architecture has a lot of variants. For the fusion task, we use Eff-Unet [23], a variant of U-Net architecture that uses EfficientNet [24] as the encoder part. To adapt the Eff-Unet to our fusion task, we use the EfficientNet-B4 variant as the encoder. We refer to this model as Eff-B4-Unet.

The second model that we employ is a simple architecture of neural networks that was proposed for the problem of image restoration [25]. It performs multiple operations in parallel, which are weighted by an attention mechanism to enable the selection of proper operations depending on the input. The layer can be stacked to form a deep network, which is differentiable and thus can be trained in an end-to-end fashion by gradient descent. This architecture is suitable for our problem because it uses attention to capture important features by examining which operations are the most beneficial, depending on the input signal. Another important aspect of this architecture is that it can learn to attend low-level features, which is important for the fusion task, as semantic or high-level representations are often not relevant or useful for the problem. The network includes operations like, dilated convolutions, separable convolutions, and pooling with various kernel sizes and rates, which are weighted by an attention mechanism. To adapt this architecture to our needs, we replaced dilated convolutions with simple convolutions as the former are better suited for the image restoration.
task and exhibit lower validation performance in preliminary experiments. Additionally, we reduce the number of stacked Operation-wise Attention (OwA) layers from 10 to 4, in order to avoid overfitting during training. Also, in our adaptation, each operation-wise attention layer consists of one operation layer, in contrast with the original implementation that stacks 4 consecutive operation layers. Figure 1 shows the modified operation-wise attention layer. In the operation layer, we use simple convolutions with filter sizes $1 \times 1$, $3 \times 3$, $5 \times 5$, $7 \times 7$, average and max pooling with a $3 \times 3$ receptive field. We refer to this model as OwAF.

IV. EXPERIMENTAL STUDY

In this section, we compare these two deep learning approaches and we use the best performing in further evaluations, in order to compare it with another fusion approach against two publicly available image forensics datasets.

A. Training and evaluation setup

a) Training set: To train the deep learning models that we describe in Section III, we need to use an image forensics dataset for training. For the model training in the fusion task, we generate a set of tampering localization outputs by applying the forensics algorithms for each image in the dataset. Currently, there are not many large-scale forensics datasets available, and this is mainly due to the fact that their generation is very time-consuming. On the other hand, it is easy to generate synthetic forgeries in images. For this work, we use the DEFACTO dataset [26], which contains more than 150,000 images with synthetic forgeries and their corresponding ground truth masks. The dataset contains four manipulation types, including splicing, copy-move, object removal, and face morphing. For our task, we use only images from the first three manipulation types. We randomly compile 15,000 images for training, 1000 for test, and 1000 for validation. For every input image in each set, we produce a set of different tampering localization maps obtained by the selected detection methods. This means that the produced training set for the fusion model consists of $15,000 \times 5$ tampering localization maps and corresponding ground truth masks for every image. We concatenate the forensics maps in the channel axis to generate training samples.

b) Parameter selection: We use the Adam optimizer [27] with an initial learning rate of 0.001, and we minimize the pixel-size binary cross-entropy loss. To achieve this, the final layer of both architectures has a sigmoid activation function. Ground truth masks are also in the $[0,1]$ range, having zeros for the pristine parts of the image and ones for the tampered regions. The training batch size is set to 4. We train the model for 20 epochs, and we save only the weights of the model that has the lowest validation error. The validation error is derived from the evaluation of the images in the DEFACTO validation set. For faster training, we only use 300 images of the validation set. We also reduce the learning rate by a factor of 10 if the validation error does not improve for 5 epochs.

c) Datasets: To evaluate the models, we use three datasets. First, we evaluate the proposed deep learning models against the DEFACTO test dataset that contains 1000 images. Then, we choose the best of the two models and compare them to another previously proposed model [4]. This comparison is performed on two different forensics datasets. The first is the IFS-TC Image Forensics Challenge dataset [14], which contains 450 images with forgeries and is designed to serve as a realistic benchmark. Focusing on splicing tampering localization, we excluded cases that were produced by copy-move operations resulting in a set of 306 forgery cases produced through splicing operations only. Tampered images in this dataset are accompanied by ground-truth maps. The second dataset is the CASIA V2.0 dataset [28] that contains 5,123 realistically tampered color images of varying sizes. This dataset does not come with ground truth masks. In order for us to be able to perform localization tests, we take the ground truth masks that were produced in another work [4], where 2,195 reliable ground truth maps were manually produced through semi-automated procedures involving image differencing, thresholding, and morphological operations.

d) Evaluation metrics: We use the F1 score, both the macro average and the F1 for the tampered class, and the average Intersection over Union (IoU) metric.
B. Results

In the first experiment, we investigate the performance of the two proposed fusion models. Table I shows the evaluation results of the two proposed models in the DEFACTO test dataset as well as results from all individual algorithms.

| Models         | Macro-F1 | F1 (tampered) | IoU |
|----------------|----------|---------------|-----|
| BLK [18]       | 0.463    | 0.090         | 0.053 |
| ADQ1 [16]      | 0.573    | 0.221         | 0.123 |
| CAGI [19]      | 0.479    | 0.142         | 0.072 |
| DCT [17]       | 0.509    | 0.186         | 0.101 |
| Splicebuster [20] | 0.554    | 0.133         | 0.087 |
| Eff-B4-Unet    | 0.908    | 0.798         | 0.600 |
| OwAF           | 0.912    | 0.829         | 0.707 |

We can see that the OwAF network outperforms the Eff-B4-Unet in every evaluation metric. Evaluation results for individual algorithms are very low when compared to the fusion approaches. This can be attributed to the fact that certain algorithms work well on specific manipulation types and images. Also, the 0.5 binarization threshold may impair the evaluation performance of many algorithms, as many algorithms might operate on lower thresholds. Averaging the results from many binarization ranges did not significantly improve the evaluation results, nonetheless. The best performing individual model is ADQ1. Another important observation is that the macro-averaged F1 score is higher compared to the F1 score for the tampered class for all evaluations. This means that the models can predict the pristine regions more accurately than the tampered ones. In terms of intersection over union (IoU) evaluation, we can see that the OwAF model still outperforms Eff-B4-Unet.

Figure 2 shows random examples from the DEFACTO test dataset. The first column includes the input images. The next five columns show the outputs of the individual tampering localization algorithms. The final two columns show the ground truth mask, which reveals the actual location of the forgery and the fusion result of the OwAF model that combines the localization outputs, respectively. It is evident from these examples that the fusion architecture learned to combine the diverse signals in order to localize the tampered region. One interesting observation is that for each input example, there are usually different algorithms that better localize the forgery. It seems that the fusion model learned to detect proper signals that contribute to a correct localization. For example, in the first row, Splicebuster and CAGI spot the tampering, but in row three, ADQ1 and DCT do so. In both cases, the fusion model has identified these signals and provides a correct result.

To further investigate the fusion performance, we compare our best performing approach with another fusion framework proposed by [4]. For evaluation, we use the two datasets described above (CASIA v2 and IFS-TC) in order to examine the generalization capabilities of the fusion model that was trained with the DEFACTO dataset. CASIA v2 is the first evaluation dataset we use. Table II shows the evaluation results. The binarization threshold is set to 0.5.

We can observe slightly better performance in every metric from individual models compared to those in Table I. This
means that this dataset contains images with manipulations that can be localized better by the individual algorithms. ADQ1 and DCT are still the best performing individual approaches. Regarding the fusion methods evaluation, we can see that our approach outperforms the competing fusion framework [4]. One notable observation is that the performance of OwAF is significantly worse than the evaluation results that are reported in Table I. This is a clear indication that our trained models have overfitted to the training set manipulations. The fusion model possibly learned to localize specific forgeries, like shapes and patterns from the outputs of individual algorithms that frequently appear in the DEFACTO dataset. For example, the DEFACTO dataset contains synthetic manipulations on specific objects such as traffic signs, birds, airplanes, humans (Figure 2). Yet, the proposed approach is still better than individual algorithms and also outperforms the fusion framework of [4] in terms of both F1 score and IoU.

Evaluation results on the First IFS-TC Image Forensics Challenge dataset are also reported in Table II. In these results, a significant decrease in the performance of the individual algorithms can be observed. One exception is the Splicebuster performance, which increased compared to previous evaluations. Splicebuster even outperforms both fusion approaches. Iakovidou et al. [4] also achieve marginally better performance than our fusion model in this dataset. One possible explanation is that our fusion model learned to focus more on the individual localization maps that achieved better performance in the training set, namely the ADQ1 and DCT. This can also be verified from the CASIA v2 evaluation results, where ADQ1 and DCT are still the best individual approaches, and our approach outperforms all others. On the contrary, in the First IFS-TC Image Forensics Challenge case, the best performing individual algorithm is Splicebuster and this possibly justifies the poor performance of OwAF.

Figure 3 shows some successful examples of tampering localization outputs produced by the fusion model and the individual methods from the two evaluation datasets. In most examples, ADQ1 and DCT visualization better localize the tampering. There are also cases where Splicebuster and CAGI better localize the forgeries. Additionally, in these specific
examples, we can see that the visual result from the method of Iakovidou et al. is very poor for the CASIA v2 samples (first four). The qualitative results are improved for the IFS-TC samples (last four), which is expected as this approach overall performs better in this dataset.

From our experiments, it is evident that the main challenge of the proposed approach stems from overfitting to the training data. Although OwAF can outperform individual forensics algorithms or other fusion models, we observe a lack of generalization to unseen manipulations. Namely, we get poor predictions for datasets that have different types of manipulations compared to those that appeared in the training dataset. Additionally, the low evaluation performance of individual models is a major indication that the forgery localization problem is very difficult and is even more challenging to design a general fusion solution for images in the wild. These observations are also reported by other researchers [2].

V. CONCLUSIONS

The main objective of our work has been to develop a fully automatic fusion approach, able to exploit diverse signals from various forensics algorithms. The fusion outcome would communicate the tampering localization results to end users in a manner that is easier to interpret and requires no additional specialized knowledge.

The reported experimental results are promising and in many cases outperform the individual forensics techniques and a competing fusion approach. An important limitation of this work is the generalization ability of the fusion model and stems from the general limitations of the underlying supervised learning scheme and the insufficient representativeness of the dataset that was used for training.

In the future, we plan to work on these generalization limitations. To this end, we will try to increase the size of the training dataset and include different manipulations from other synthetic datasets. Additionally, we will experiment with task-specific regularization techniques, like feature map dropout. Finally, another interesting research direction is to experiment with multi-stream fusion architectures that besides the forensics localization maps, will extract features from the input image itself.

ACKNOWLEDGMENTS

This work has been supported by the WeVerify H2020 project, partially funded by the European Commission under contract number 825297.

REFERENCES

[1] P. Korus, “Digital image integrity—a survey of protection and verification techniques,” Digital Signal Processing, 2017.
[2] M. Zampoglou, S. Papadopoulos, and Y. Kompatsiaris, “Large-scale evaluation of splicing localization algorithms for web images,” Multimedia Tools and Applications, 2017.
[3] M. Fontani, T. Bianchi, A. De Rosa, A. Piva, and M. Barni, “A framework for decision fusion in image forensics based on Dempster–Shafer theory of evidence,” IEEE transactions on Information Forensics and Security, 2013.
[4] C. Iakovidou, S. Papadopoulos, and Y. Kompatsiaris, “Knowledge-based fusion for image tampering localization,” in IFIP International Conference on Artificial Intelligence Applications and Innovations, 2020.
[5] M. Kaur and S. Gupta, “A fusion framework based on fuzzy integrals for passive-blind image tamper detection,” Cluster Computing, 2019.
[6] H. Li, W. Luo, X. Qiu, and J. Huang, “Image forgery localization via integrating tampering possibility maps,” IEEE Transactions on Information Forensics and Security, 2017.
[7] “Expert criticizes allegations of Russian MH17 manipulation,” accessed on Jan 21, 2021. [Online]. Available: https://www.spiegel.de/international/world/expert-criticizes-allegations-of-russian-mh17-manipulation-a-1037125.html.
[8] Z. Marinova, J. Spangenberg, D. Teyssou, S. Papadopoulos, N. Sarris, A. Alaphilippe, and K. Bontcheva, “Weverify: Wider and enhanced verification for your project overview and tools,” in 2020 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 2020.
[9] M. Zampoglou, S. Papadopoulos, Y. Kompatsiaris, R. Bouwmeester, and J. Spangenberg, “Web and social media image forensics for news professionals,” in Proceedings of the International AAAI Conference on Web and Social Media, 2016.
[10] L. Verdoliva, “Media forensics and deepfakes: an overview,” IEEE Journal of Selected Topics in Signal Processing, vol. 14, no. 5, pp. 910–932, 2020.
[11] M. Barni and A. Costanzo, “A fuzzy approach to deal with uncertainty in image forensics,” Signal Processing: Image Communication, 2012.
[12] G. Chetty and M. Singh, “Nonintrusive image tamper detection based on fuzzy fusion,” International Journal of Computer Science and Network Security, 2010.
[13] B. Liu and C.-M. Pun, “Deep fusion network for splicing forgery localization,” in Proceedings of the European Conference on Computer Vision (ECCV) Workshops, 2018.
[14] “Report on the ieee-ifc challenge,” accessed on Mar 2016. [Online]. Available: http://ific.recod.ic.unicamp.br.
[15] M. Zampoglou, S. Papadopoulos, and Y. Kompatsiaris, “Detecting image splicing in the wild (web),” in 2015 IEEE International Conference on Multimedia & Expo Workshops (ICMEW), 2015.
[16] Z. Lin, J. He, X. Tang, and C.-K. Tang, “Fast, automatic and fine-grained tampered jpeg image detection via dct coefficient analysis,” Pattern Recognition, 2009.
[17] S. Ye, Q. Sun, and E.-C. Chang, “Detecting digital image forgeries by measuring inconsistencies of blocking artifacts,” in 2007 IEEE International Conference on Multimedia and Expo, 2007.
[18] W. Li, Y. Yuan, and N. Yu, “Passive detection of doctored jpeg image via block artifact grid extraction,” Signal Processing, 2009.
[19] C. Iakovidou, M. Zampoglou, S. Papadopoulos, and Y. Kompatsiaris, “Content-aware detection of jpeg grid inconsistencies for intuitive image forensics,” Journal of Visual Communication and Image Representation, 2018.
[20] D. Cuzzolin, G. Poggi, and L. Verdoliva, “Splicebuster: A new blind image splicing detector,” in 2015 IEEE International Workshop on Information Forensics and Security (WIFS), 2015.
[21] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, “Deep learning for computer vision: A brief review,” Computational intelligence and neuroscience, 2018.
[22] O. Ronneberger, P. Fischer, and T. Brox, “U-net: Convolutional networks for biomedical image segmentation,” in International Conference on Medical image computing and computer-assisted intervention, 2015.
[23] B. Baheti, S. Innani, S. Gajre, and S. Talbar, “Eff-unicorn: A novel architecture for semantic segmentation in unstructured environment,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2020.
[24] M. Tan and Q. Le, “Efficientnet: Rethinking model scaling for convolutional neural networks,” in International Conference on Machine Learning, 2019.
[25] M. Suganuma, X. Liu, and T. Okatani, “Attention-based adaptive selection of operations for image restoration in the presence of unknown combined distortions,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019.
[26] G. Mahfoudi, B. Tajini, F. Retraint, F. Morain-Nicolier, J. L. Dugelay, and P. Marc, “Defacto: Image and face manipulation dataset,” in 2019 27th European Signal Processing Conference (EUSIPCO), 2019.
[27] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” in 3rd International Conference on Learning Representations, 2015.
[28] J. Dong, W. Wang, and T. Tan, “Casia image tampering detection evaluation database,” in 2013 IEEE China Summit and International Conference on Signal and Information Processing, 2013.
[29] A. Voudenimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, “Deep learning for computer vision: A brief review,” Computational intelligence and neuroscience, 2018.