January 21-23, 2021 Herl'any, Slovakia

SAMI2021

IEEE 19th World Symposium on Applied Machine Intelligence and Informatics

Lightweight Deep Learning Model for Detection of Copy-move Image Forgery with Post-processed Attacks

(Paper id: 29)

Authors

Muhammad Naveed Abbas[1], Mohammad Samar Ansari[2] , Mamoona Naveed Asghar[2],Nadia Kanwal[2], Terry O'Neill[1], Brian Lee[2]

[1]*Deptt. of Accounting & Business Computing,* Athlone Institute of Technology, Ireland

[2]Software Research Institute, Athlone Institute of Technology, Ireland

Institiúid Teicneolaíochta Bhaile Átha Luain

Athlone Institute of Technology

ABSTRACT

To counter the rapidly complicating image forgery methods due to easily accessible technologically advanced tools, passive image forensic methods have also undergone massive evolution. Presently, deep learning based techniques are regarded as state-of-the-art for image processing/image forgery detection and classification due to their enhanced accuracy and automatic feature extraction capabilities. But the existing deep learning based techniques are time and resource-intensive as well. To cater for these solutions with complexities as stated, this research focuses on experimentation using two state-of-the-art deep learning models; SmallerVGGNet (inspired from VGGNet) and MobileNet*V2*. These two models are time and resource friendly deep learning frameworks for digital image forgery detection on embedded devices. After rigorous analysis, the study considers a suitably modified version of MobileNet*V2* to be more effective on copy-move forgery detection which also caters for inconsistencies executed post-forgery including visual-appearance related such as brightness change, blurring and noise adding and geometric transformations such as cropping and rotation. The experimental results demonstrate that the proposed MobileNet*V2* based model shows 84% True Positive Rate (TPR) and 14.35% False Positive Rate (FPR) for the detection of digital image forgery post-processed with the said multiple attacks.

Research Motivation & Contribution

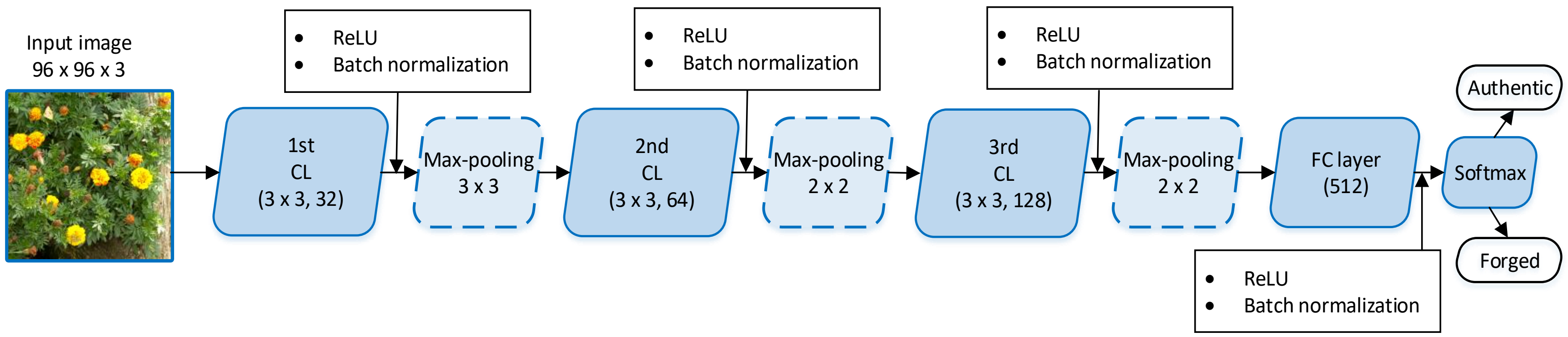
- Literature shows that the existing techniques on digital image forgery authentication using deep learning are time and resource-intensive. Therefore, this research proposes a time, resource friendly and embedded devices-compatible deep learning based technique for digital image forgery detection and analytics.
- The proposed technique is copy-move forgery-centric and caters for the attacks executed after the forgery including visual-appearance related such as brightness change, blurring and noise adding and geometric transformations such as cropping and rotation.
- The contributions of this paper can be outlined as:
  - ✓ Generation of a composite dataset composed from the publicly available authentic forged image datasets consisting of copy-move forged images post-processed with multiple attacks.
  - ✓ Investigation to propose a best-performing lightweight deep learning model from a custom-built conventional convolutional neural network (CNN) framework or modified inverted residual block-based CNN framework.
  - ✓ Identification of a deep learning based solution which is time and resource efficient, robust and competently accurate.

Methodology

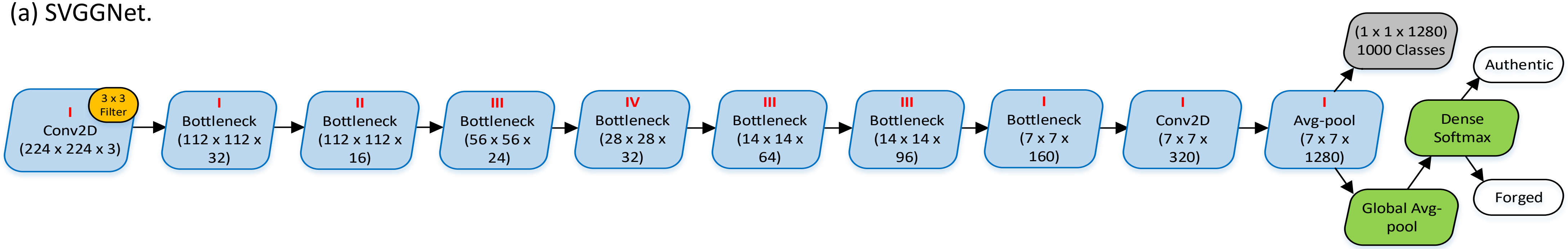
In order to detect and classify the copy-move forgery along with post-processed attacks in digital images using deep learning models, the following steps are taken:

- Implementation of SVGGNet (architecture visualized in Fig. 1(a)), a compressed version of VGGNet framework, was built to take input image of size 96×96×3.
- Implementation of a highly efficient and lightweight network, MobileNetV2 model (architecture visualized in Fig. 1(b)), .
- Dataset Preparation, Data Preprocessing and Augmentation
  - ✓ dataset preparation was composed from three databases: (1) CoMoFoD [16]; (2) MICC-F2000 [17]; and (3) CASIA ITDE 2.0 [18].
- Design Implementation Controlling Preset Hyper-parameters, Methods and Functions

METHODOLOGY(CONT.)



(a) SVGGNet.



(b) MobilNet*V2*. The layer(s) highlighted in grey with dotted outline depict(s) the removed one(s) from the original pre-trained model and the newly added and retrained head of the model is highlighted in green. Roman numerals shown in red font represent the number of repetitions for that particular block.

Fig. 1. Deep learning models architectures implemented in this research.

TESTBED SETUP

- Both the proposed networks were implemented in Keras running on top of the deep learning framework TensorFlow™
- After data modelling, the trained models were evaluated using the validation data partition to analyze their performance on outputs with known values for predictive analytics.
- The resulting models were then deployed to test their predictive probability, as presented and discussed in the Results section of this paper.
- The schematic flowchart of design implementation with both CNN architectures, SVGGNet and MobileNet*V2*, showing various predefined controlling hyper-parameters and methods/functions is visualized in Fig. 2.

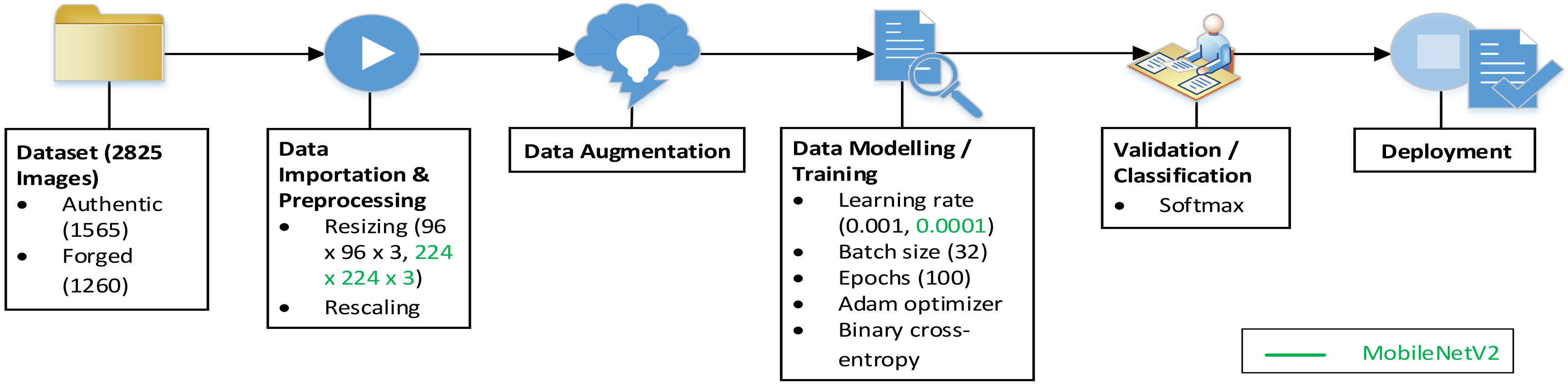


Fig. 2. Schematic flowchart of design implementation for both models.

Results And Discussion

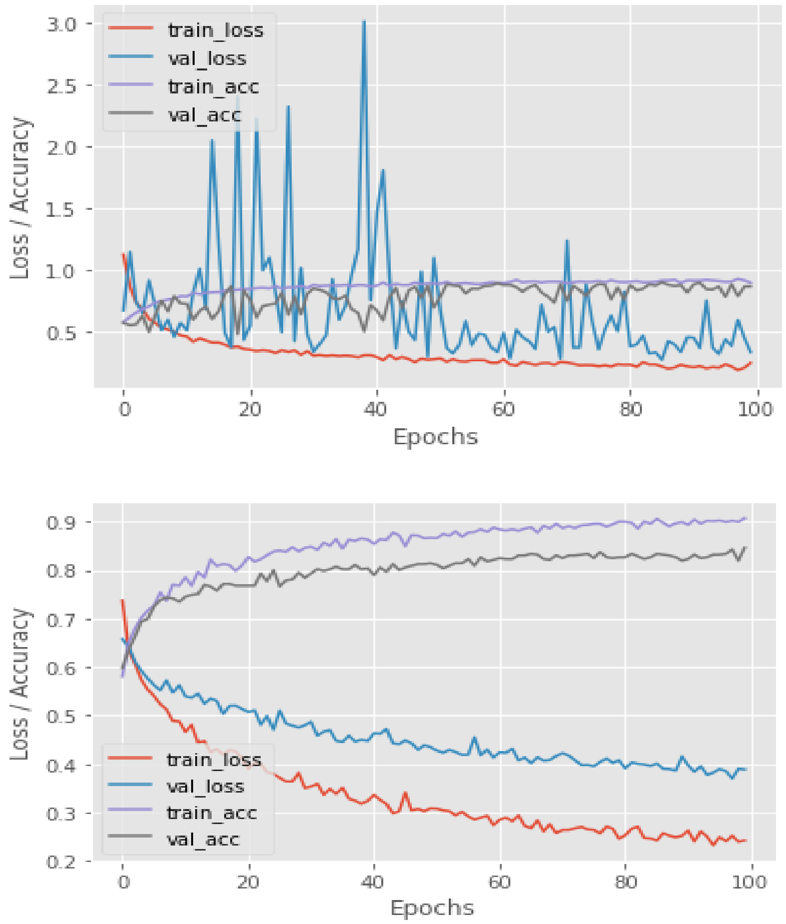


Fig. 3. Training vis-à-vis validation loss and accuracy plots for both models SVGGNet (top) and MobilNet*V2* (bottom).

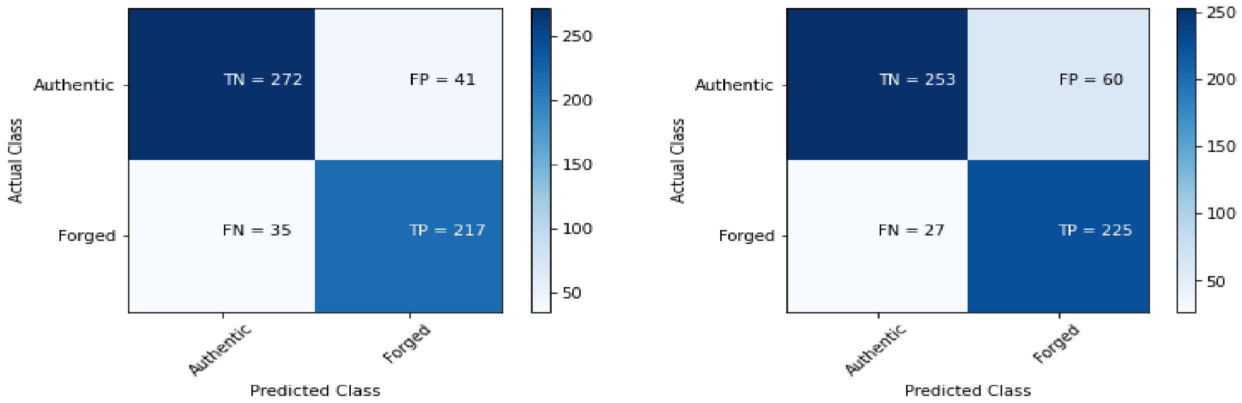


Fig. 4. Confusion matrices for both models SVGGNet (left) and MobilNet*V2* (right).

TABLE I. Comparative Summary – Evaluation Metrics.

Evaluation Metric	SVGGNet	MobileNetV2
Accuracy	87%	85%
TPR	87%	85%
FPR	13%	19%

COMPARATIVE ANALYSIS OF MODELS

TABLE II. Predictions Comparative Summary of both models.

Dataset and Image Details	Input Images	SVGGNet		MobileNetV2	
		TPR%	FPR%	TPR%	FPR%
CoMoFoD					
***Original**	15	93	28.6	91	26.7
Forged + Brightness Change, Blurred, Noisy	15				
MICC-F2000					
***Original**	15	40	4	77	2
Forged + Geometric (Scaling & Rotation)	15				
Overall					
Original	30	67	16.3	84	14.35
Forged	30				
***Original images from CASIA ITDE V2.0 dataset are also included.**					

VISUAL RESULTS

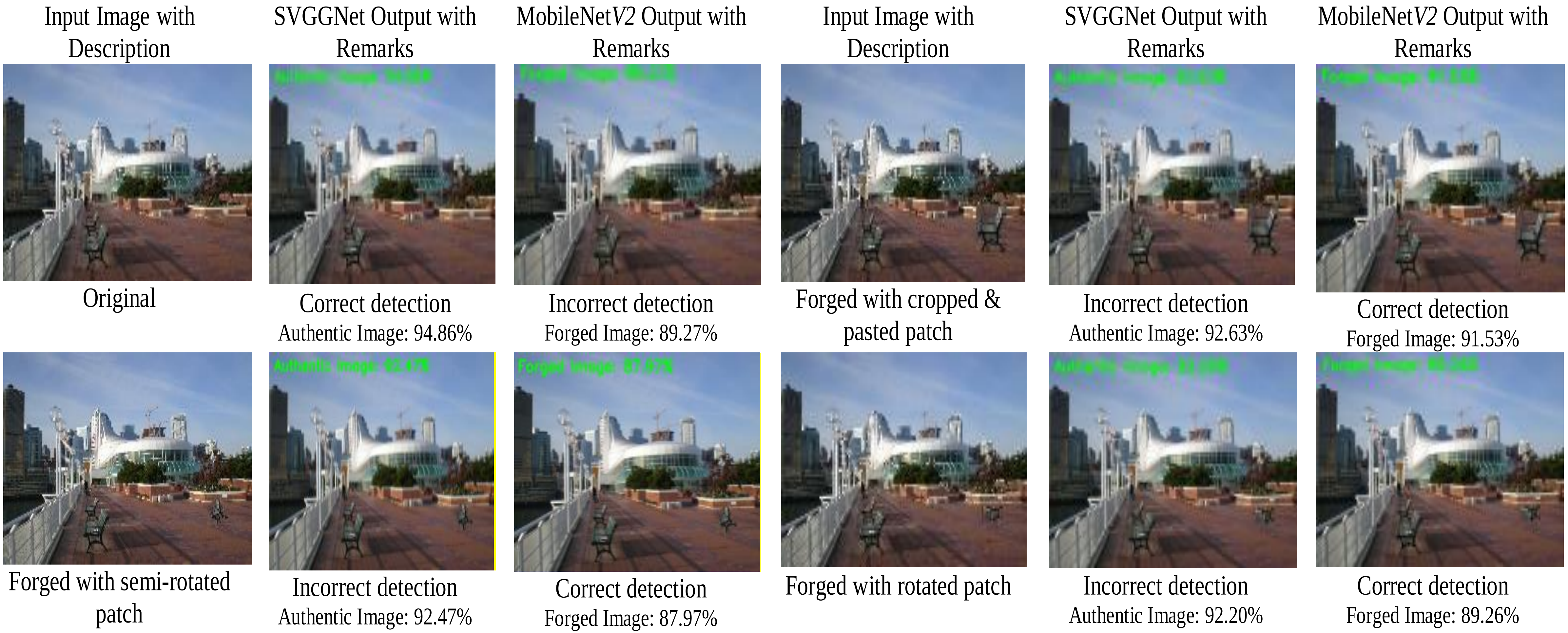


Fig. 5. Prediction results sample images from MICC-F2000 database - SVGGNet vis-à-vis MobileNet*V2* .

SUMMARY OF THE FINDINGS

- Regarding inference time for both networks, it remained at 3.09 seconds on the average for SVGGNet model. Whereas, the inference time for the MobileNet*V2* model remained at 4.20 seconds on the average.
- According to the results, it can say that MobileNet*V2* model is a standout performer during the deployment phase by showing values of 84% and 14.35% for TPR and FPR metrics respectively as compared to those of 67% and 16.30% for SVGGNet model respectively.
- The lightweight and computationally efficient characteristics of MobileNet*V2* also make it a preferred choice to address the problem underpinning this research.

Conclusions & Future Work

In order to detect and classify copy-move forgery in digital images efficiently using a lightweight yet robust deep learning model, the model proposed through this research can be regarded as a worth-mentioning contribution of this work. Moreover, the copy-move forged images post-processed with multiple attacks related to visual-appearance and geometrical operations detected with high confidence using the MobileNet*V2*, add to the novelty of this research. From the experimental results, it is evident that appropriately modified MobileNet*V2* emerged as a robust and resource-friendly CNN framework by occupying a disk size of merely 11 MB, validating the finding by [15], where the researchers highlighted that it has disk size of only 13 MB. Hence it can be said that given the resource-constrained environment, the proposed modified MobileNet*V2* model is a computationally lightweight, reliable and accurate solution for the desired task. In future, this work is extendable to multiple-class forgery detection and analytics (splicing and retouching) along with localisation in digital images.

REFERENCES

[1] S. Teerakanok and T. Uehara, "Copy-move forgery detection using GLCM-based rotation-invariant feature: a preliminary research," in *2018 42nd IEEE Int. Conf. on Comput. Software & Appl. (COMPSAC)*, Tokyo, Japan, 2018, pp. 365–369, doi: 10.1109/COMPSAC.2018.10259.

[2] H. Phan-Xuan, T. Le-Tien, T. Nguyen-Chinh, T. Do-Tieu, Q. Nguyen-Van, and T. Nguyen-Thanh, "Preserving spatial information to enhance performance of image forgery classification," in *2019 Int. Conf. on Adv. Technol. for Commun. (ATC)*, Hanoi, Vietnam, 2019, pp. 50–55, doi: 10.1109/ATC.2019.8924504.

[3] N. B. A. Warif et al., "Copy-move forgery detection: survey, challenges and future directions," *J. Netw. Comput. Appl.*, vol. 75, pp. 259–278, 2016, doi: 10.1016/j.jnca.2016.09.008.

[4] M. A. Elaskily, H. K. Aslan, O. A. Elshakankiry, O. S. Faragallah, F. E. A. El-Samie, and M. M. Dessouky, "Comparative study of copy-move forgery detection techniques," in *2017 Int. Conf. on Adv. Control Circuits Syst. (ACCS) Syst. & 2017 Int. Conf. on New Paradigms in Electron. & Inf. Technol. (PEIT)*, Alexandria, Egypt, 2017, pp. 193–203, doi: 10.1109/ACCS-PEIT.2017.8303041.

[5] B. Ustubioglu, G. Ulutas, M. Ulutas, and V. V. Nabiyev, "A new copy move forgery detection technique with automatic threshold determination," *AEU - Int. J. Electron. Commun.*, vol. 70, no. 8, pp. 1076–1087, Aug. 2016, doi: 10.1016/j.aeue.2016.05.005.

[6] A. B. Z. Abidin, H. B. A. Majid, A. B. A. Samah, and H. B. Hashim, "Copy-move image forgery detection using deep learning methods: a review," in *2019 6th Int. Conf. on Res. and Innov. in Inf. Syst. (ICRIIS)*, Johor Bahru, Malaysia, 2019, pp. 1–6, doi: 10.1109/ICRIIS48246.2019.9073569.

[7] J. Chen, X. Kang, Y. Liu, and Z. J. Wang, "Median filtering forensics based on convolutional neural networks," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 1849–1853, Nov. 2015, doi: 10.1109/LSP.2015.2438008.

[8] B. Bayar and M. C. Stamm, "Constrained convolutional neural networks: a new approach towards general purpose image manipulation detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 11, pp. 2691–2706, Nov. 2018, doi: 10.1109/TIFS.2018.2825953.

[9] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *2016 IEEE Int. Workshop on Inf. Forensics and Secur. (WIFS)*, Abu Dhabi, United Arab Emirates, 2016, pp. 1–6, doi: 10.1109/WIFS.2016.7823911.

[10] B. Yang, X. Sun, E. Cao, W. Hu, and X. Chen, "Convolutional neural network for smooth filtering detection," *IET Image Process.*, vol. 12, no. 8, pp. 1432–1438, Aug. 2018, doi: 10.1049/iet-ipr.2017.0683.

[11] Z. Shi, X. Shen, H. Kang, and Y. Lv, "Image manipulation detection and localization based on the dual-domain convolutional neural networks," *IEEE Access*, vol. 6, pp. 76437–76453, Nov. 2018, doi: 10.1109/ACCESS.2018.2883588.

[12] M. A. Elaskily et al., "A novel deep learning framework for copy-move forgery detection in images," *Multimed. Tools Appl.*, vol. 79, pp. 19167–19192, Mar. 2020, doi: 10.1007/s11042-020-08751-7.

[13] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," in *3rd Int. Conf. on Learn. Representations (ICLR) 2015*, San Diego, CA, USA, 2015, pp. 1–14, [Online]. Available: https://arxiv.org/abs/1409.1556

[14] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L. C. Chen, "MobileNet*V2*: inverted residuals and linear bottlenecks," in *2018 IEEE/CVF Conf. on Comput. Vision and Pattern Recognit.*, Salt Lake City, UT, USA, 2018, pp. 4510–4520, doi: 10.1109/CVPR.2018.00474.

[15] A. Jadon, A. Varshney, and M. S. Ansari, "Low-complexity high-performance deep learning model for real-time low-cost embedded fire detection systems," in *Third Int. Conf. on Comput. and Network Commun. (CoCoNet'19)*, Trivandrum, Kerala, India, 2020, vol. 171, no. 2019, pp. 418–426, doi: 10.1016/j.procs.2020.04.044.

[16] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD - new database for copy-move forgery detection," in *Proc. ELMAR-2013*, Zadar, Croatia, 2013, pp. 49–54.

[17] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 1099–1110, Sept. 2011, doi: 10.1109/TIFS.2011.2129512.

[18] J. Dong, W. Wang, and T. Tan, "CASIA image tampering detection evaluation database," in *2013 IEEE China Summit and Int. Conf. on Signal and Inf. Process.*, Beijing, China, 2013, pp. 422–426, doi: 10.1109/ChinaSIP.2013.6625374.

ACKNOWLEDGEMENT

I acknowledge Athlone Institute of Technology, Ireland to provide me the best support during this research work. This paper is a part of MSc Degree thesis submitted to the Athlone Institute of Technology, Ireland.

AIT

Institiúid Teicneolaíochta
Bhaile Átha Luain
Athlone Institute
of Technology

Thank you

For queries and contact

Please email at

Mamoona N. Asghar: masghar@ait.ie

Marie Sklodowska-curie Career-Fit Postdoc Research Fellow

Software Research Institute,

Athlone Institute of Technology,

Athlone, Westmeath, Ireland