

# COVID-19 digital x-rays forgery classification model using deep learning

Eman I. Abd El-Latif<sup>1</sup>, Nour Eldeen Khalifa<sup>2</sup>

<sup>1</sup>Department of Mathematics and Computer Science, Faculty of Science, Benha University, Benha, Egypt

<sup>2</sup>Information Technology Department, Faculty of Computers and Artificial Intelligence, Cairo University, Giza, Egypt

## Article Info

### Article history:

Received Aug 10, 2022

Revised Jan 12, 2023

Accepted Mar 10, 2023

### Keywords:

COVID-19

Deep learning

Forgery detection

Image forgery

Medical image forgery

## ABSTRACT

Nowadays, the internet has become a typical medium for sharing digital images through web applications or social media and there was a rise in concerns about digital image privacy. Image editing software's have prepared it incredibly simple to make changes to an image's content without leaving any visible evidence for images in general and medical images in particular. In this paper, the COVID-19 digital x-rays forgery classification model utilizing deep learning will be introduced. The proposed system will be able to identify and classify image forgery (copy-move and splicing) manipulation. Alexnet, Resnet50, and Googlenet are used in this model for feature extraction and classification, respectively. Images have been tampered with in three classes (COVID-19, viral pneumonia, and normal). For the classification of (Forgery or no forgery), the model achieves 0.9472 in testing accuracy. For the classification of (Copy-move forgery, splicing forgery, and no forgery), the model achieves 0.8066 in testing accuracy. Moreover, the model achieves 0.796 and 0.8382 for 6 classes and 9 classes problems respectively. Performance indicators like Recall, Precision, and F1 Score supported the achieved results and proved that the proposed system is efficient for detecting the manipulation in images.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Eman I. Abd El-Latif

Department of Mathematics and Computer Science, Faculty of Science, Benha University

Benha, Egypt

Email: eman.mohamed@fsc.bu.edu.eg

## 1. INTRODUCTION

There was widespread fear that the Severe Acute Respiratory Syndrome (SARS) virus had publishing around the world by the end of 2003, owing to its alarmingly high infection rates in Asia and outbreaks in the Middle East, as well as in nations such as Russia that had never seen it previously [1], [2]. This prompted individuals to raise awareness of viruses, which have developed into important hazards in the twenty-first century. The World Health Organization (WHO) designated 2019-nCov (COVID-19) as the coronavirus of the year [3]. Several of the researches devoted to various problems connected to COVID-19 and solved by area of computer science for example expecting COVID-19 symptoms with several kinds of pneumonia utilizing X-rays scans [4], examining the function of new technologies in fighting the COVID-19 pandemic [5], discovering the effects of coronavirus on power industry [6] and more. The majority of papers focus on categorization and classification COVID-19 CT and X-ray images [7]–[10]. The purpose of this research is to detect and classify different types of forgery in the COVID-19 dataset while the medical images were being transmitted from one location to another.

Data transmission through the Internet has become important for numerous fields to share data such as medicine, education, and digital forensics. Medical images can be transmitted and delivered through the

Internet to allow the diagnosis among medical staff and access to the history of the patient from any place. There is various software used for changing the content of an image to create a forged one. This type of change is called image forgery. Forged images display that the alteration in the image cannot be noticed by a visual check. Therefore, checking the authentication of medical image content has become vital because any alteration in the medical images can cause a wrong diagnosis.

There are two approaches employed in image forgery detection: active and passive approaches [11], [12]. The active technique is categorized into two approaches: digital signature and watermarking. In these techniques, a watermark and the signature are embedded into images during the pre-processing stage. The most public types of passive approaches are image splicing and copy-move (CM). In CM technique, a fragment of the image is copied and embedded into another area in the same image [13], [14]. The splicing technique used fragments of different images and pastes them into another image [15], [16]. The existing algorithms achieve acceptable performance in detecting passive image forgery. However, they cannot achieve high detection accuracy with a small forgery region.

The proposed model's primary goal is to notice the splicing and copy-move manipulation in COVID-19, viral pneumonia, and normal images. Deep transfer learning (DTL) presents an outstanding performance in different computer vision problems included image classification [17], and semantic segmentation [18]. Deep learning is a type of multi-layer neural network, in which every layer makes the output from the preceding convolution layer available to the next layer as an input. It can extract complex features from medical images automatically. Deep transfer learning (DTL) can be used on images used in medicine to detect a CM and splicing forgery that the naked eye cannot see. Alexnet [19], Googlenet [20], and Resnet [21] use learned features from training images and then classify the image. The rest of the paper is ordered. Section 2 presents the related work of forgery image detection. The proposed algorithm introduces in section 3. Section 4 contains the experimental results. The conclusions show in the final section.

## 2. RELATED WORKS

Various algorithms are proposed in this section to deal with image forgery. First, we will discuss the numerous splicing techniques and then copy-move techniques. In [22], a method for noticing splicing forgery depending on Haar wavelet transform (HWT) and uniform local binary pattern (ULBP) is presented. First, the RGB image is transformed into the YCbCr model and then HWT is applied to produce the four sub-bands. For every band, ULBP is computed. The final vector is concatenated from all sub-bands. For classification, support vector machine (SVM) is used.

An algorithm in [23] is focused on convolutional neural network (CNN) and HWT is suggested to identify the spliced images. HWT is applied after CNN is used to extract features. Finally, SVM is used to classify images. An algorithm for detecting the alternating in the image is suggested in [24]. It is focused on using LBP and discrete cosine transform (DCT). For each block in the chrominance component, LBP and DCT are applied. For detection, SVM is used.

Ulutas *et al.* [25] presented a passive image algorithm to recognize the forged areas on medical images. LBP rotation invariant and scale-invariant feature transform (SIFT) are applied to extract the key points from the medical images. By matching the key points, forged regions are detected. In [26], CNN and error level analysis (ELA) are used to discover forgery in COVID-19 medical images by detecting the noise pattern. The algorithm achieves an accuracy of 92% for detecting image is forged or not.

The algorithm in [27] is used Markov features for extracting features from two domains: DWT and LBP. Then, features are combined from both domains and fed to SVM for classification. Six benchmark datasets are used to evaluate the algorithm. In [28], an algorithm is based on feature matching and CNN to detect CM forgery. In CNN, many convolution and pooling layers are utilized for feature extraction and then apply characterization among original and tampered images. To identify a CM forgery in [29], DWT and DCT are used for feature extraction. Apply DWT to the image first, and then divide it into blocks. DCT is used for all block, and the correlation coefficients are compared.

## 3. THE PROPOSED MODEL ARCHITECTURE

In this paper, a DLT approach is employed to identify the features of tampered regions. Splice and copy-move are image forgery techniques that are difficult to tell apart from genuine ones. Many algorithms are developed to detect image forgery. The existing algorithms suffer from low accuracy. Deep learning offers a solution for digital image authentication because it extracts complex features from an image. The model relies on three DTL models Alexnet, Googlenet, and Resnet50 to make features extraction and classification processes at the same time as illustrated in Figure 1. These models need the least training time than other pre-trained DLT models. Algorithm 1 shows the steps of the proposed model. The architecture of Alexnet is

consisting of eight layers, the first five layers are convolutional, and the remaining layers are fully connected. After the first two convolutional layers, there is a max-pooling layer in size  $3 \times 3$ . The remainder of the convolution layers is connected to fully connected layers. After every convolution layer, an activation function is utilized called rectified linear unit (ReLU) nonlinearity. Different filters are used in each convolution layer. For example, 96 kernels of size  $11 \times 11 \times 3$  are used in the first layer.

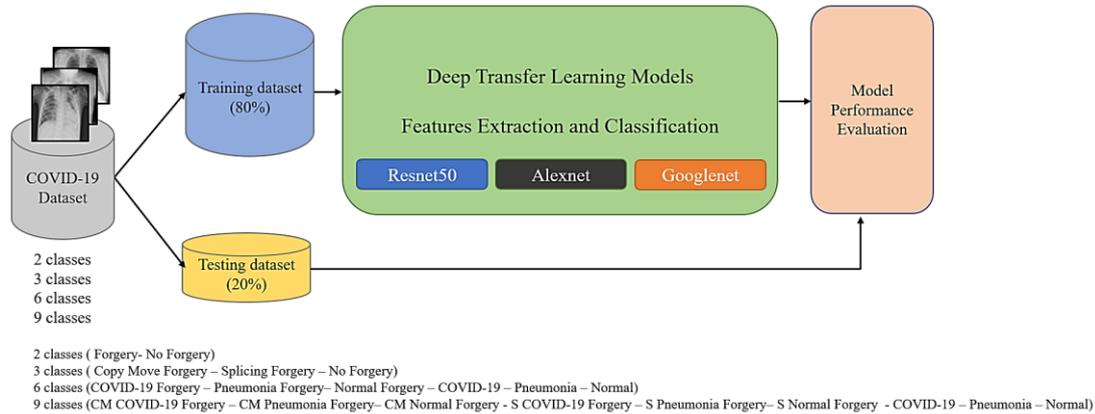


Figure 1. Proposed model architecture

ResNet stands for residual network, and it has many versions, Resnet50 is one of these versions. Resnet50 has used 50 neural network layers with 48 convolution layers and two pooling layers. It consists of five stages every stage with a convolution layer and Individuality block. Each block contains three convolution layers, and every Individuality block has three convolution layers.

There are three versions of Inception Networks, which are called inception versions 1, 2, and 3. The GoogleNet or Inception V1 consists of 22 layers deep, 27 pooling layers, and 9 inception Layers and it is proposed in 2014. The inception layer is a collection of all  $1 \times 1$  convolutional layers,  $3 \times 3$  convolutional layer, and  $5 \times 5$  convolutional layer to reduce the size of parameters in the network. The output of inception is merged and sent to the next layer. At the end of the network, global average pooling is used to reduce the number of trainable parameters.

#### Algorithm 1: The Suggested Model Algorithm

Input: COVID-19 Database and the Tampered Dataset

Output: Classification of the copy-move and splicing forgery of three classes {COVID-19, Viral Pneumonia, Normal}

1. Copy Move (CM) forgery is created by copying and pasting a portion of an image from each class.
2. A portion of each class is copied and pasted into the various images to produce splicing forgery.
3. Download DTL models: Alexnet, Resnet50, and Googlenet
4. Train the proposed model with two, three, six, and nine classes
5. For every image in the dataset
6. Scale the input image to its default DTL aspects.
7. Provide the images to the DTL model for extraction and classification of features.
8. End

#### 4. DATASET CHARACTERISTICS

The COVID-19 Radiography database utilized for training and testing is taken from the open-source platform [30]. The dataset included three classes: 3,616 COVID-19, 10,129 normal and 1,345 viral pneumonia images. The following operations are applied to the COVID-19, normal, and viral pneumonia images to create the tampered images.

In the first operation, a region from each class of the original image is copied and pasted into the same image to make a copy-move forgery. An area from the medical images is copied and pasted into other regions in the different images to generate splicing forgery images. The dataset is available online on Mendeley data [31]. the dataset consists of {COVID-19 2,000 images, CM COVID-19 2,000 images, S COVID-19 2,000 images, Viral Pneumonia 1,340 images, CM Viral Pneumonia 1,340 images, S Viral Pneumonia 850 images, Normal 2,000 images, CM Normal 2,000 images, S Normal 2,000 images}. Figure 2 shows the original images

as shown in Figure 2(a), the result of copy-move as shown in Figure 2(b), and splicing forgery as shown in Figure 2(c) of the COVID-19 image, viral Pneumonia, and normal respectively.

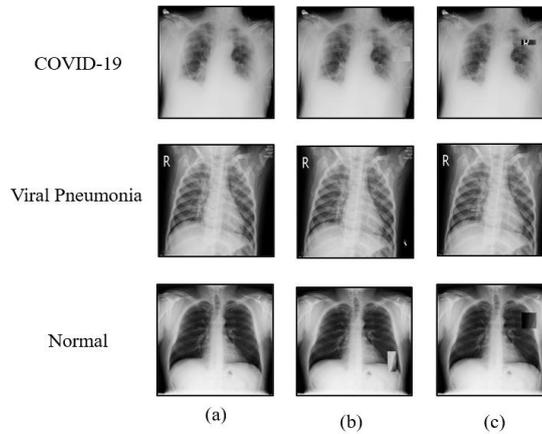


Figure 2. Sample images from the Radiography database, (a) original images, (b) Copy-move, and (c) Splicing forgery techniques

## 5. EXPERIMENTAL RESULTS

This section presents the results of the conducted experiments and the metrics used to evaluate the performance of the proposed model. For each experiment, a computer with 32 GB of RAM and an Intel Xeon processor was utilized. The system contains an NVIDIA TITAN XP Graphics Card. The development of experiments was GPU-specific to the software package MATLAB R2021b. The following hyperparameters were applied to all experimental outcomes during the training and testing phases:

- Model DTL: Alexnet-Googlenet-Resnet50
- Training: 80%, Testing: 20%.
- Optimizer: Adamboost
- Momentum: 0.9
- Learning Rate: 0.001
- Epochs: 40
- Batch size: 32
- Early stopping: 5 epochs

### 5.1. Evaluation metrics

The experimental results of the algorithm are measured using different metrics such as accuracy, precision, F-Measure, and recall. When dealing with data that is not balanced, precision and recall are better suited for identifying a model's errors. The predictive performance of a model is summarized by the F-score, which is the harmonic mean of precision and recall. The definitions are presented from (1) to (4),

$$\text{Testing Accuracy} = \frac{\text{TPos} + \text{TNeg}}{(\text{TPos} + \text{FPoS}) + (\text{TNeg} + \text{FNeg})} \quad (1)$$

$$\text{Precision} = \frac{\text{TPos}}{(\text{TPos} + \text{FPoS})} \quad (2)$$

$$\text{Recall} = \frac{\text{TruePos}}{(\text{TPos} + \text{FNeg})} \quad (3)$$

$$\text{F1 Score} = 2 * \frac{\text{Precision} * \text{Recall}}{(\text{Precision} + \text{Recall})} \quad (4)$$

where TPos is the total number of true positive samples, TNeg is the total number of true negative samples, FalsePos is the total number of false positive samples, and FalseNeg is the total number of false negative samples from a confusion matrix.

## 5.2. Results and discussion

Four classification experiments were conducted to evaluate the performance of the proposed model. The first classification experiment includes two classes (Forgery or no forgery). Table 1 shows the classification results obtained from Alexnet, Google net, and Resnet50. As shown in Table 1, Resnet50 achieves the highest accuracy possible in the recall, precision, F-score, and testing accuracy if it is compared to the other DTL models.

Table 1. Testing accuracy and performance metrics for the first classification experiment (Forgery or no forgery) using different DTL models

	Recall	Precision	F Score	Testing Accuracy
Alexnet	0.8955	0.9232	0.9091	0.9109
Googlenet	0.9222	0.9463	0.9341	0.9363
Resnet50	0.9347	0.9544	0.9445	<b>0.9472</b>

The second classification experiment was dedicated to three classes, and they are (Copy-move forgery, splicing forgery, or no forgery). The testing accuracies are 80.66% in Resnet50, 77.73% in Googlenet, and 66.96 % in Alexnet as shown in Table 2. The results proved the effectiveness of Resnet50 in detecting forged images same as in the first classification experiment.

Table 2. Testing accuracy and performance metrics for the second classification experiment for 3 classes (CM forgery, S forgery or no forgery) using different DTL models

	Recall	Precision	F Score	Testing Accuracy
Alexnet	0.6888	0.6616	0.6749	0.6696
Googlenet	0.7882	0.7732	0.7807	0.7773
Resnet50	0.8123	0.8045	0.8084	<b>0.8066</b>

To test the ability of the proposed model, different forgeries techniques for the different main classes are proposed. The Third classification experiment was conducted on six classes, and they are {CM forgery in COVID-19, splicing in COVID-19, CM forgery in Viral Pneumonia, splicing in Viral Pneumonia, CM forgery in Normal, splicing in Normal} as presented in Table 3. The classification testing accuracy was 79.6% using Resnet50 which is the highest testing accuracy possible.

Table 3. Testing accuracy and performance metrics for the third classification experiment for 6 classes using different DTL models

	Recall	Precision	F Score	Testing Accuracy
Alexnet	0.7179	0.712	0.715	0.7072
Googlenet	0.7668	0.7598	0.7633	0.7607
Resnet50	0.7913	0.7864	0.7888	<b>0.7960</b>

The Fourth classification experiment was dedicated to classifying different nine classes, and they are CM forgery in COVID-19, Splicing in COVID-19, COVID-19, CM forgery in Viral Pneumonia, splicing in Viral Pneumonia, Viral Pneumonia, CM forgery in Normal, Splicing in Normal, Normal). In Table 4, the testing accuracies were 83.82% in Resnet50, 77.16% in Googlenet, and 68.15 % in Alexnet. The results proved the effectiveness of Resnet50 in detecting forged images same as in the first, second, and third classification experiments.

Table 4. Testing accuracy and performance metrics for the fourth classification experiment for 9 classes using different DTL models

	Recall	Precision	F Score	Testing Accuracy
Alexnet	0.6844	0.7003	0.6923	0.6815
Googlenet	0.7715	0.798	0.7846	0.7716
Resnet50	0.8304	0.8382	0.8343	<b>0.8382</b>

## 6. CONCLUSION

Image splicing and copy-move forgery are well-known techniques in the forgery domain. The spliced image was carried out by copying and pasting some portions from one image into other images. In this paper, a proposed model for identifying two techniques in image forgery is proposed. To achieve good results, the proposed algorithm used three DLTs that extract features from images. The selected dataset consisted of three classes (COVID-19, Viral pneumonia, and Normal) class and we made two operations in images to generate CM and splicing forgery. We used the difference between the normal, viral, and COVID-19 images to train the model. The proposed model can efficiently identify image splicing and copy-move forgery of images. The proposed algorithm achieved a relatively high detection accuracy of 94.72% of Resnet50 for the classification of two classes. The model accomplished 80.66% in testing accuracy for three classes (Copy-move forgery, splicing forgery, and no forgery). Moreover, the model achieves 79.60% and 83.82% for the 6 and 9 classes classification respectively. Performance indicators such as recall, precision, and F1 Score supported the obtained results and proved that the proposed model was efficient for detecting manipulation in digital medical images.

### Compliance with Ethical Standards:

**Ethical statement:** This material is the author's original work, which has not been previously published elsewhere. The paper is not currently being considered for publication elsewhere.

**Author contribution:** All authors contributed to the study's conception and design. Material preparation was performed by Eman Ibrahim. The first draft of the manuscript was written by Eman Ibrahim, and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

**Data availability statement:** The data that support the findings of this study are available from author Eman Ibrahim, upon reasonable request.

**Funding:** There was no external funding for this research.

**Conflict of interest:** The corresponding author certifies that there is no conflict of interest on behalf of all authors.

## REFERENCES

- [1] L. Chang, Y. Yan, and L. Wang, "Coronavirus disease 2019: Coronaviruses and blood safety," *Transfusion Medicine Reviews*, vol. 34, no. 2, pp. 75–80, 2020, doi: 10.1016/j.tmr.2020.02.003.
- [2] V. Chamola, V. Hassija, V. Gupta, and M. Guizani, "A comprehensive review of the COVID-19 pandemic and the role of IoT, drones, AI, blockchain, and 5G in managing its impact," *IEEE Access*, vol. 8, pp. 90225–90265, 2020, doi: 10.1109/ACCESS.2020.2992341.
- [3] T. Singhal, "A review of coronavirus disease-2019 (COVID-19)," *Indian Journal of Pediatrics*, vol. 87, no. 4, pp. 281–286, 2020, doi: 10.1007/s12098-020-03263-6.
- [4] K. H. Almotairi *et al.*, "Impact of artificial intelligence on COVID-19 pandemic: A survey of image processing, tracking of disease, prediction of outcomes, and computational medicine," *Big Data and Cognitive Computing*, vol. 7, no. 1, p. 11, 2023, doi: 10.3390/bdcc7010011.
- [5] A. A. Abd El-Aziz, N. E. M. Khalifa, A. Darwsih, and A. E. Hassanien, "The role of emerging technologies for combating COVID-19 pandemic," *Studies in Systems, Decision and Control*, vol. 322, pp. 21–41, 2021, doi: 10.1007/978-3-030-63307-3\_2.
- [6] A. A. Abd El-Aziz, N. E. M. Khalifa, and A. E. Hassanien, "Exploring the impacts of covid-19 on oil and electricity industry," *Studies in Systems, Decision and Control*, vol. 369, pp. 149–161, 2021, doi: 10.1007/978-3-030-72933-2\_10.
- [7] J. Civit-Masot, F. Luna-Perejón, M. D. Morales, and A. Civit, "Deep learning system for COVID-19 diagnosis aid using X-ray pulmonary images," *Applied Sciences (Switzerland)*, vol. 10, no. 13, 2020, doi: 10.3390/app10134640.
- [8] A. Waheed, M. Goyal, D. Gupta, A. Khanna, F. Al-Turjman, and P. R. Pinheiro, "CovidGAN: Data augmentation using auxiliary classifier GAN for improved COVID-19 detection," *IEEE Access*, vol. 8, pp. 91916–91923, 2020, doi: 10.1109/ACCESS.2020.2994762.
- [9] N. Narayan Das, N. Kumar, M. Kaur, V. Kumar, and D. Singh, "Automated deep transfer learning-based approach for detection of COVID-19 infection in chest x-rays," *Irbm*, vol. 43, no. 2, pp. 114–119, 2022, doi: 10.1016/j.irbm.2020.07.001.
- [10] A. A. Ardakani, A. R. Kanafi, U. R. Acharya, N. Khadem, and A. Mohammadi, "Application of deep learning technique to manage COVID-19 in routine clinical practice using CT images: Results of 10 convolutional neural networks," *Computers in Biology and Medicine*, vol. 121, 2020, doi: 10.1016/j.combiomed.2020.103795.
- [11] S. Mushtaq and A. H. Mir, "Digital image forgeries and passive image authentication techniques: A survey," *International Journal of Advanced Science and Technology*, vol. 73, pp. 15–32, 2014, doi: 10.14257/ijast.2014.73.02.
- [12] T. K. Huynh, K. V. Huynh, T. Le Tien, and S. C. Nguyen, "A survey on Image Forgery Detection techniques," *Proceedings - 2015 IEEE RIVF International Conference on Computing and Communication Technologies: Research, Innovation, and Vision for Future, IEEE RIVF 2015*, pp. 71–76, 2015, doi: 10.1109/RIVF.2015.7049877.
- [13] M. Ali Qureshi and M. Deriche, "A review on copy move image forgery detection techniques," *2014 IEEE 11th International Multi-Conference on Systems, Signals and Devices, SSD 2014*, 2014, doi: 10.1109/SSD.2014.6808907.

- [14] W. N. Nathalie Diane, S. Xingming, and F. K. Moise, "A survey of partition-based techniques for copy-move forgery detection," *Scientific World Journal*, vol. 2014, 2014, doi: 10.1155/2014/975456.
- [15] M. F. Jwaïd and T. N. Baraskar, "Study and analysis of copy-move & splicing image forgery detection techniques," *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, pp. 697–702, 2017, doi: 10.1109/I-SMAC.2017.8058268.
- [16] M. Elmaci, A. N. Toprak, and V. Aslantas, "A comparative study on the detection of image forgery of tampered background or foreground," *9th International Symposium on Digital Forensics and Security, ISDFS 2021*, 2021, doi: 10.1109/ISDFS52919.2021.9486363.
- [17] B. Zhou, A. Lapedriza, J. Xiao, A. Torralba, and A. Oliva, "Learning deep features for scene recognition using places database," *Advances in Neural Information Processing Systems*, vol. 1, no. January, pp. 487–495, 2014, [Online]. Available: [https://www.researchgate.net/publication/279839496\\_Learning\\_Deep\\_Features\\_for\\_Scene\\_Recognition\\_using\\_Places\\_Database](https://www.researchgate.net/publication/279839496_Learning_Deep_Features_for_Scene_Recognition_using_Places_Database).
- [18] E. Shelhamer, J. Long, and T. Darrell, "Fully convolutional networks for semantic segmentation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 4, pp. 640–651, 2017, doi: 10.1109/TPAMI.2016.2572683.
- [19] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, 2017, doi: 10.1145/3065386.
- [20] C. Szegedy *et al.*, "Going deeper with convolutions," *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 07-12-June-2015, pp. 1–9, 2015, doi: 10.1109/CVPR.2015.7298594.
- [21] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings*, 2015.
- [22] E. I. A. El-Latif, A. Taha, and H. H. Zayed, "Image splicing detection using uniform local binary pattern and wavelet transform," *ARN Journal of Engineering and Applied Sciences*, vol. 14, no. 20, pp. 7679–7684, 2019, doi: 10.36478/JEASCI.2019.7679.7684.
- [23] E. I. Abd El-Latif, A. Taha, and H. H. Zayed, "A passive approach for detecting image splicing based on deep learning and wavelet transform," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 3379–3386, 2020, doi: 10.1007/s13369-020-04401-0.
- [24] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," *Signal, Image and Video Processing*, vol. 11, no. 1, pp. 81–88, 2017, doi: 10.1007/s11760-016-0899-0.
- [25] G. Ulutas, A. Ustubioglu, B. Ustubioglu, V. V. Nabyev, and M. Ulutas, "Medical image tamper detection based on passive image authentication," *Journal of Digital Imaging*, vol. 30, no. 6, pp. 695–709, 2017, doi: 10.1007/s10278-017-9961-x.
- [26] S. H. Gill *et al.*, "Extended forgery detection framework for covid-19 medical data using convolutional neural network," *Computers, Materials and Continua*, vol. 68, no. 3, pp. 3773–3787, 2021, doi: 10.32604/cmc.2021.016001.
- [27] N. Kaur, N. Jindal, and K. Singh, "A passive approach for the detection of splicing forgery in digital images," *Multimedia Tools and Applications*, vol. 79, no. 43–44, pp. 32037–32063, 2020, doi: 10.1007/s11042-020-09275-w.
- [28] F. M. Al-Azrak *et al.*, "An efficient method for image forgery detection based on trigonometric transforms and deep learning," *Multimedia Tools and Applications*, vol. 79, no. 25–26, pp. 18221–18243, 2020, doi: 10.1007/s11042-019-08162-3.
- [29] K. Hayat and T. Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms," *Computers and Electrical Engineering*, vol. 62, pp. 448–458, 2017, doi: 10.1016/j.compeleceng.2017.03.013.
- [30] E. Guanabara, K. Ltda, E. Guanabara, and K. Ltda, "COVID-19 radiography database," 2023, [Online]. Available: <https://www.kaggle.com/tawsifurrahman/covid19-radiography-database>.
- [31] E. I. Nour Eldeen Khalifa, Abd El-Latif, "COVID-19 digital x-rays forgery dataset," 2022.

## BIOGRAPHIES OF AUTHORS



**Eman I. Abd El-Latif**    received the M.Sc. and Ph.D. degree in computer science, at Faculty of Science, Benha University, Egypt, in 2016 and 2020 respectively. She is currently working a lecturer at computer science and mathematics department, Benha University, Egypt. Her areas of research include Digital Forensics, Security (Encryption-Steganography) and image processing. She can be contacted at email: eman.mohamed@fsc.bu.edu.eg.



**Nour Eldeen Khalifa**    received his B.Sc., M.Sc. and Ph.D. degree in 2006, 2009 and 2013 respectively, all from Cairo University, Faculty of Computers and Artificial Intelligence, Cairo, Egypt. He also had a Professional M.Sc. Degree in Cloud Computing in 2018. He authored/coauthored more than 40 publications and 2 edited books. He had more than 2000 citations. He reviewed several papers for international journals and conferences including (Scientific Reports, IEEE IoT, Neural Computing, and Artificial Intelligence Review). Currently, he is an associate professor at Faculty of Computers and Artificial Intelligence, Cairo University. His research interests include wireless sensor networks, cryptography, multimedia, network security, machine, and deep learning. He can be contacted at email: nourmahmoud@cu.edu.eg.