IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 17, 2022, accepted April 28, 2022, date of publication May 3, 2022, date of current version May 11, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3172273

An Efficient CNN Model to Detect Copy-Move Image Forgery

KHALID M. HOSNY[1], **(Senior Member, IEEE), AKRAM M. MORTDA**[2], **MOSTAFA M. FOUDA**[3], **(Senior Member, IEEE), AND NABIL A. LASHIN**[1]

[1]Department of Information Technology, Zagazig University, Zagazig 44519, Egypt
[2]Department of Information Technology, Faculty of Information Technology and Computer Science, Sinai University, Arish 16020, Egypt
[3]Department of Electrical and Computer Engineering, Idaho State University, Pocatello, ID 83209, USA

Corresponding author: Khalid M. Hosny (k_hosny@yahoo.com)

ABSTRACT Recently, digital images have become used in many applications, where they have become the focus of digital image processing researchers. Image forgery represents one hot topic on which researchers prioritize their studies. We concentrate on the copy-move image forgery topic as a deceptive forgery type. In copy-move image forgery, a part of an image is copied and placed in the same image to produce the forgery image. In this paper, an accurate convolutional neural network(CNN) architecture is proposed for the effective detection of copy-move image forgery. The proposed architecture is computationally lightweight with a suitable number of convolutional and max-pooling layers. We also present a fast and accurate testing process with 0.83 seconds for every test. Many empirical experiments have been conducted to ensure the efficiency of the proposed model in terms of accuracy and time. These experiments were done on benchmark datasets and have achieved 100% accuracy.

INDEX TERMS Image forgery detection, copy-move, convolutional neural network, image processing.

I. INTRODUCTION

Digital images are essential data that are used in many applications such as forensics [1], as evidence in the court, computer-aided medical diagnosis systems [2], social networks [3], and the military [4]. Based on their importance, it is necessary to ensure their authenticity and keep their contents tamper-proof. Many computer programs enable users and ordinary people to falsify digital images, which results in the difficult detection of fake images by the eye. Because fraud tools have been widely available, it is now required to assess whether two types of pictures are fabricated or genuine. In other words, it is necessary to develop modern techniques to detect forged images.

The main approaches for discovering image forgery are divided into active and passive approaches [5], as shown in Figure 6. The active approach enables us to insert watermarks, Digital Signatures onto images while creating them. The passive approach enables us to change correct information to incorrect information and shadow important images. Digital image forgery can be classified into five types: copy-move forgery, image splicing, image retouching, morphing, and enhancement. Figures 1, 2, 3, 4, and 5 are examples of the five types of digital image forgery.

The copy-move is one of the most common types of digital image forgery. Many approaches for detecting copy-move forgery in digital images were proposed. Generally, we could classify these approaches into three main groups: First, the traditional copy-move forgery detection approach involves well-known local feature extractors such as SIFT, SURF, and ORB [6]. Second, the orthogonal moment-based approach uses geometric invariant orthogonal moments to extract the features. The third is the deep learning-based copy-move forgery detection approach, in which various approaches of deep learning are used.

A. TRADITIONAL COPY-MOVE FORGERY DETECTION APPROACH

Hashmi *et al.* [9] proposed an algorithm for copy-move forgery (CMF) detection based on the Discrete Wavelet Transform. According to DCT and SVD, Zhao *et al.* [7] introduced an efficient method for CMF. This approach gives good results in the case of multiple CMFs. Chihaoui *et al.* [8] combine Invariant Feature Transform (SIFT) and Singular Value Decomposition (SVD) methods to introduce an efficient

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

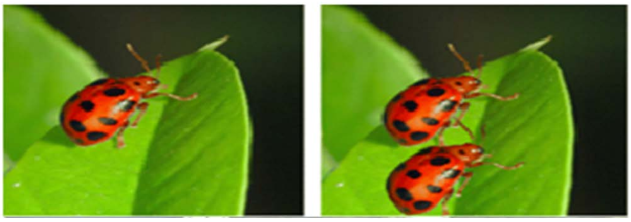


FIGURE 1. Copy move: the left image is the original, and the right is copy-move.

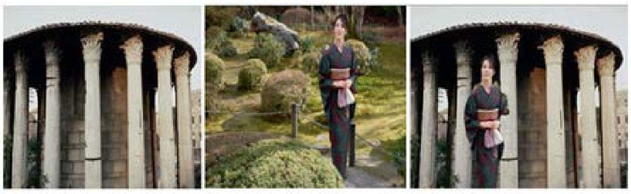


FIGURE 2. Image splicing: in the left and center are original images, and in the right is the splicing.

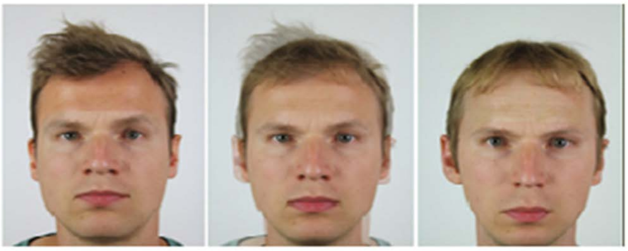


FIGURE 3. Image morphing: in the left and center are original images, and in the right is the morphed.

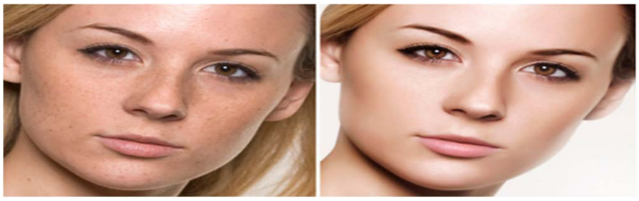


FIGURE 4. Retouching image: the left image is the original face, and the right image is the retouching face.

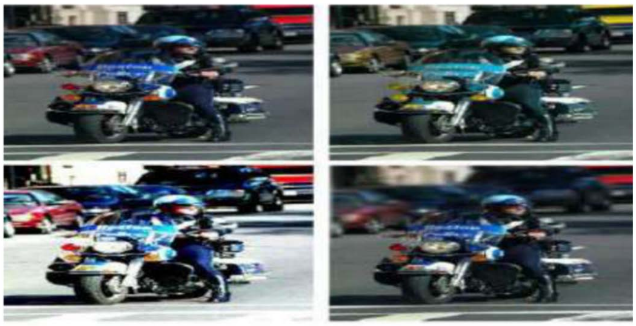


FIGURE 5. Image Enhanced: The upper left corner is the original, followed by various enhancements such as color change blurring of the background. Finally, in the lower right corner is the enhanced image.

approach for the automatic detection of duplicated regions in the same image. The proposed approach demonstrated high robustness against the geometrical transformations. Dhivya *et al.* [10] suggested an approach for CMF detection based on 2-Level DWT to separate the bands and blocks and SURF for feature extraction.

Diwan *et al.* [14] suggested a new technique for CMF. They used the good results of the CenSurE keypoint and the FERAK as feature descriptors and produced a stable and accurate CMF detection algorithm. Priyanka *et al.* [11] merged DCT and SVD and introduced an efficient CMF detection algorithm. The proposed approach gives high accuracy in the presence of different image deformations. A novel technique for CMF detection based on SIFT and the reduced LBP has been introduced by Park *et al.* [12]. This approach reveals when compared with other existing methods.

B. MOMENT-BASED COPY-MOVE FORGERY DETECTION APPROACH

Recently, various techniques for CMFD based on image moments have been proposed. Hosny *et al.* [20] suggested a fast and accurate algorithm for CMFD based on polar complex exponential transform moments PCETMs. The proposed approach exhibited high accuracy with different types of image deformations. The previous approach [20] has been upgraded using the quaternion concept applicable to color images Hosny *et al.* [21]. Meena *et al.* [22] introduced a very appropriate method for CMFD based on Gaussian Hermite Moments GHMs. The empirical results proved the accuracy of the proposed approach to detect the copy moved forged regions. Good characteristics of both techniques: speed-up robust feature SURF and PCET, was the motive for Wang *et al.* [23] to introduce an efficient and accurate method for CMFD, SURF is used to detect the key points.

In contrast, the features of the images are extracted using the PCETMs. Wang *et al.* [24] merged the singular value decomposition SVD and the PCET approaches to introduce the SVD-PCET approach. At first, the invariant geometric moments of an image are extracted using the PCET, then SVD is used to reduce the dimension of the obtained feature matrix. Various experiments proved the accuracy of the SVD-PCET as a CMFD approach.

C. DEEP LEARNING-BASED COPY-MOVE FORGERY DETECTION APPROACH

One of the hot topics that have been used in various fields is deep learning. The CMFD represents one of these fields. Deep learning mainly depends on CNN. Through CNN, their many stages. At each stage, a set of features are generated. Some features are used as a training set. Methods based on deep learning reveal better performance than traditional and moment-based approaches. Recently, many CMFD approaches based on deep learning have been presented. Elaskily *et al.* [25] presented an efficient approach for automatic CMFD based on CNN, and the suggested approach achieved 100% accuracy when applied to different datasets.

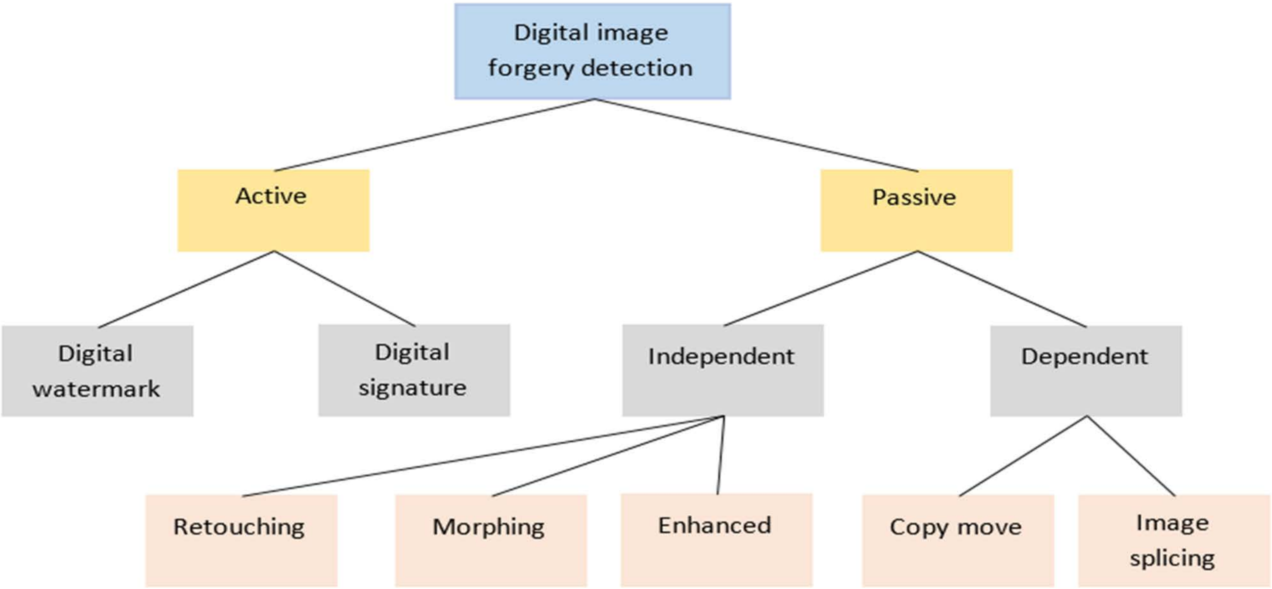


FIGURE 6. Type of digital image forgery detection.

Goel *et al.* [28] suggested a CMFD system based on a novel technique called dual branch CNN. The proposed system proves good results in terms of time and performance. Ortega *et al.* [27] proposed two approaches for CMFD based on deep learning: a custom architecture model and a transfer learning model. The proposed system has been tested over eight benchmark datasets. Abhishek *et al.* [26] introduced an efficient system to detect and localize the image forgeries based on deep CNN and semantic segmentation. The obtained results give accuracy above 98%. Jaiswal *et al.* [29] presented a CMFD model it used multi-scale input and two blocks of convolutional layers: encoder and decoder blocks. The empirical results proved the high accuracy of the proposed system. As a result of the previous discussion, it shows a shortage of previous works, and the shortage motivates the author to propose an efficient CNN-based method.

The main contributions presented by this study can be summarized as follow:

- An efficient and accurate CNN model was proposed. It achieved a promising accuracy score as compared with the other investigated models.
- The proposed model is lightweight. It contains three convolutional layers, three max-pooling, 266306 hyper-parameters, and one fully connected layer.
- An analytical comparison of normal and forgery is conducted between the proposed model and the other investigated models (M. Elaskily *et al.* [25], Amerini *et al.* [15], Amerini *et al.* [16], Elaskily *et al.* [17], Mishra *et al.* [18], Kaur *et al.* [19], J. Zhong *et al.* [31], Y. Wu *et al.* [32], A. Islam *et al.* [33], and Y. Zhu *et al.* [34]). The obtained results are superior to other recently published approaches.
- Three benchmark datasets were used in the experiments. These datasets are MICC-F220 [15], MICC-F2000 [15] and MICC-F600 [16]. It is allowed us to present accurate experiments.

The rest of this study contains four sections as follows: Section 2 discusses, in preliminaries, the CNN description. The structure of the proposed approach is presented in Section 3. Our results and discussed in Section 4. Finally, sec. 5 the conclusion.

II. PRELIMINARIES

A. THE DESCRIPTION OF CNN

In this section, we describe in brief the CNN model. CNN is a convolution neural network. Its task is to extract the important features in the image. Deep learning consists of three basic layers: the convolution layer, pooling layer, and fully connected layer.

CNN includes many layers: convolutional layer, max-pooling layer, flattening layer, and full connection layer, as shown in Figure 7.

A. **The convolutional layer:** is the activation function, and it is a non-linear function. It has several types; the activation function is most commonly used. It is a non-linear function with several types, as shown in Figure 8. The most commonly used them are:
   - ReLU (rectified linear unit) Its importance is reducing the number of accounts performed.
   - Sigmoid, which is used in the output layer.

B. **Max-pooling layer:** It collects the features extracted from the image, reduces the dimensions, and extracts the most important features present in the image, as shown in Figure 9.

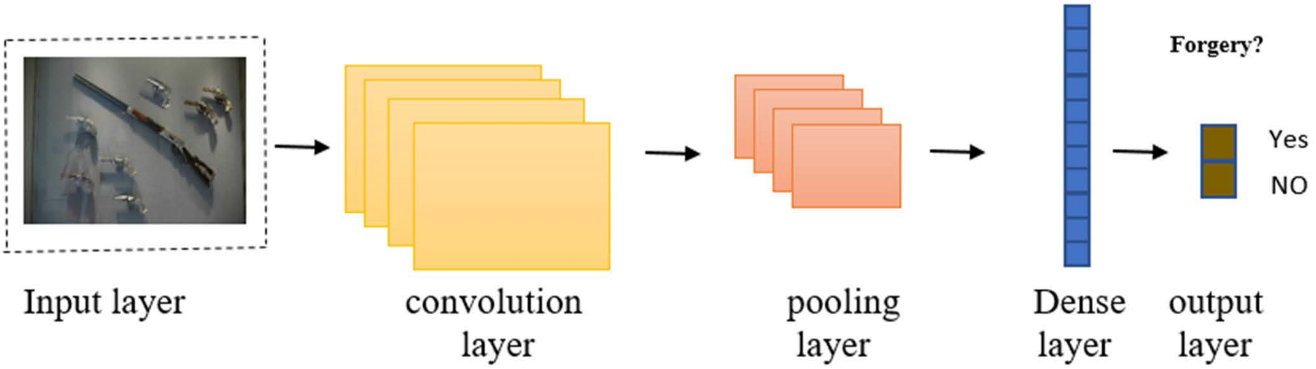
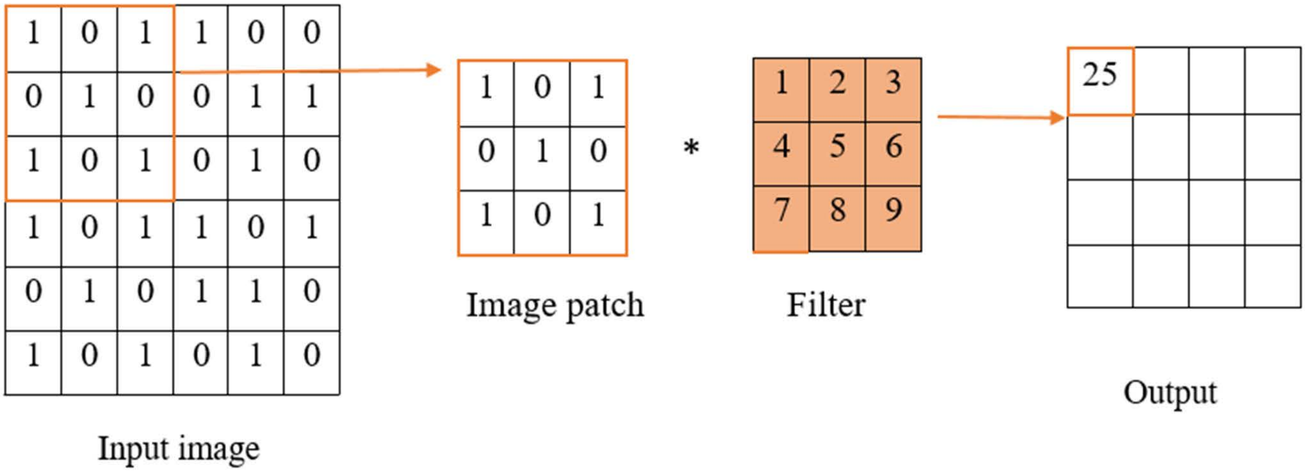


FIGURE 7. CNN layers.



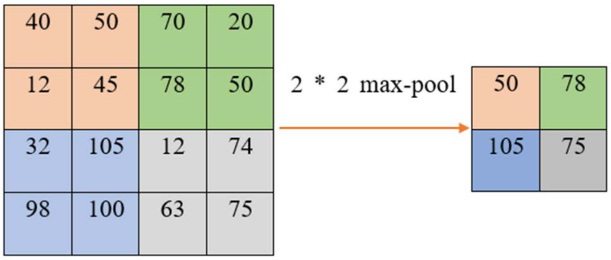
1	0	1	1	0	0
0	1	0	0	1	1
1	0	1	0	1	0
1	0	1	1	0	1
0	1	0	1	1	0
1	0	1	0	1	0

1	0	1
0	1	0
1	0	1

1	2	3
4	5	6
7	8	9

25			

FIGURE 8. Convolution layer.



40	50	70	20
12	45	78	50
32	105	12	74
98	100	63	75

50	78
105	75

FIGURE 9. Max poling layer.

C. **Flattening layer:** it converts the characteristics taken from max-pooling into a one-dimensional matrix

D. **Fully connected layer:** it puts all the neurons together.

III. PROPOSED METHOD

In this paper, an accurate deep CMF detection method was introduced. The proposed approach is based on the CNN model, as shown in Figure 10. The traditional approach works on a block-based algorithm, while the CNN approach works on the whole image. The presented approach has three stages: preprocessing, feature extraction, and classification. The input image is resized to enter the next stage without cropping any image parts in the preprocessing data stage. The feature extraction stage contains three convolution layers, followed by a max-pooling layer. At the end of this stage, a full connection layer connects all features with the dense layer. Finally, the classification stage is called to classify the data into two classifications (forged or original).

The convolution layers as feature mining, in which each convolution layer generates its feature maps using its own set of filters (i.e., ReLU). The feature maps produced from the first convolution layer are used in the next max-pooling layer to produce resized pooled feature maps, considered the inputs of the next convolution layer. The last feature maps merged with the final max-pooling are formatted as vectors and incorporated into Fully Connected.

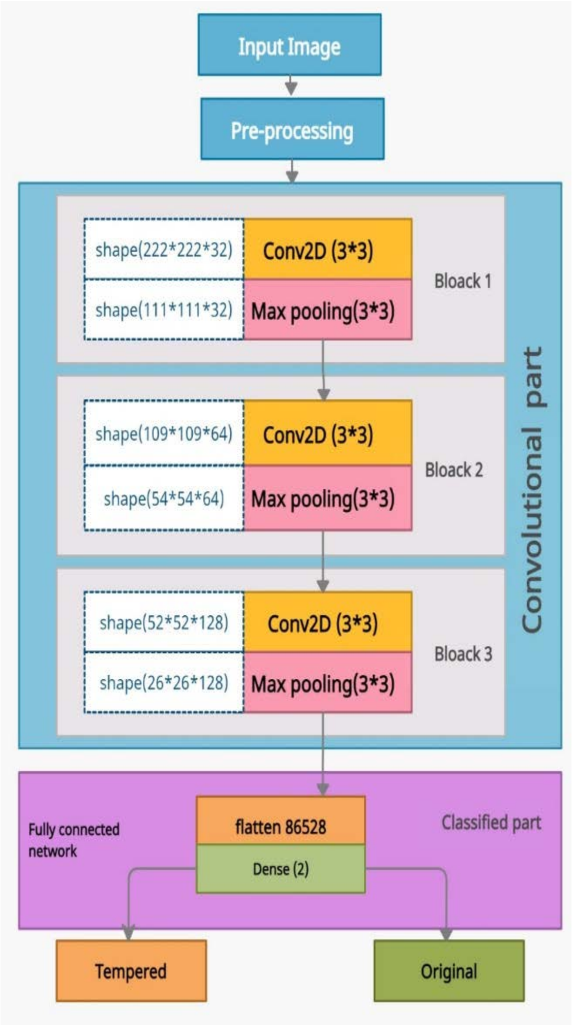


FIGURE 10. The structure of the proposed algorithm CNN layers.

Finally, the dense layer classifies the features extracted from the fully connected layer into two classes (original or tampered).

The proposed model uses the optimizer "rmsprop" and batch size 32, which allows it to be efficiently trained.

IV. RESULTS AND DISCUSSION

This section and a comprehensive assessment of the proposed approach's findings. The tests have been run on the Google Collaborator server with Google compute engine backend (GPU) RAM: 2.5GB/12GB. The TensorFlow with Keras as a backend, using python 3.0.

A. DATASETS

The common usable and famous datasets used to test CMF detection techniques include MICC-F2000 [15], MICC-F600 [16] and MICC-F220 [15]. The contents of these datasets are exposed in Table1.

B. EVALUATION METRICS

To estimate the accuracy of the proposed approach, we used the following accuracy measure:

$$\text{Accuracy} = \frac{(\mathrm{T_N} + \mathrm{T_P})}{(\mathrm{T_P} + \mathrm{F_P} + \mathrm{T_N} + \mathrm{F_N})} \times 100 \tag{1}$$

$$precision = \frac{TP}{TP + FP} * 100 \tag{2}$$

$$Recall = \frac{TP}{TP + FN} * 100 \tag{3}$$

$$F1 - score = \frac{2 * (precision * precall)}{(precision + Recall)} \tag{4}$$

$\mathrm{T_P}$ represent the number of tampered images that are genuinely detected as tampered images, while $\mathrm{F_P}$ represent the number of original images that are falsely detected as tampered images. The F_N refers to the number of tampered images falsely detected as original images. $\mathrm{T_N}$ represent the number of original images that are genuinely detected as original images.

We have used the Logarithmic loss (Log Loss) to determine the false classified classes. If we have M classes containing N samples, the Logarithmic loss is:

$$logless = \frac{-1}{N} \sum_{a=1}^{N} \sum_{b=1}^{M} Z_{ab}.log\,(P_{ab}). \tag{5}$$

where Z_{ab} indicates whether (a) belongs to category (b) or not, the P_{ab} indicates that this sample (a) may belong to category (b). the accuracy value being higher If the Logarithmic loss is near zero.

The Test time (TT) is a key factor in assessing the given method time varies with other algorithms. The TT is the time average spent testing images for (k) iterations of the test process.

C. THE RESULTS OVER THE MICC-F2000 DATA SET

Our study tested over the MICC-F2000 [15] dataset, where the obtained results have been evaluated against recently published approaches [15]–[17], [25], [31]–[34]. In this paper, the original and forgery classes are indicated as The original is positive (showed by + signed in Table 2), while the forgery is negative (showed by – signed in table 2). In table 2, the color blue indicates the number of correctly detected images. The proposed model achieves the accuracy of 100% at no of epochs 35. The investigated models have achieved an accuracy of 98% for M. A. Elaskily *et al.* at no of epochs 35 [25], 90.9% for Amerini *et al.* [15], 92.855% for Amerini *et al.* [16], 96.025% for Elaskily *et al.* [17], 97.79% for J. Zhong *et al.* [31], 94.17% for Y. Wu *et al.* [32], 94.77% for A. Islam *et al.* [33], and 97.59% for Y. Zhu *et al.* [34], as shown in figure 11.

Results obtained through Table 3 specified that the proposed approach is superior to the compared method [25], with values 2, −2, and −4.53 for accuracy, Log loss, and TT, respectively. These results were the best. Through Table 3,

TABLE 1. the details of the MICC-F220, MICC-F2000, and MICC-F600 datasets.

Dataset	Composition				Size of image	No. of training Images				No. of validation Images				No. of testing Images				The input shape
MICC-F220	220 images				722 × 480 pixels and 800 × 600 pixels	160 images				40 images				40 images				224 × 244 × 3 pixels
	tampered	110	original	110		tampered	80	original	80	tampered	20	original	20	tampered	10	original	10	
MICC-F2000	2000 images				2048 × 1536 pixels	1000 images				500 images				500 images				224 × 244 × 3 pixels
	tampered	700	original	1300		tampered	350	original	650	tampered	125	original	375	tampered	142	original	358	
MICC-F600	600 images				800 × 532 and 3888 × 2592 pixels	360 images				180 images				60 images				224 × 244 × 3 pixels
	tampered	152	original	448		tampered	96	original	264	tampered	48	original	132	tampered	16	original	44	

TABLE 2. the confusion matrices of investigated architectures and the proposed architecture with the MICC-F2000 dataset.

Model	Classes	+	-	Total
Proposed Model	+	358	0	358
	-	0	140	140
	Total	358	140	498
Jun-Liu Zhong et al. [31] Model				
	+	351	7	358
	-	4	136	140
	Total	355	143	498
Yue Wu et al. [32] Model				
	+	343	15	358
	-	14	126	140
	Total	357	141	498
Ashraful Islam et al. [33] Model				
	+	344	14	358
	-	12	128	140
	Total	356	142	498
Ye Zhu et al. [34] Model				
	+	353	5	358
	-	7	133	140
	Total	360	138	498

TABLE 3. Comparison between the proposed method and previously on the MICC-F2000 dataset when 25,35 epochs.

Metric		Method		Efficiency gain = proposed – compared
		The Proposed method	M.A. Elaskily et al. [25]	
25 epochs	Accuracy	97.6	95.1	2.5
	log less%	2.4	4.99	-2.59
	TT (sec)	40.2	46.56	-6.36
35 epochs	Accuracy	100	98	2
	log less%	zero	2	-2
	TT (sec)	47.78	52.31	-4.53

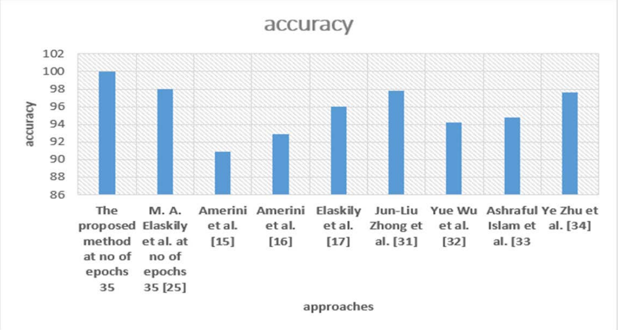


FIGURE 11. The accuracy of the proposed approach against recently published approaches with the MICC-F2000 dataset.

we summarized the results obtained at no of epochs 25. These results were the closest to the best results in Table 3. Also, the superiority of these results was in favor of the proposed approach with an average efficiency gain of 2.5, −2.59, and −6.36 with the accuracy, log loss, and TT, respectively. Table 4 presented experimental results among the proposed approach and other compared approaches [15]–[17], [25], [31]–[34]. The results showed outperformance in terms of accuracy and TT.

D. THE RESULTS OVER THE MICC-F600 DATA SET

The proposed approach was tested over the MICC-F600 [16] data set. The obtained results have been evaluated against other recently published methods [15]–[17], [25], [31]–[34]. The confusion matrices for the proposed and existing methods are shown in table 5. The color blue indicates the number of correctly detected images. The investigated models have achieved an accuracy of 96.078% for M. A. Elaskily *et al.* at

TABLE 4. Comparison between the proposed method and previously published approaches on the MICC-F2000 dataset.

Comparison methods	The proposed method at no of epochs 35	M. A. Elaskily et al. at no of epochs 35 [25]	Amerini et al. [15]	Amerini et al. [16]	Elaskily et al. [17]	Jun-Liu Zhong et al. [31]	Yue Wu et al. [32]	Ashraful Islam et al. [33]	Ye Zhu et al. [34]
TP	100	97.73	93.42	94.86	98.40	98	95.8	96	98.6
FP	Zero	1.39	11.61	9.15	6.35	2.86	10	8.6	5
FN	Zero	2.27	6.58	5.14	1.60	2	4.2	4	1.4
TN	100	98.61	88.39	90.85	93.65	97.14	90	91.4	95
Accuracy	100	98	90.90	92.855	96.025	97.79	94.17	94.77	97.59
TT(mm:ss)	00:47	01:19	312:18	180:15	46:58	2:36	16:06	18:34	6:12

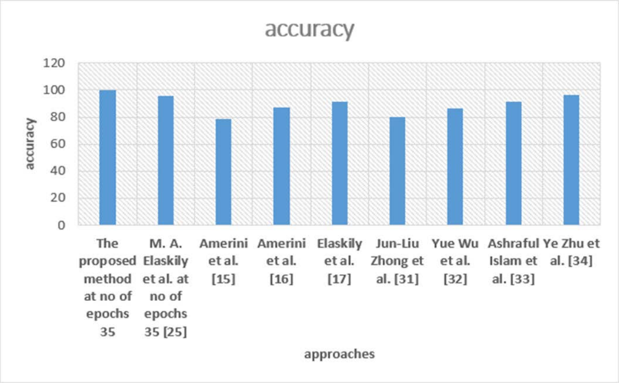


FIGURE 12. The accuracy of the proposed approach against recently published approaches with the MICC-F2000 dataset.

TABLE 5. the confusion matrices of investigated architectures and the proposed architecture with the MICC-F600 dataset.

Model	Classes	+	-	Total
Proposed Model	+	46	0	46
	-	0	14	14
	Total	46	14	60
Jun-Liu Zhong et al. [31] Model				
	+	39	7	46
	-	5	9	14
	Total	44	16	60
Yue Wu et al. [32] Model				
	+	41	5	46
	-	3	11	14
	Total	44	16	60
Ashraful Islam et al. [33] Model				
	+	43	3	46
	-	2	12	14
	Total	45	15	60
Ye Zhu et al. [34] Model				
	+	45	1	46
	-	1	13	14
	Total	46	14	60

no of epochs 35 [25], 78.35% for Amerini *et al.* [15], 87.165% for Amerini *et al.* [16], 91.575% for Elaskily *et al.* [17], 80.0% for J. Zhong *et al.* [31], 86.66% for Y. Wu *et al.* [32], 91.66% for A. Islam *et al.* [33], and 96.66% for Y. Zhu *et al.* [34], as sh The proposed model achieves an accuracy of 100% at no epochs 35.

TABLE 6. the proposed method versus PREVIOUSLY METHODS on the MICC-F600 when 25,35 EPOCHS.

	Metric	Method		Efficiency gain = proposed – compared
		The Proposed method	M.A. Elaskily et al. [25]	
25 epochs	Accuracy	97.8	94.11	3.69
	log less%	2.2	5.88	-3.68
	TT (sec)	9.6	9.81	-0.21
35 epochs	Accuracy	100	96.08	3.9
	log less%	Zero	3.9	-3.9
	TT (sec)	7.73	8.93	-1.2

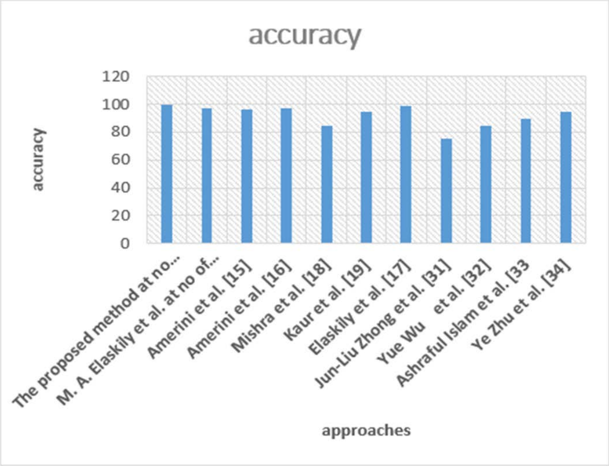


FIGURE 13. The accuracy of the proposed approach against recently published approaches with the MICC-F2000 dataset.

The introduced approach has the best results at no of epochs 35, where when compared with the results in [25], the obtained efficiency gain was in favor of it with values 3.9, −3.9, and −1.2 in terms of accuracy, Log loss, and TT respectively. These results appear in Table 6. We summarized the results obtained at no of epochs 25 in Table 6. These results were the closest to the best results we obtained in Table 6. Also, these results' superiority favored the proposed approach with an average efficiency gain of 3.69, −3.68, and −0.21 with the accuracy, log loss, and TT, respectively.

TABLE 7. The proposed method VERSUS previously published approaches on MICC-F600.

Comparison methods	The proposed method at no of epochs 35	M. A. Elaskily et al. at no of epochs 35 [25]	Amerini et al. [15]	Amerini et al. [16]	Elaskily et al. [17]	Jun-Liu Zhong et al. [31]	Yue Wu et al. [32]	Ashraful Islam et al. [33]	Ye Zhu et al. [34]
TP	100	96.77	69.20	81.60	94.50	84.78	89.13	93.48	97.82
FP	Zero	5.0	12.50	7.27	11.35	35.71	21.43	14.28	6.15
FN	Zero	3.23	30.80	18.40	5.5	15.21	10.87	6.52	2.18
TN	100	95.0	87.50	92.73	88.65	64.28	78.57	85.72	92.85
Accuracy	100	96.078	78.35	87.165	91.575	80.0	86.66	91.66	96.66
TT(mm:ss)	00:7	00:24	115:00	76:21	17:37	1:50	1:13	3:02	1:02

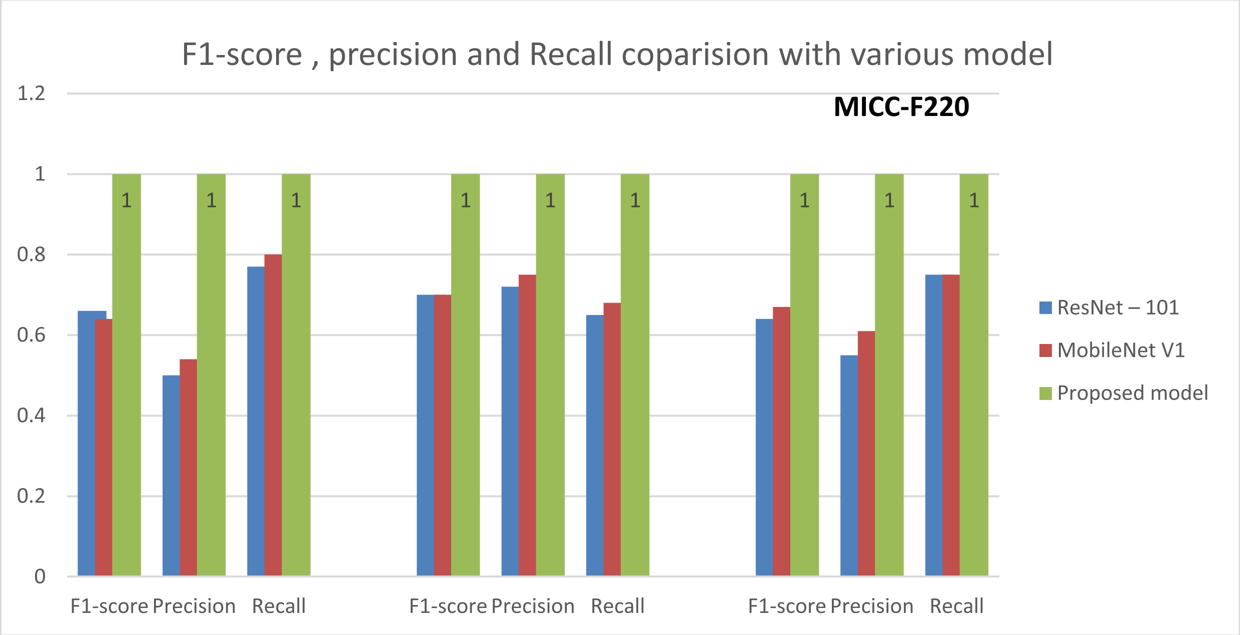


FIGURE 14. F1-score, precision, and Recall comparison with ResNet-101, MobileNet v1, and proposed model for MICC-F2000, MICC-F600, and MICC-F220 dataset.

TABLE 8. the confusion matrices of investigated architectures and the proposed architecture with the MICC-F220 dataset.

Model	Classes	+	-	Total
Proposed Model	+	10	0	10
	-	0	10	10
	Total	10	10	20
Jun-Liu Zhong et al. [31] Model				
	+	8	2	10
	-	3	7	10
	Total	11	9	20
Yue Wu et al. [32] Model				
	+	9	1	10
	-	2	8	10
	Total	11	9	20
Ashraful Islam et al. [33] Model				
	+	10	0	10
	-	2	8	10
	Total	12	8	20
Ye Zhu et al. [34] Model				
	+	10	0	10
	-	1	9	10
	Total	11	9	20

TABLE 9. the proposed method versus PREVIOUSLY METHODS on the MICC-F220 when 25,35 epochs.

Metric		Method		Efficiency gain = proposed – compared
		The Proposed method	M.A. Elaskily et al. [25]	
25 epochs	Accuracy	97.8	96.15	2.05
	log less%	1.8	3.85	-2.05
	TT (sec)	1.1	1.6	-0.5
35 epochs	Accuracy	100	97.62	2.38
	log less%	zero	2.38	-2.38
	TT (sec)	0.83	1.31	-0.48

Table 7 presented experimental results among the proposed approach and other compared approaches [15]–[17], [25]. The results showed outperformance favoring the proposed approach regarding accuracy and TT.

E. THE RESULTS USING THE MICC-F220 DATASET

The last experiment was performed over one benchmark dataset called MICC-F220 [15]. The obtained results have

TABLE 10. The proposed method VERSUS previously published approaches on MICC-F220.

	The proposed method at no of epochs 35	Mohamed A. Elaskily et al. [25] at no of epochs 35	Amerini et al. [15]	Amerini et al. [16]	Mishra et al. [18]	Kaur et al. [19]	Elaskily et al. [17]	Jun-Liu Zhong et al. [31]	Yue Wu et al. [32]	Ashraful Islam et al. [33]	Ye Zhu et al. [34]
TP	100	95.45	100	100	73.64	97.27	100	80	90	100	100
FP	zero	zero	8	6	3.64	7.27	1.80	30	20	20	10
FN	zero	4.55	Zero	Zero	26.36	2.73	Zero	20	10	0	0
TN	100	100	92	94	96.36	92.73	98.20	70	80	80	90
Accuracy	100	97.62	96.00	97.00	85.00	95.00	99.1	75	85	90	95
TT(mm:ss)	0: .83	0:14	24:13	16:05	0:2.85	N/A	2:48	0:30	0:26	1:2	0:53

TABLE 11. F1-score, precision and recall comparison with ResNet-101, MobileNet v1, and proposed model.

Dataset	ResNet – 101 [30]			MobileNet V1 [30]			Proposed model		
	F1-score	Precision	Recall	F1-score	Precision	Recall	F1-score	Precision	Recall
MICC-F600	0.70	0.72	0.65	0.70	0.75	0.68	1.0	1.0	1.0
MICC-F220	0.64	0.55	0.75	0.67	0.61	0.75	1.0	1.0	1.0
MICC-F2000	0.66	0.50	0.77	0.64	0.54	0.80	1.0	1.0	1.0

been evaluated against other recently published methods [25], [15]–[19], [31]–[34]. We demonstrated the confusion matrices for the proposed approach and investigated approaches shown in table 8. The color blue indicates the number of correctly detected images. The proposed model achieves accuracy of 100% at no of epochs 35, the investigated models are achieved accuracy of 97.62% for M. A. Elaskily *et al.* at no of epochs 35 [25], 96.0% for Amerini *et al.* [15], 97.0% for Amerini *et al.* [16], 99.1% for Elaskily *et al.* [17], 85.0% for Mishra *et al.* [18], 95.0% for Kaur *et al.* [19], 75.0% for J. Zhong *et al.* [31], 85.0% for Y. Wu *et al.* [32], 90.0% for A. Islam *et al.* [33], and 95.0% for Y. Zhu *et al.* [34], as shown in figure 13.

The introduced approach has the best results at no of epochs 35, where when compared with the results in [25], the obtained efficiency gain was in favor of it with values 2.38, −2.38, and −0.48 in terms of accuracy, Log loss, and TT respectively. These results appear in Table 9.

We summarized the results obtained at no of epochs 25 in Table 9. These results were the closest to the best results we obtained. Also, the superiority of these results was in favor of the proposed approach with an average efficiency gain of 2.05, −2.05, and −0.5 with the accuracy, log loss, and TT, respectively.

Table 10 presented experimental results among the proposed approach and other compared approaches [15]–[19], [25]. The results showed outperformance favoring the proposed approach regarding accuracy and TT.

The proposed method varies from the Dhananjay *et al.* [30] method on a different dataset, MICC-F600 [16], MICC-F220 [15], and MICC-F2000 [15]. The proposed approach has the best results. Tables 11 and 14 show that the proposed approach outperforms F1-score, precision, and recall.

V. CONCLUSION

In conclusion, this study introduced a Copy-move Forgery Detection methodology based on deep neural learning. The proposed model can recognize the tampered images, classifying the candidate's image into two types of classification: forged and original. The proposed system can create feature vectors from an image's features. The suggested approach automatically uses the full connection layer to find feature correspondences and dependencies. The proposed model must be trained first to be ready to test and then classify the tampered images. The performance of the proposed model was assessed through three benchmark datasets: MICC-F2000, MICC-F600, and MICC-F220. The numerical results after investigating and compared with other approaches reveal superiority in favor of the proposed approach. The proposed method achieved 100% accuracy at no epochs 35 with all datasets. In the case of TT, we also achieved good results compared with the existing algorithms. For the datasets MICC-F2000, MICC-F600, and MICC-F220, we obtained a TT equal to 47.48sec, 7.73 sec, and 0.83 sec, respectively. All empirical results proved the high superiority of the proposed model against other reported algorithms in terms of accuracy and TT.

REFERENCES

[1] A. Ross, S. Banerjee, and A. Chowdhury, "Security in smart cities: A brief review of digital forensic schemes for biometric data," *Pattern Recognit. Lett.*, vol. 138, pp. 346–354, Oct. 2020.

[2] M. M. Eltoukhy, M. Elhoseny, K. M. Hosny, and A. K. Singh, "Computer aided detection of mammographic mass using exact Gaussian–Hermite moments," *J. Ambient Intell. Humanized Comput.*, pp. 1–9, Jun. 2018, doi: 10.1007/s12652-018-0905-1.

[3] F. Marcon, C. Pasquini, and G. Boato, "Detection of manipulated face videos over social networks: A large-scale study," *J. Imag.*, vol. 7, no. 10, p. 193, Sep. 2021, doi: 10.3390/jimaging7100193.

[4] K. Sunitha and A. N. Krishna, "Efficient keypoint based copy move forgery detection method using hybrid feature extraction," in *Proc. 2nd Int. Conf. Innov. Mech. Ind. Appl. (ICIMIA)*, Mar. 2020, pp. 670–675.

[5] S. Velmurugan, T. Subashini, and M. Prashanth, "Dissecting the literature for studying various approaches to copy move forgery detection," *Int. J. Adv. Sci. Technol.*, vol. 29, pp. 6416–6438, Jun. 2020.

[6] X. Tian, G. Zhou, and M. Xu, "Image copy-move forgery detection algorithm based on ORB and novel similarity metric," *IET Image Process.*, vol. 14, no. 10, pp. 2092–2100, 2020.

[7] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic Sci. Int.*, vol. 233, nos. 1–3, pp. 158–166, 2013, doi: 10.1016/j.forsciint.2013.09.013.

[8] T. Chihaoui, S. Bourouis, and K. Hamrouni, "Copy-move image forgery detection based on SIFT descriptors and SVD-matching," in *Proc. 1st Int. Conf. Adv. Technol. Signal Image Process. (ATSIP)*, Mar. 2014, pp. 125–129.

[9] M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, "Copy move forgery detection using DWT and SIFT features," in *Proc. 13th Int. Conf. Intellient Syst. Design Appl.*, Dec. 2013, pp. 188–193.

[10] S. Dhivya, B. Sudhakar, and K. Devarajan, "2-level DWT based copy move forgery detection with surf features," in *Proc. 3rd Int. Conf. Commun. Electron. Syst. (ICCES)*, Oct. 2018, pp. 800–805.

[11] P. G. Singh and K. Singh, "An improved block based copy-move forgery detection technique," *Multimedia Tools Appl.*, vol. 79, pp. 13011–13035, May 2020.

[12] J. Park, T. A. Kang, Y. H. Moon, and I. K. Eom, "Copy-move forgery detection using scale invariant feature and reduced local binary pattern histogram," *Symmetry*, vol. 12, p. 492, Apr. 2020, doi: 10.3390/sym12040492.

[13] X. Tian, G. Zhou, and M. Xu, "Image copy-move forgery detection algorithm based on ORB and novel similarity metric," *IET Image Process.*, vol. 14, pp. 2092–2100, Oct. 2020.

[14] A. Diwan, R. Sharma, A. Roy, and S. Mitra, "Keypoint based comprehensive copy-move forgery detection," *IET Image Processing*, vol. 15, pp. 1298–1309, May 2021.

[15] I. Amerini, L. Ballan, R. Cardelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1099–1110, Mar. 2011.

[16] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage," *Signal Process., Image Commun.*, vol. 28, no. 6, pp. 659–669, Jul. 2013.

[17] M. Elaskily, H. Elnemr, M. Dessouky, and O. Faragallah, "Two stages object recognition based copy-move forgery detection algorithm," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15353–15373, 2019.

[18] N. Mishra, S. Sharma, and R. Patel, "Region duplication forgery detection technique based on SURF and HAC," *Sci. World J.*, vol. 7, pp. 1–8, Nov. 2013.

[19] H. Kaur and J. Saxena, "Simulative comparison of copy-move forgery detection methods for digital images," *Int. J. Electron., Elect. Comput. Syst.*, vol. 4, pp. 62–66, Sep. 2015.

[20] K. M. Hosny, H. M. Hamza, and N. A. Lashin, "Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators," *Imag. Sci. J.*, vol. 66, no. 6, pp. 330–345, Aug. 2018.

[21] K. Hosny, H. Hamza, and N. Lashin, "Copy-for-duplication forgery detection in colour images using QPCETMs and sub-image approach," *IET Image Process.*, vol. 13, no. 9, pp. 1437–1446, 2019.

[22] K. Meena and V. Tyagi, "A copy-move image forgery detection technique based on Gaussian-Hermite moments," *Multimedia Tools Appl.*, vol. 78, pp. 33505–33526, Dec. 2019.

[23] C. Wang, Z. Zhang, Q. Li, and X. Zhou, "An image copy-move forgery detection method based on SURF and PCET," *IEEE Access*, vol. 7, pp. 170032–170047, 2019.

[24] Y. Wang, X. Kang, and Y. Chen, "Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures," *J. Inf. Secur. Appl.*, vol. 54, Oct. 2020, Art. no. 102536.

[25] M. Elaskily, H. Elnemr, A. Sedik, M. Dessouky, G. El Banby, O. Elshakankiry, A. Khalaf, H. Aslan, O. Faragallah, and F. A. El-Samie, "A novel deep learning framework for copy-moveforgery detection in images," *Multimedia Tools Appl.*, vol. 79, pp. 19167–19192, Jul. 2020.

[26] Abhishek and N. Jindal, "Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation," *Multimedia Tools Appl.*, vol. 80, pp. 3571–3599, Jan. 2021.

[27] Y. Rodriguez-Ortega, D. M. Ballesteros, and D. Renza, "Copy-move forgery detection (CMFD) using deep learning for image and video forensics," *J. Imag.*, vol. 7, no. 3, p. 59, Mar. 2021, doi: 10.3390/jimaging7030059.

[28] N. Goel, S. Kaur, and R. Bala, "Dual branch convolutional neural network for copy move forgery detection," *IET Image Process.*, vol. 15, p. 656, Feb. 2021.

[29] A. Jaiswal and R. Srivastava, "Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model," *Neural Process. Lett.*, vol. 54, pp. 75–100, Aug. 2021, doi: 10.1007/s11063-021-10620-9.

[30] K. Dhananjay, S. Ahirrao, and K. Kotecha, "Efficient approach towards detection and identification of copy move and image splicing forgeries using mask R-CNN with MobileNet V1," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–21, Jan. 2022, doi: 10.1155/2022/6845326.

[31] J.-L. Zhong and C.-M. Pun, "An end-to-end dense-inceptionNet for image copy-move forgery detection," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2134–2146, 2020, doi: 10.1109/TIFS.2019.2957693.

[32] Y. Wu, W. Abd-Almageed, and P. Natarajan, "BusterNet: Detecting copy-move image forgery with source/target localization," in *Proc. Conf. Comput. Vis. Pattern Recognit.*, 2018, pp. 168–184. [Online]. Available: https://link.springer.com/conference/eccv

[33] A. Islam, C. Long, A. Basharat, and A. Hoogs, "DOA-GAN: Dual-order attentive generative adversarial network for image copy-move forgery detection and localization," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Jun. 2020, pp. 4676–4685.

[34] Y. Zhu, Ch. Chen, G. Yan, Y. Guo, and Y. Dong, "AR-Net: Adaptive attention and residual refinement network for copy-move forgery detection," *IEEE Trans. Ind. Informat.*, vol. 16, pp. 6714–6723, 2020, doi: 10.1109/TII.2020.2982705.

KHALID M. HOSNY (Senior Member, IEEE) was born in Zagazig, Egypt, in 1966. He received the B.Sc., M.Sc., and Ph.D. degrees from Zagazig University, Egypt, in 1988, 1994, and 2000, respectively. From 1997 to 1999, he was a Visiting Scholar with the University of Michigan, Ann Arbor, and the University of Cincinnati, Cincinnati, USA. He is currently a Professor in information technology with the Faculty of Computers and Informatics, Zagazig University. He has published three edited books and more than 100 articles in international journals. His research interests include image processing, pattern recognition, multimedia security, and computer vision. According to the recent edition of the Stanford rank, he is included in the list of top 1% scientists worldwide. He is a Senior Member of ACM. He is an editor and a scientific reviewer for more than 50 international journals.

AKRAM M. MORTDA was born in Elbhara, Egypt, in 1993. He received the B.Sc. degree in information technology from the Faculty of Information Technology and Computer Science, Sinai University, Egypt, in 2016. He is currently working as a Teaching Assistant with the Information Technology Department, Faculty of Information Technology and Computer Science, Sinai University. His research interests include image processing and deep learning.

MOSTAFA M. FOUDA (Senior Member, IEEE) received the Ph.D. degree in information sciences from Tohoku University, Japan, in 2011. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, Idaho State University, ID, USA. He also holds the position of an Associate Professor with Benha University, Egypt. He has worked as an Assistant Professor at Tohoku University, Japan. He was a Postdoctoral Research Associate with Tennessee Technological University, TN, USA. He has been engaged in research on cybersecurity, communication networks, wireless mobile communications, smart healthcare, smart grids, AI, blockchain, and the IoT. He has published more than 60 papers in prestigious peer-reviewed journals and conferences. He received the prestigious 1st place award during his graduation from the Faculty of Engineering at Shoubra, Benha University, in 2002. He has served as the Symposium/the Track Chair of the IEEE VTC2021-Fall Conference. He has also served as the Workshops Chair, the Session Chair, a Technical Program Committee (TPC) Member, and a Designated Reviewer in leading international conferences, such as IEEE GLOBECOM, ICC, PIMRC, ICCVE, IWCMC, and 5G World Forum. He also served as a Guest Editor of some special issues of several top-ranked journals, such as IEEE WIRELESS COMMUNICATIONS (WCM) and *IEEE Internet of Things Magazine* (IoTM). He also serves as a Referee for some renowned IEEE journals and magazines, such as IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE WIRELESS COMMUNICATIONS, IEEE WIRELESS, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, IEEE TRANSACTIONS ON SMART GRID, IEEE ACCESS, IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING, and *IEEE NETWORK*. He is an Editor of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY (TVT) and an Associate Editor of IEEE ACCESS.

NABIL A. LASHIN received the B.Sc. degree in communication and electronics engineering from Zagazig University, Egypt, in 1993, the M.Sc. degree in communication and electronics engineering from Cairo University, in 1999, and the Ph.D. degree in electrical engineering and computer science from the Technical University of Berlin, Germany, in 2005. He is currently an Assistant Professor in information technology with Zagazig University.