Multimedia Tools and Applications
https://doi.org/10.1007/s11042-019-08162-3

An efficient method for image forgery detection based on trigonometric transforms and deep learning

Faten Maher Al_Azrak[1] · Ahmed Sedik[2] · Moawad I. Dessowky[1] · Ghada M. El Banby[3] · Ashraf A. M. Khalaf[4] · Ahmed S. Elkorany[1] · Fathi E. Abd. El-Samie[1]

Received: 6 March 2019 / Revised: 17 August 2019 / Accepted: 2 September 2019

Abstract
Image forgery detection is the basic key to solve many problems, especially social problems such as those in Facebook, and court cases. The common form of image forgery is the copy-move forgery, in which a section of the image is copied and pasted in another location within the same image. In this type of image forgery, it is easy to perform forgery, but more difficult to detect it, because the features of the copied parts are similar to those of the other parts of the image. This paper presents an approach for copy-move forgery detection based on block processing and feature extraction from the transforms of the blocks. In addition, a Convolutional Neural Network (CNN) is used for forgery detection. The feature extraction is implemented with serial pairs of convolution and pooling layers, and then classification between the original and tampered images is performed with and without transforms. A comparison study between different trigonometric transforms in 1D and 2D is presented for detecting the tampered parts in the image. This comparison study is based on the completeness rate for the detection. This comparison ensures that the DFT in 1D or 2D implementations is the best choice to detect copy-move forgery compared to other trigonometric transforms. In addition, the paper presents a comparison study between ten cases using the CNN learning technique to detect the manipulated image. The basic idea is to use a CNN to detect and extract features. The proposed CNN approach can also be used for active forgery detection because of its robustness to detect the manipulation of digital watermarked images or images with signatures.

Keywords Image forgery detection · Trigonometric transforms · Copy-move forgery · Multimedia security · Deep learning · CNN

1 Introduction

Nowadays, it is difficult to trust any image posted in any place like social media, Facebook [25], newspapers, and magazines, especially about famous characters like actors, singers, and even

✉ Fathi E. Abd. El-Samie
fathi_sayed@yahoo.com

Extended author information available on the last page of the article

politicians. This is attributed to the large spread of image tampering by any person, even non-experts. Manipulation of images has become a passion for many people. For this reason, it is a must to find methods to detect image manipulation. An efficient method among those methods is based on deep learning. Deep learning is a type of machine learning [28]. Deep learning presents a high performance in several applications such as medical image analysis [20, 30], intelligent IoT applications [29], big data analysis [12, 14] and speaker recognition [32].

There are many types of image forgery [23] like copy-move, splicing, and retouching. The foremost common type is the copy-move forgery, during which a part of the image is copied from some location within the image and pasted in a different location within the same image. This makes some items to disappear from the image or be duplicated with similar contrast, color, noise, or other features. This makes it difficult to notice such forgeries in contrast to the case of other types of forgery such as splicing and retouching. This paper presents a strong technique to detect copy-move forgery.

Copy–move forgery detection algorithms in [33] are divided into two basic types: block-based algorithm and key-point-based algorithm. In block-based algorithms, firstly, the image is divided into blocks, and then features are extracted from each block according to a certain method. After that, these feature representations from the original and the forgery pasted parts are compared.

In [7], the authors presented a copy-move forgery detection algorithm using DCT on fixed overlapping blocks to extract features as vectors, and then sort the feature vectors lexicographically to detect similar blocks. In the algorithm in [6], after dividing the image into blocks, features are extracted using Principal Component Analysis (PCA), which reduces the feature vectors size compared to that of the DCT. Unfortunately, this algorithm cannot detect rotation with copy-move forgery. In [18], the authors presented an algorithm for forgery detection based on the Discreet Wavelet Transform (DWT), and then applied the Singular Value Decomposition (SVD) on the low-frequency sub-band of the DWT. This algorithm is appropriate only for JPEG compressed images with quality levels up to 70. In [22], the authors used invariant moments to extract features on a block-by-block basis and used K-dimensional (KD) tree as a sorting tool to detect similar blocks.

The algorithm of expanding blocks in [21] depends on a direct block comparison instead of working on features. The image is split into overlapping blocks from which mean features are extracted. The blocks are sorted and classified into groups, and each group has similar features. The $A, A+1,$ and A-1 groups form a bucket. Blocks are compared with other blocks in the same bucket only. If a block does not match any other block in the bucket, this block will be canceled. Comparisons start with a small region, and blocks with no matches are canceled and so on.

In the key-point-based algorithms, the image is represented by a set of points acting as features of the image, and each point is called a key point, because it has specific magnitude and orientation that are different from those of the other points. The feature extraction and descriptor techniques of key-point-based algorithms can be divided into three types: Scale Invariant Feature Transform (SIFT), Harris corner detector, and Speeded Up Robust Features (SURF) algorithms. After that, the similar key points can be estimated. In [2], the authors used SIFT and DWT to detect copy-move parts in the tampered image. In [13], a set of key-point-based features called MIFT has been used for finding matched regions between the original and tampered images. In [19], the authors used Polar Harmonic Transform (PHT) to extract feature vectors from circular blocks to find the manipulated sections. In [35], to detect the matched parts, the authors used a specific threshold calculated based on the standard deviation of each block, and sorting is performed based on the thresholds.

This paper is organized as follows. Section 2 introduces the related traditional work for Copy-Move Forgery Detection (CMFD) using 2DDCT. Section 3 presents the proposed algorithm for CMFD using different trigonometric transforms (1D and 2D). Section 4 produces the formal trigonometric equations used in this algorithm. Section 5 produces the DWT formulation. Section 6 shows the proposed algorithm steps as a flowchart. Section 7 presents the results of forgery detection evaluated with completeness rate of detection. Section 8 presents deep learning results. Finally, Section 9 gives the conclusion of the paper.

2 Traditional algorithm for copy-move forgery detection based on 2D DCT

In [4], at first, the image is converted to a gray-scale image of dimensions ($U \times V$), and then divided into overlapping square blocks of fixed size with dimensions ($B \times B$), so that the number of image blocks (N_B) is equal to (U-(B-1)) × (V-(B-1)). After that, the 2DDCT is applied on each block, and each obtained coefficient block has the same size as that of the image block. The complexity and run time can be reduced by ignoring the outer values of the coefficient block and working only on the central circle of the block, which contains the most effective values. After that, the circle is divided to four parts; and each part is represented by a vector, so that each circle has four vectors $\{v_1, v_2, v_3, v_4\}$, and then each vector is converted to only one value by taking its mean. Hence, the circle will be converted to a vector of size (1 × 4) that represents the features of the block. In [4], all features of blocks can be represented in matrix form with dimensions (U-B + 1) (V-B + 1) × 4 in the form of:

$$\widehat{m_i b_j} = \begin{bmatrix} m_1 b_1 & m_2 b_1 & m_3 b_1 & m_4 b_1 \\ m_1 b_2 & m_2 b_2 & m_3 b_2 & m_4 b_2 \\ .. & .. & .. & .. \\ m_1 b_{(U-B+1)(V-B+1)} & m_2 b_{(U-B+1)(V-B+1)} & m_3 b_{(U-B+1)(V-B+1)} & m_4 b_{(U-B+1)(V-B+1)} \end{bmatrix} \tag{1}$$

The $\left(\widehat{m_i b_j}\right)$ is then lexicographically sorted. Since each row of $\left(\widehat{m_i b_j}\right)$ could be a vector, the sorted set is outlined as $\left(\widehat{m_i b_j}\right)$. Based on $\left(\widehat{m_i b_j}\right)$, the matching Euclidean distance between adjacent pairs of $\left(\widehat{m_i b_j}\right)$ is calculated. If the distance between adjacent circle features is smaller than a definite threshold ($\mathrm{Th}_{\mathrm{feature}}$), then we tend to initialize a black map P with size ($U \times V$) and take into account the inquired blocks as a pair of candidates for the forgery [4].

$$match\_feat = \sqrt{\sum\left(\widehat{m_i b_j} - \widehat{m_i b_{j+k}}\right)^2} < \mathrm{TH}_{\mathrm{feature}} \tag{2}$$

After detecting the similar pair blocks, the locations of the centeral pixels of the pair of blocks are used to calculate the space between blocks, and a certain threshold ($\mathrm{Th}_{\mathrm{distance}}$) is used to detect if the blocks are duplicated or not duplicated. Assume that (u, v) is the center of the circle [4].

$$dif\_dist = \sqrt{\left(u_j - u_{j+k}\right)^2 + \left(v_j - v_{j+k}\right)^2} > \mathrm{Th}_{\mathrm{distance}} \tag{3}$$

Equations (2) and (3) are used to determine the matched blocks.

3 Proposed forgery detection algorithms

3.1 Proposed forgery detection algorithms based on trigonometric transforms

In active forgery detection, there are additional information, such as digital watermarks or digital signatures, which are embedded into the transmitted image to guarantee authentication. If any tampering or manipulation occurs on the content of the transmitted image, this leads to changes in the additional information (digital watermarks or digital signatures). So, we offer an appropriate method to detect if there is similarity between the transmitted and received watermarked data or not.

This paper presents the traditional steps but with all trigonometric transforms in 1D and 2D and also with DWT. The objective is to select the best transform to detect the difference between the original image and the tampered one. The completeness rate is used for comparing between different transformation methods. The completeness rate is used as a measure of similarity between the detected regions and the tampered regions.

$$Completness(\%) = \frac{N_c}{N_f} \times 100 \tag{4}$$

where N_c is the number of the correctly detected tampered pixels, and N_f is the total number of tampered pixels.

For both the original and tampered images, we firstly divide both into overlapping blocks, and then apply the trigonometric transforms (2DDCT (traditional work), 1DDCT and DWT, 2DDCT and DWT, DST, DST and DWT, 1DDFT, 1DDFT and DWT, 2DDFT, 2DDFT and DWT) on each block.

After that, we extract features from each block, so that each image is represented with a feature matrix with dimensions ((*U-B* + 1) (*V-B* + 1) × 4). Then, we determine the difference in features and difference distance between the original and tampered images or between the transmitted watermarked image and the tampered one, (*dif _feat*) and (*dif _ dist*), respectively. We take the decision according the threshold as in Eqs. (5) and (6) as follows [4].

$$[m_b(i,j)] = \begin{bmatrix} m_b(1,1) & m_b(1,2) & m_b(1,3) & m_b(1,4) \\ m_b(2,1) & m_b(2,2) & m_b(2,3) & m_b(2,4) \\ \vdots & \vdots & \vdots & \vdots \\ m_b((U-B+1)\,(V-B+1),1) & m_b((U-B+1)\,(V-B+1),2) & m_b((U-B+1)\,(V-B+1),3) & m_b((U-B+1)\,(V-B+1),4) \end{bmatrix} \tag{5}$$

$$RSE = \sqrt{\sum_{i=1}^{4}\sum_{j=1}^{4}\left(m_{bo}(i,j) - m_{bt}(i,j)\right)^2} > T \tag{6}$$

3.2 Proposed algorithm based on deep learning

Another strategy adopted in this paper for forgery detection is based on deep learning. Deep learning is a type for machine learning in which a model learns to perform classification tasks directly from images. Deep learning is advantageous here due to the ability of multiple filters incorporated in the training process to extract discriminative features from the input images to better represent images with and without tampering. Features are learnt automatically by a CNN and presented to a classifier. The CNN includes the feature extractor in the training

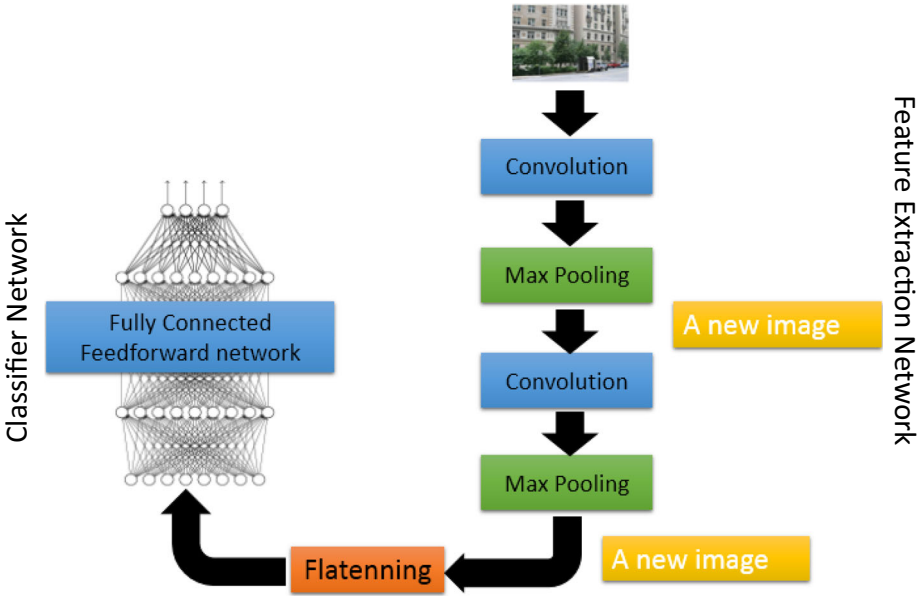


Fig. 1 The architecture of a CNN

process [24]. It consists of convolutional layers followed by an activation function, pooling layers, fully-connected layers and a classification layer. The inclusion of a dropout layer adopts a regularization technique for reducing over-fitting [17, 27, 31] (Fig. 1).

The input image enters the feature extraction network, which consists of sequential pairs of convolutional layer and pooling layer to produce a distinctive feature map. The features are involved in the classification process to produce the output of the deep neural network. Through the training stage, the weights of all layers are regulated using the back-propagation algorithm.

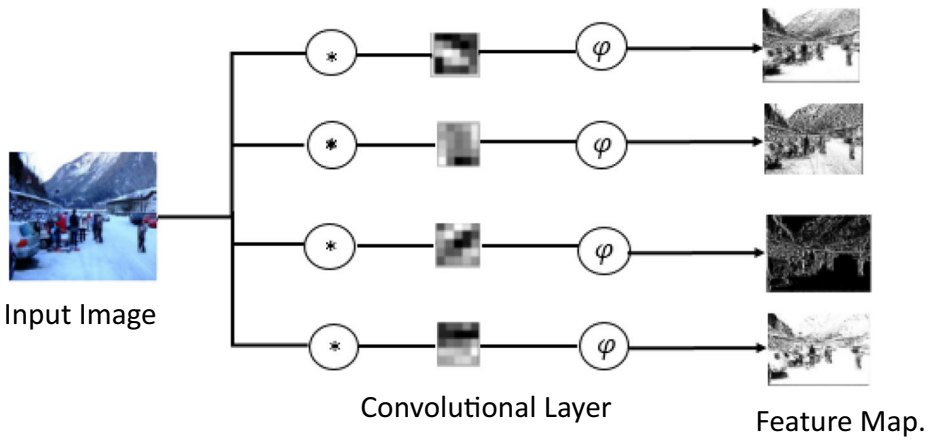


Fig. 2 The convolutional layer operation

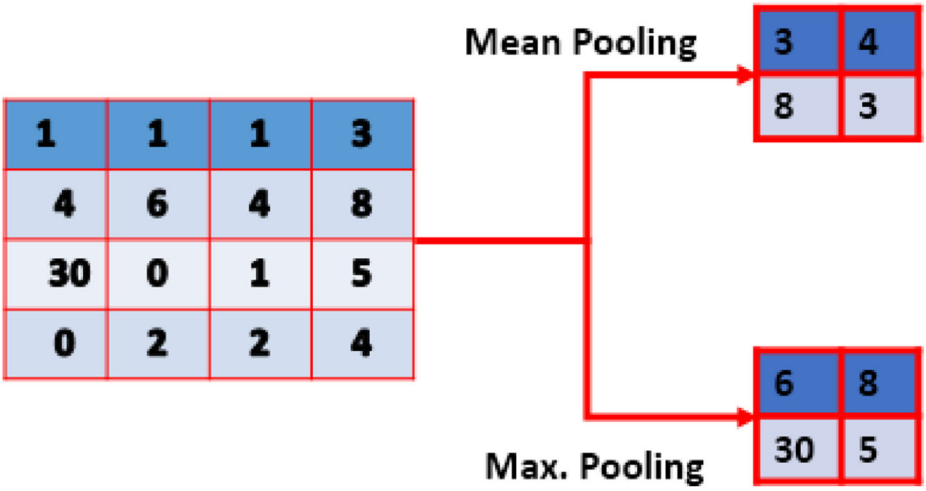


Fig. 3 Pooling using two different methods

3.2.1 Feature extractor network

It depends on serial sequential pairs of convolutional layer and pooling layer.

A. **Convolutional layer**

The convolutional layer consists of a combination of 2D digital filters, called convolution filters. The input image is convolved with the digital filters to generate the feature maps, which contain unique features of the original image. The number of feature maps is equivalent to the number of filters used. After each convolution process, there is an activation function. Fig. 2 presents the convolution layer process. For example, if the number of digital filters applied on

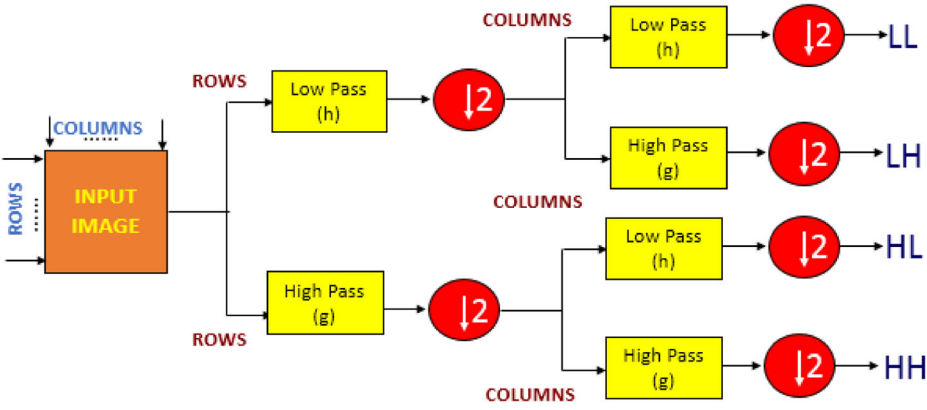


Fig. 4 One-level 2DDWT

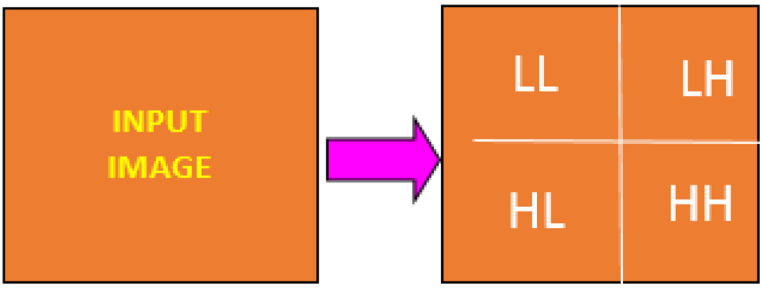


Fig. 5 One-level DWT on an image

the input image, with a depth of 3, is 16 filters, the depth of this image would be 16 instead of 3. The decrease of the weight and height of the input image occurs due to the pooling process.

The new value of a certain pixel p_{new} is the summation of the old surrounding pixels p multiplied by the applied filter elements w. It can be calculated as:

$$p_{new} = \sum_{i \in s} p_i . w_i \tag{7}$$

In the training phase, there is a need to use an activation function. An efficient one among the activation functions used in deep learning is the Rectified Linear Unit (ReLU) function. It allows faster and more effective training by mapping negative values to zero and maintaining positive values.

$$f(x) = \max(0, x) \tag{8}$$

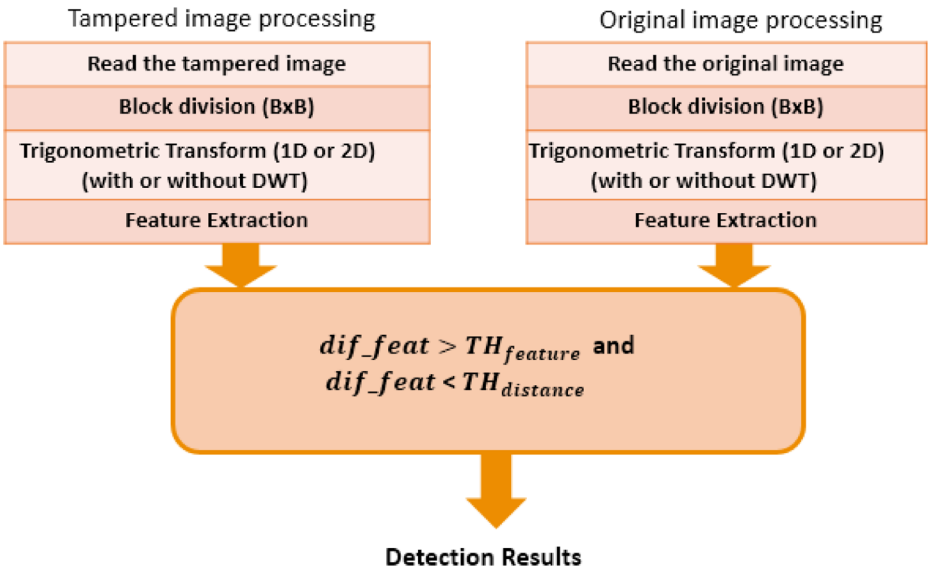


Fig. 6 Steps of the proposed algorithm based on feature matching

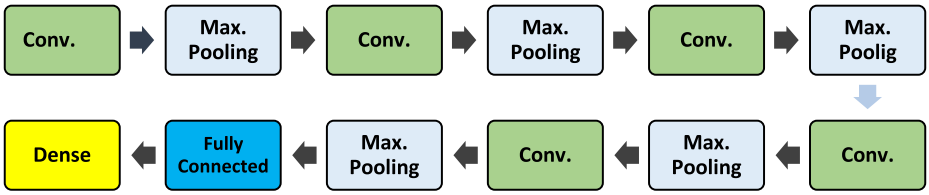


Fig. 7 Layers of the proposed deep learning model

B. **Pooling Layer**

The pooling layer is another type of feature extraction layers. The pooling layer decreases the size of the image. It combines neighboring pixels of a certain area of the input image into a single representative value. This value is the maximum or mean value of the pixels. Figure 3 shows both methods. The max-pooling layer is used in the proposed algorithm.

3.2.2 Classification network

It includes two layers: fully connected layer and classification layer.

A. **Fully-connected layer**

It is used to convert the data from a 2D image to a 1D vector. This layer does not involve any operation, it just connects between the output of the pooling layer and the input of the classification layer.

B. **Classification layer**

Table 1 Summery of the proposed deep learning model

Layer Type	Output Shape
Conv.	(222, 222, 16)
Pooling	(111, 111, 16)
Conv.	(109, 109, 32)
Pooling	(54, 54, 32)
Conv.	(52, 52, 64)
Pooling	(26, 26, 64)
Conv.	(24, 24, 128)
Pooling	(12, 12, 128)
Conv.	(10, 10, 256)
Pooling	(5, 5, 256)
Global Average Layer	(256)
Dense	(2)

Table 2 Description of the dataset used in the experiments

Dataset	MICC-F220
Number of the used images	220 images: 110 tampered and 110 original
Size of the used images	(532 × 800) pixels
Programs used for tampering of images	Photoshop 8.0
Software for applying the algorithm	Matlab R2014a
Image type and format	JPEG
Block size	(8 × 8) pixels
Number of blocks per image	(532–8 + 1) × (800–8 + 1) blocks

This is the final layer of the CNN that converts the output of the fully-connected layer to a probability of each image or object being in a certain class. Typically, soft-max type of algorithms is used in this layer to provide the classification output as follows.

$$P(y = j|\mathbf{x}) = \frac{e^{\mathbf{x}^T \mathbf{w}_j}}{\sum_{k=1}^{K} e^{\mathbf{x}^T \mathbf{w}_k}} \tag{9}$$

3.2.3 Back-propagation algorithm

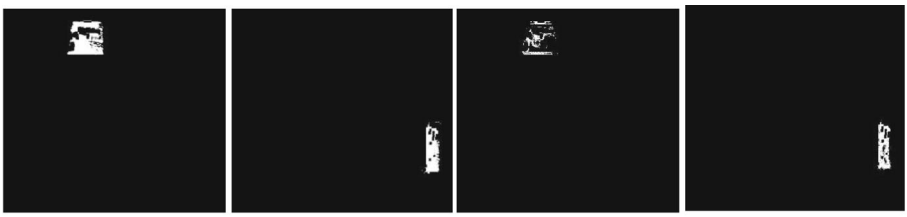
The main target of the training phase is to optimize the loss function to be as minimum as possible. The optimization process can be carried out by different algorithms for deep learning. In this work, Adam optimizer [16] is used to optimize the loss function. This function is cross-entropy. Using the alternative label convention $t = (1 + y)/2$, so that $t \in \{0, 1\}$, the cross-entropy loss is defined as:

$$V(f(x), t) = -t.ln(f(x)) - (1-t)\ln(1-f(x)) \tag{10}$$

The cross-entropy loss is closely related to the Kullback-Leibler divergence between the empirical distribution and the predicted distribution. This function is not naturally represented as a product of the true label and the predicted value, but it is convex and can be minimized using stochastic gradient descent methods. The cross-entropy loss is ubiquitous in modern deep neural networks.

(a1) (b1) (a2) (b2)

Fig. 8 Original (a1& a2) and tampered images (b1& b2)



(c1) (c2) (d1) (d2)

(e1) (e2) (f1) (f2)

(g1) (g2) (h1) (h2)

(i1) (i2) (j1) (j2)

(k1) (k2)

◀ **Fig. 9** Forgery detection results based on different transforms for the two images in Fig. 9 (c1) & (c2) 1DDCT and DWT, (d1) & (d2) 2DDCT (Traditional work), (e1) & (e2) 2DDCT and DWT, (f1) & (f2) DST, (g1) & (g2) DST and DWT, (h1) & (h2) 1DDFT (i1) & (i2) 1DDFT and DWT, (j1) & (j2) 2DDFT (k1) & (k2), 2DDFT and DWT

4 Trigonometric transforms

4.1 DFT formal definition

In [3, 9, 10, 34], there is a basic explanation of the DFT in one dimension and two dimensions.

The DFT transforms a sequence of N complex numbers $[x_0, x_1, \ldots..,x_{N-1}]$ into another sequence of complex numbers $[X_0, X_1, \ldots\ldots, X_{N-1}]$.

4.1.1 1D Discrete Fourier Transform

The 1DDFT is applied on the image column-by-column for each block of size ($N \times N$).

$$X_k = \sum_{n=0}^{N-1} x_n . \exp^{-i2\pi kn/N} \tag{11}$$

$$X_k = \sum_{n=0}^{N-1} x_n . [\cos(2\pi kn/N) - i . \sin(2\pi kn/N)] \tag{12}$$

4.1.2 2D Discrete Fourier Transform

The 2DDFT is applied on each block of size ($N_1 \times N_2$) pixels

$$X_{k_1,k_2} = \sum_{n_1=0}^{N_1-1} \left(w_{N_1}^{k_1,n_1} \sum_{n_2=0}^{N_2-1} w_{N_2}^{k_2,n_2} \cdot x_{n_1,n_2} \right) \tag{13}$$

where $w_{N_l} = \exp -2i\pi/N_l, n_l = 0, 1, \ldots.., N_l - 1$

Table 3 Completeness rate (%) for the two images with different scenarios

	Completeness rate %								
	1DDCT	2DDCT	2DDCT	DST	DST	1DDFT	1DDFT	2DDFT	2DDFT
With DWT	Yes	No	Yes	No	Yes	No	Yes	No	yes
Image#1	63.761	19.653	64.492	67.936	74.814	75.334	75.767	77.094	80.798
Image#2	67.572	52.104	66.276	69.161	75.627	76.672	76.686	83.765	84.629

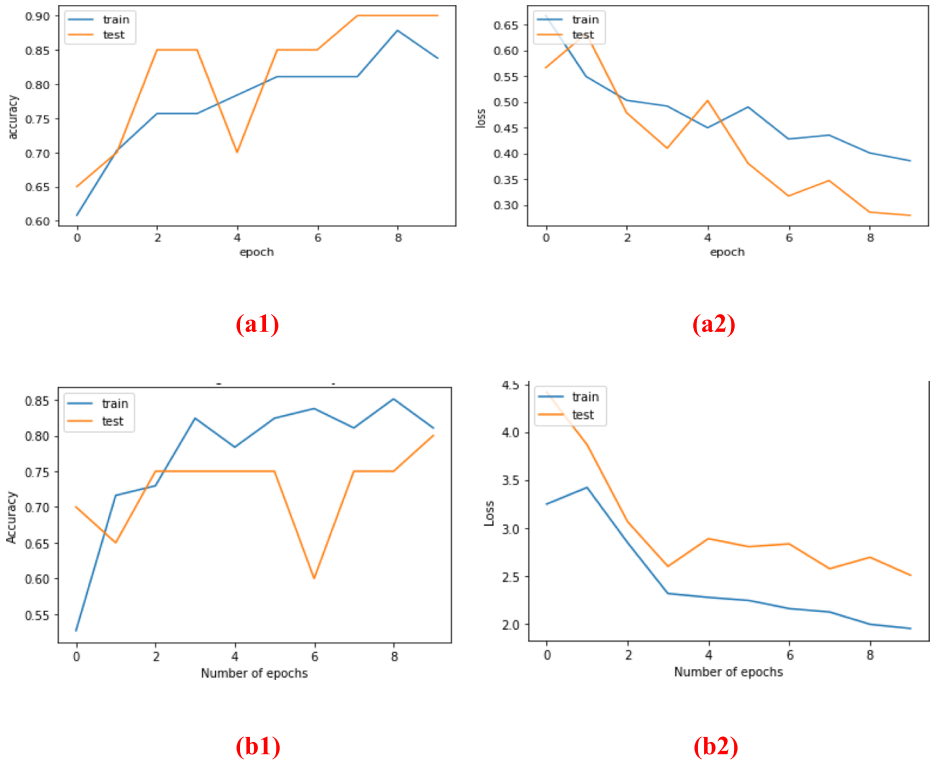


Fig. 10 Accuracy (in the left side) and loss (in the right side) of the different scenarios of forgery detection with CNN, (a1) & (a2) 1DDCT and DWT, (b1) & (b2) 2DDCT, (c1) & (c2) 2DDCT and DWT, (d1) & (d2) DST, (e1) & (e2) DST and DWT, (f1) & (f2) 1DDFT, (g1) & (g2) 1DDFT and DWT, (h1) & (h2) 2DDFT, (i1) & (i2) 2DDFT and DWT, and (j1) & (j2) no transform

4.2 Discrete Cosine Transform

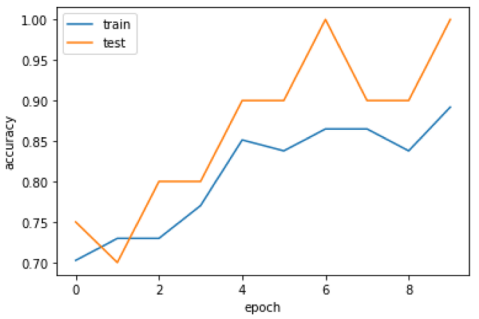
In [10], the DCT is defined as a real, linear, and invertible transform. The N real numbers [x_0, x_1, ….., $x_{N\text{-}1}$] are transformed into the N real numbers [X_0, X_1,……, $X_{N\text{-}1}$].

4.2.1 1D Discrete Cosine Transform

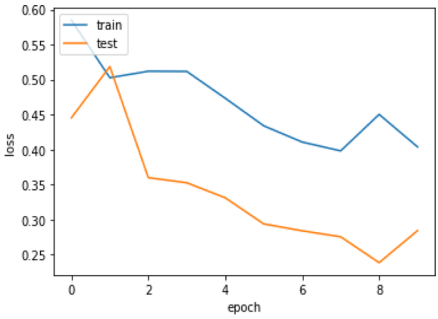
$$X_k = \sum_{n=0}^{N-1} x_n \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right] \quad ,k = 0,\ldots,N-1. \tag{14}$$

4.2.2 2D Discrete Cosine Transform

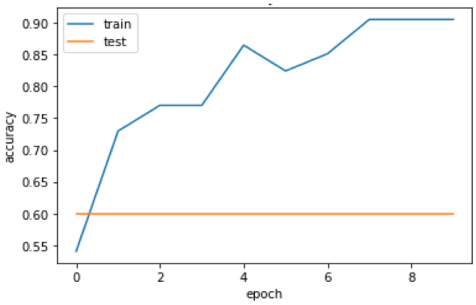
$$X_{k_1,k_2} = \sum_{n_1=0}^{N_1-1}\left(\sum_{n_2=0}^{N_2-1} x_{n_1,n_2}\cos\left[\frac{\pi}{N_2}\left(n_2+\frac{1}{2}\right)k_2\right]\right)\cos\left[\frac{\pi}{N_2}\left(n_1+\frac{1}{2}\right)k_1\right] \tag{15}$$

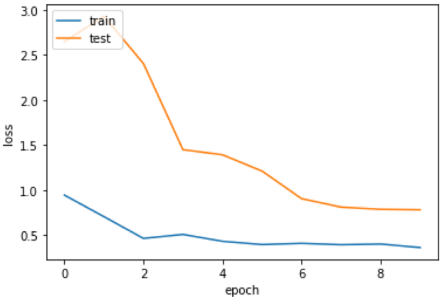


(c1)



(c2)





(d1)

(d2)

Fig. 10 (continued)

4.3 Discrete Sine Transform

The DST is another real, linear, and invertible transform. Its formula is given by:

$$X_k = \sum_{n=0}^{N-1} x_n \sin\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)(k+1)\right] \quad k = 0, \ldots, N-1. \tag{16}$$

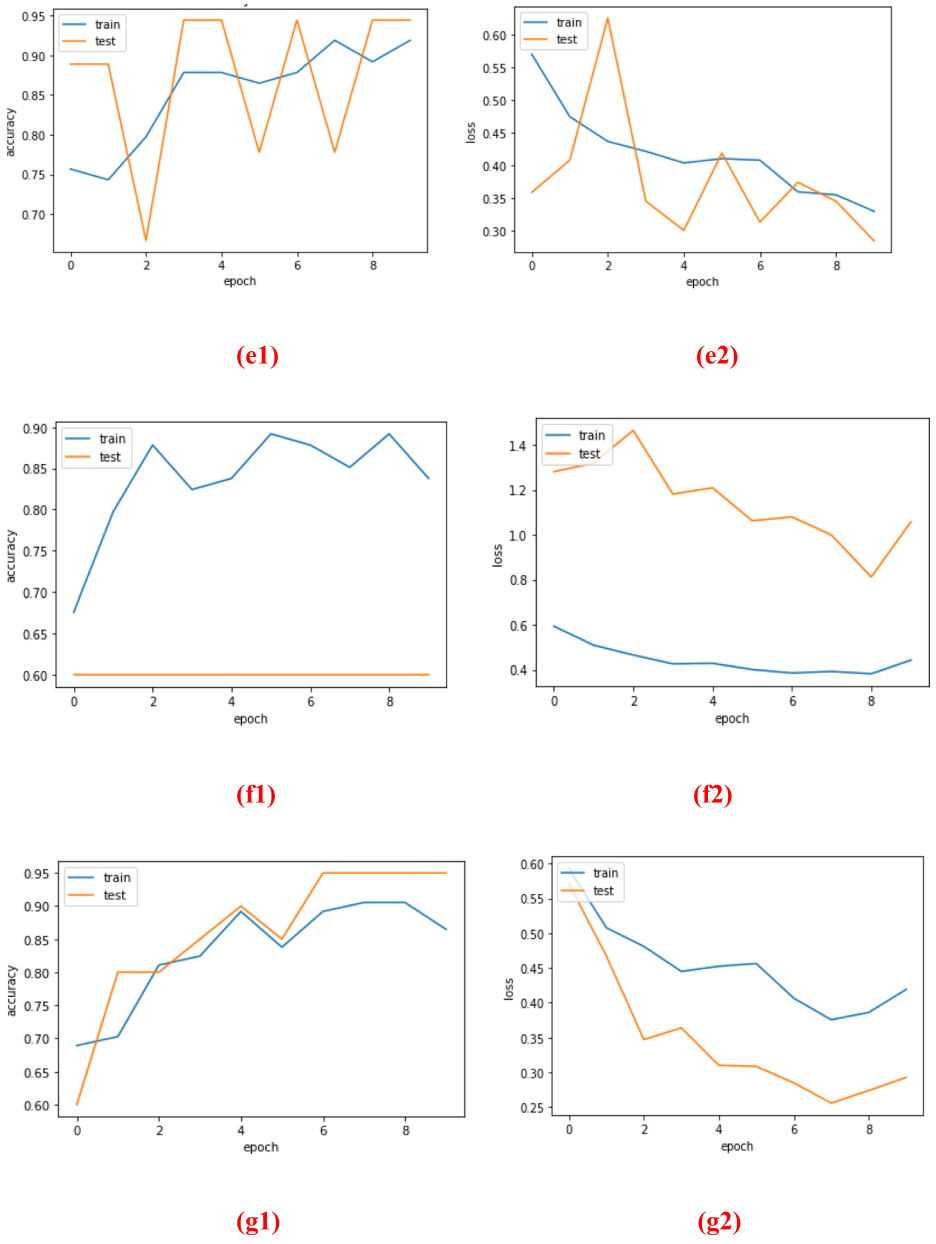


Fig. 10 (continued)

5 Discrete Wavelet Transform

In [1, 8], the authors applied a one-level 1DDWT on the rows, and then on the columns of the image as shown in Fig. 4.This leads to four distinct bands: LL, LH, HL and HH. Here, L

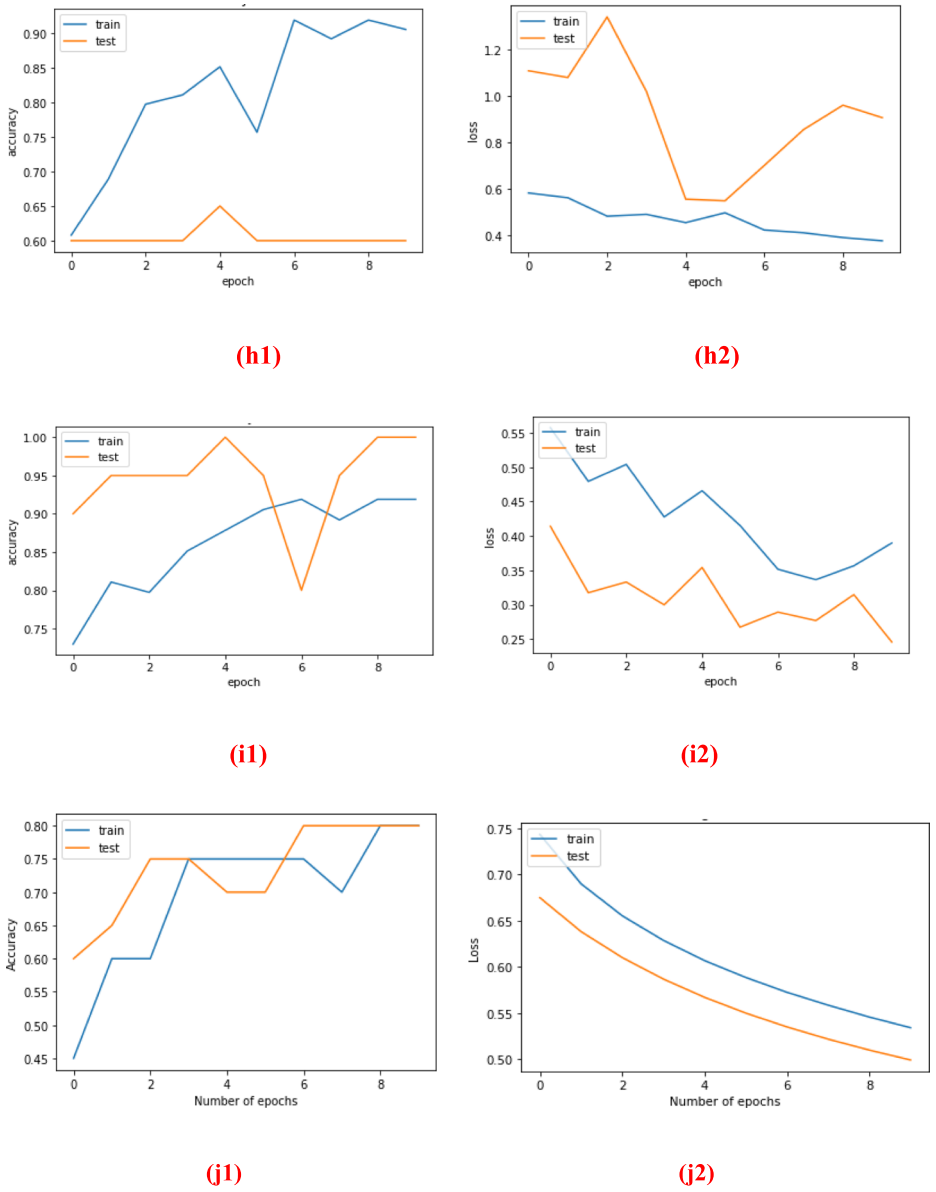


Fig. 10 (continued)

stands for low-pass filtering, and H stands for high-pass filtering. The LL band corresponds roughly to a down-sampled (by a factor of two) version of the original image. The LH band tends to preserve localized horizontal features, whereas the HL band tends to preserve localized vertical features within the original image. Finally, the HH band tends to isolate localized high-frequency point features within the image.

Table 4 Accuracy of all forgery detection scenarios with CNN

Type of transform to generate the input of the CNN	Accuracy %
1DDCT & DWT	90%
2DDCT	80%
2DDCT & DWT	100%
DST	60%
DST & DWT	94.4%
1DDFT	60%
1DDFT & DWT	95%
2DDFT	60%
2DDFT & DWT	100%
No transform	80%

The work in this paper adopts Haar wavelet with $\psi_{Haar}(x)$ and $\varphi_{Haar}(x)$ as a high-pass filter and a low-pass filter, respectively [3].

$$\psi_{Haar}(x) = \begin{cases} 1 & 0 < x < 0.5 \\ -1 & 0.5 < x < 1 \\ 0 & Otherwise \end{cases} \tag{17}$$

$$\varphi_{Haar}(x) = \begin{cases} 1 & 0 < x < 1 \\ 0 & Otherwise \end{cases} \tag{18}$$

For each block, the Haar wavelet transform is used to extract the four bands (LL, LH, HL, HH) and get a new block as in Fig. 5 with the same size as the original block, but with the Haar wavelet components as elements. Trigonometric transforms are applied after that.

6 Steps of the proposed algorithms

6.1 Proposed algorithm based on feature matching

This algorithm is mainly composed of extracting two groups of features from the original and tampered images, and then taking the difference between them to be compared with an absolute threshold. The steps of this algorithm are illustrated in Fig. 6. The main advantage of this detection algorithm is the small feature vector, where a block of size (8 × 8) is represented by a 1 × 4 feature vector, compared with the feature vectors in [11, 15, 26], which are of sizes (1 × 64), (1 × 16), and (1 × 32), respectively.

6.2 Proposed algorithm based on deep learning

The forgery detection algorithm presented in this paper based on deep learning can achieve high performance with considerably low computational cost. It is based on the architecture of the CNN displayed in Fig. 7. Table 1 shows a summary of the layers of the proposed CNN architecture.

The proposed forgery detection algorithm depends on three phases: the pre-processing phase, the feature extraction phase, and the classification phase. In the data pre-processing phase, a trigonometric transform is carried out on the input images, and then they are resized to a unified size

specified in the input layer. The feature extraction stage consists of a set of layers that encloses neurons arranged in 4 dimensions: the number of samples, the width and height of the input image, as well as the number of filters used in each CNN layer.

In the proposed algorithm, the feature extraction stage consists of a series of three CNN layers, each followed by a max-pooling layer. After these layers, a Global Average Pooling (GAP) layer exists, and after that the fully-connected layer. Finally, a dense layer deciding between two classes (original or tampered) is used for the classification phase. CNN layers act as feature extractors, where each CNN layer applies its specific filters and produces its feature maps. Beginning by the feature maps produced from the first CNN layer, the following max-pooling layer produces resized pooled feature maps, which act as input to the next CNN layer. The final pooled feature maps of the last max-pooling layer are formulated as vectors and inserted into the GAP layer.

7 Experiments and discussions

7.1 Dataset

The proposed algorithms have been carried out on MICC-F220 dataset [5]. Table 2 gives a description of this dataset. It is composed by 220 images: 110 tampered and 110 original. Images have a size of (532 × 800) pixels. We used Photoshop 8.0 for tampering of the images. The software used to apply the proposed algorithms is Matlab R2014a, where the image is read and converted to a gray-scale image, and then the remaining steps of the algorithm are applied. The image is divided into overlapping blocks each with (8 × 8) pixels, so that the total number of blocks is (532–8 + 1) × (800–8 + 1) =416.325 × 10^3 blocks, and this small block size enables us to detect small tampered objects. The statistical properties used are the mean, where each block is divided into four parts, and then we take the mean of each part.

7.2 Experimental results and analysis

The obtained results are presented in the next figures and tables. In Fig. 8, two original images and their tampered versions are presented. Figure 9 gives the detection results in all scenarios with different transforms. Table 3 presents the completeness rate (%) for all detection scenarios.

Figure 9 illustrates the detection results obtained with black and white images, where the black parts represent the matched parts between the original and tampered images and the white parts represent the difference between the two images. From these black-and-white detection images for all the transforms in 1D and 2D, we can observe that the frame edges of the cut region are all approximately detected using 2DDFT and 2DDFT with DWT. From Table 3, we can easily observe that the best detection results can be obtained from 2DDFT with DWT, where the completeness rate reaches 80% and 85% for image#1 and image#2, respectively.

8 Deep learning results

Simulation experiments of the scenarios based on deep learning have been performed on MICC-F220 dataset using python 3.5 (https://www.python.org/downloads/release/python-350/), Tensorflow [36] and Keras [37]. Figures 10 shows the accuracy and loss for training and testing phases along the epochs for each scenario. Ten epochs and a batch size of 10 have

been considered in the training process. Table 1 summarizes the accuracy of each scenario. From all obtained results, it can be observed that feeding the 2DDCT with DWT and 2DDFT with DWT outputs to the CNN achieves an accuracy of 100%. So, the dependence on the CNN gives a breakthrough in the forgery detection performance.

From Table 4, we can clearly observe that the addition of the DWT before the trigonometric transforms leads to an enhancement of the forgery detection accuracy. The accuracy of forgery detection with 2DDCT only is (80%), with 2DDFT only is (60%), and with DWT prior to these two transforms reaches (100%).

9 Conclusions

This paper presented two algorithms for detecting the copied or pasted parts in tampered images based on 1D and 2D trigonometric transforms. These algorithms depend on feature matching and deep learning. Simulation results have shown good robustness of the proposed feature-matching based forgery detection algorithm that is based on 2DDFT and DWT. Different metrics have been evaluated in the comparison between the feature-based algorithms such as the completeness rate. The completeness rate results of forgery detection are maximal with the 2DDFT and DWT. In addition, deep learning has been used with the forgery detection scenarios to enhance the detection performance. The accuracy with deep learning reached 100%, in two different scenarios, which reflects the feasibility of image forgery detection based on discrete transforms and deep learning.

References

1. Acharya T, Chakrabarti C (2006) A survey on lifting-based discrete wavelet transform architectures. Journal of VLSI Signal Processing Systems for Signal, Image and Video Technology 42:321–339
2. Amerini I, Serra G, Del Bimbo A, Caldelli R, Ballan L (2011) A sift-based forensic method for copy–move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security 6: 1099–1110
3. Amolins K, Dare P, Zhang Y (2007) Wavelet based image fusion techniques—an introduction, review and comparison. ISPRS J Photogramm Remote Sens 62:249–263
4. Cao Y, Yang Q, Fan L, Gao T (2012) A robust detection algorithm for copy-move forgery in digital images. Forensic Sci Int 214:33–43
5. Dang-Nguyen DT, Boato G, Conotter V, Pasquini C (2015) RAISE: a raw images dataset for digital image forensics. In Proceedings of the 6th ACM multimedia systems conference, pp. 219–224
6. Farid H, Popescu A (2004) Exposing digital forgeries by detecting duplicated image regions. Department Computer Science, Dartmouth College, Technology Report TR2004–515
7. Fridrich AJ, Lukáš AJ, Soukal BD (2003) Detection of copy-move forgery in digital images. In Proceedings of digital forensic research workshop
8. Fridrich A et al (2003) Detection of copy-move forgery in digital images
9. Graps A (1995) An introduction to wavelets. IEEE Comput Sci Eng 2:50–61
10. Hafed ZM, Levine MD (2001) Face recognition using the discrete cosine transform. Int J Comput Vis 43: 167–188
11. Huang Y, Long D, Sun W, Lu W (2011) Improved DCT-based detection of copy-move forgery in images. Forensic Sci Int 206:178–184
12. Huh J-H (2018) Big data analysis for personalized health activities: machine learning processing for automatic keyword extraction approach. Symmetry 10(4):93
13. Jaberi M, Muhammad G, Hussain M, Bebis G (2014) Accurate and robust localization of duplicated region in copy–move image forgery. Mach Vis Appl 25:451–475
14. Jung S-H, Huh J-H (2019) A novel on transmission line tower big data analysis model using altered K-means and ADQL. Sustainability 11(13):3499
15. Kim P (2017) Matlab deep learning. With Machine Learning, Neural Networks and Artificial Intelligence

16. Kingma DP, Ba J (2014) Adam: a method for stochastic optimization. arXiv preprint arXiv:1412.6980
17. LeCun Y, Bottou L, Bengio Y, Haffner P (1998) Gradient-based learning applied to document recognition. Proc IEEE 86(11):2278–2324
18. Li G, Wu Q, Sun S, Tu D (2007) A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. In Multimedia and expo, 2007 IEEE international conference on, pp. 1750–1753
19. Li L, Wu X, Zhu H, Li S (2014) Detecting copy-move forgery under affine transforms for image forensics. Comput Electr Eng 40:1951–1962
20. Litjens G et al (2017) A survey on deep learning in medical image analysis. Med Image Anal 42:60–88
21. Lynch G, Liao H-YM, Shih FY (2013) An efficient expanding block algorithm for image copy-move forgery detection. Inf Sci 239:253–265
22. Mahdian B, Saic S (2007) Detection of copy–move forgery using a method based on blur moment invariants. Forensic Sci Int 171:180–189
23. Nath V, Gaharwar R, Gaharwar G (2015) Comprehensive study of different types image forgeries. International Conference of Recent Advances Engineering Science and Management, New Delhi
24. Nishanth K, Karthik G (2015) Identification of diabetic maculopathy stages using fundus images. J Mol Image Dynamic
25. Patil SS, Khade BS, Dhongde JD, Patil NP, Patil AN (2014) Digital image forgery detection using basic manipulations in Facebook. Int J Sci Technol Res 3:356–359
26. Popescu A, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions, Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004–515
27. Ranzato MA, Huang FJ, Boureau YL, LeCun Y (2007). Unsupervised learning of invariant feature hierarchies with applications to object recognition. In Computer vision and pattern recognition, 2007. CVPR'07. IEEE conference on (pp. 1–8). IEEE.
28. Schmidhuber J (2015) Deep learning in neural networks: An overview. Neural Netw 61:85–117
29. Seo Y-S, Huh J-H (2019) Automatic emotion-based music classification for supporting intelligent IoT applications. Electronics 8(2):164
30. Shen D, Wu G, Suk H-I (2017) Deep learning in medical image analysis. Annu Rev Biomed Eng 19:221–248
31. Srivastava N, Hinton G, Krizhevsky A, Sutskever I, Salakhutdinov R (2014) Dropout: a simple way to prevent neural networks from overfitting. The Journal of Machine Learning Research 15(1):1929–1958
32. Wang Z-Q, Tan K, Wang D (2019) Deep learning based phase reconstruction for speaker separation: a trigonometric perspective. In: ICASSP 2019–2019 IEEE international conference on acoustics, speech and signal processing (ICASSP). IEEE, p. 71–75
33. Warif NBA, Choo KKR, Wahab AWA, Shamshirband S, Ramli R, Salleh R, Idris MYI (2016) Copy-move forgery detection: survey, challenges and future directions. J Netw Comput Appl 75:259–278
34. Winograd S (1978) On computing the discrete Fourier transform. Math Comput:175–199
35. Zandi M, Mansouri A, Mahmoudi-Aznaveh A (2014) Adaptive matching for copy-move forgery detection. In Information forensics and security (WIFS), 2014 IEEE international workshop on, pp. 119–124

Faten Maher Al_azrak , received the B.Sc. (Honors) from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2013. She works as demonstrator at the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2013. Her research areas of interest are image processing, and digital communications.

Ahmed Sedik received B.sc and M.Sc. of engineering, Faculty of Engineering, Tanta University, Egypt in 2012 and 2018 respectively. He is a teaching assistant at the faculty of Artificial intelligence, Kafrelsheikh University. He is working towards the Ph.D. degree from the Faculty of Engineering, Minia University, Egypt.

Moawad I. Dessowky , received the B.Sc. (Honors) and M.Sc. degrees from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1976 and 1981, respectively, and the Ph.D. from McMaster University, Canada, in 1986. He joined the teaching staff of the Department of Electronics and Electrical Communication Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1986. He has published more than 200 scientific papers in national and international conference proceedings and journals. He is currently a Professor Emeritus at the Faculty of Electronic Engineering, Menoufia University. He has received the most cited paper award from Digital Signal Processing journal for 2008. His current research areas of interest include spectral estimation techniques, image enhancement, image restoration, super resolution reconstruction of images, satellite communications, and optical communications.

Ghada M. El Banby received the M.Sc. and Ph.D. degrees in Automatic Control Engineering from Menoufia University, Egypt in 2006, and 2012, respectively. She works as an associate professor at the Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University. Her current research interests include computer vision, data fusion, systems, image processing, signal processing, medical imaging, modeling, and control systems.

Ashraf A. M. Khalaf (PhD) received his B. Sc. and M.Sc. degrees in electrical engineering from Minia University, Egypt, in 1989 and 1994 respectively. He received his Ph.D in electrical engineering from Graduate School of Natural Science and Technology, Kanazawa University, Japan, in March 2000. He is currently working as an associate professor at electronics and communications engineering department, Minia University, Egypt. His current research areas of interest include adaptive systems, filtering, signal and image processing, neural networks, deep learning, biomedical signal processing, and optical communications.

Ahmed S. Elkorany , received the B.Sc. degree in electronics and electrical communications (with honor degree) in May 2003 from Faculty of Electronic Engineering, Menoufia University. He was appointed as a Demonstrator in Dec. 2003 in the same department. He received the M.Sc. and the Ph.D. in electrical communications (microwaves and antennas) in 2007 and 2011, respectively, both from the same faculty. In Dec. 2011, he was appointed as a Lecturer also in the same dept. Finally, in 2018, he was appointed as an associate professor in the same dept. His research is focused on numerical techniques, CAD tools, programming languages, UWB antennas and systems, EBG structures, image processing, mobile communications and cognitive radio.

Fathi E. Abd. El-Samie , received the B.Sc. (Honors), M.Sc., and PhD. from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2005. He has received the most cited paper award from Digital Signal Processing journal for 2008. His current research areas of interest include image enhancement, image restoration, image interpolation, superresolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications.

Affiliations

Faten Maher Al_Azrak [1] · Ahmed Sedik [2] · Moawad I. Dessowky [1] · Ghada M. El Banby [3] · Ashraf A. M. Khalaf [4] · Ahmed S. Elkorany [1] · Fathi E. Abd. El-Samie [1]

Faten Maher Al_Azrak
Eng_fatenmaher@yahoo.com

Ahmed Sedik
ahmedsedik93@gmail.com

Moawad I. Dessowky
dr_moawad@yahoo.com

Ghada M. El Banby
ghada.elbanby@el-eng.menofia.edu.eg

Ashraf A. M. Khalaf
ashkhalaf@yahoo.com

Ahmed S. Elkorany
elkoranyahmed@yahoo.com

[1] Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[2] Department of the Robotics and Inteligent Machines, Faculty of Artificial Inteligence, Kafrelsheikh University, Kafrelsheikh, Egypt

[3] Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[4] Department of Electrical Engineering, Electronics and Communications Engineering, Faculty of Engineering, Minia University, Minia 61111, Egypt