Indonesian Journal of Electrical Engineering and Computer Science
Vol. 22, No. 2, May 2021, pp. 1177~1190
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i2.pp1177-1190

A comparative analysis of image copy-move forgery detection algorithms based on hand and machine-crafted features

Ismail Taha Ahmed[1], Baraa Tareq Hammad[2], Norziana Jamil[3]
[1,2]College of Computer Sciences and Information Technology, University of Anbar, Anbar, Iraq
[3]College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia

Article Info

Article history:

Received Jan 9, 2021
Revised Mar 22, 2021
Accepted Apr 11, 2021

Keywords:

Deep leaning methods
Digital Image forgery
Hand-crafted features
Image copy-move forgery detection algorithms
Machine-crafted features

ABSTRACT

Digital image forgery (DIF) is the act of deliberate alteration of an image to change the details transmitted by it. The manipulation may either add, delete or alter any of the image features or contents, without leaving any hint of the change induced. In general, copy-move forgery, also referred to as replication, is the most common of the various kinds of passive image forgery techniques. In the copy-move forgery, the basic process is copy/paste from one area to another in the same image. Over the past few decades various image copy-move forgery detection (IC-MFDs) surveys have been existed. However, these surveys are not covered for both IC-MFD algorithms based hand-crafted features and IC-MFDs algorithms based machine-crafted features. Therefore, The paper presented a comparative analysis of IC-MFDs by collect various types of IC-MFDs and group them rely on their features used. Two groups, i.e. IC-MFDs based hand-crafted features and IC-MFDs based machine-crafted features. IC-MFD algorithms based hand-crafted features are the algorithms that detect the faked image depending on manual feature extraction while IC-MFD algorithms based machine-crafted features are the algorithms that detect the faked image automatically from image. Our hope that this presented analysis will to keep up-to-date the researchers in the field of IC-MFD.

Corresponding Author:

Ismail Taha Ahmed
College of Computer Sciences and Information Technology
University of Anbar, Anbar, Iraq
Anbar, Iraq
Email: ismail.taha@ uoanbar.edu.iq

1. INTRODUCTION

Images play an important role as effective carriers of information in technology. Through using various advanced imaging devices like smartphones, huge amount of high-resolution digital images are taken and exchanged through people daily. The images are influenced by various kinds of manipulations that may not be easily identified. The manipulation may either add, delete or alter any of the properties of the image, without offering any hint as to the update. The original and forgery image are shown in Figure 1.

Methods for the detection of forgery images are classified into two groups, active and passive. The active methods are closely associated with information that belongs to the original image such as watermarking or steganographic data. However, the absence of this information can limit active methods applications. Therefore, to assess its authenticity, passive methods may not depend on previous details concerning the original image.

Passive image forgery detection can be narrowly divided into a few categories such as copy-move, resampling, and camera source identification. A copy-move forgery is one of the essential ways of passive

forgery detection where it has been copied and pasted into the same image in one or more regions. Copy-move forgery is easily can be executed and reasonably successful in manipulating images, especially when the properties of the source and target regions are of the same image are normally well-matched between the region and the image being manipulated. Figure 2 shows the original and copy-move image forgery.

(a) (b)

Figure 1. (a) Original image, (b) forgery image

(a) (b)

Figure 2. (a) Original image, (b) copy-move image forgery [1]

There are some literature surveys about IC-MFDs. In [2], A survey was presented on recent developments in CMFD and explains the whole process involved in CMFD. In [3], a brief review on passive digital image forensic approaches is discussed. Various types of traces for passive digital image forensics: traces left in image acquisition, traces left in image storage, and traces left in image editing. In [4], a literature review of digital image forensics, covering active and passive methods as well as relevant discussions regarding deep learning. In [5], the survey covers different forgery detection techniques, different types of feature-matching methods. In [6], a survey was presented a state of the art on keypoint based copy-move forgery detection. In [7], a survey was presented on the innovative experiments in the forgery recognition tactics built on the likeness and connection between the pasted part and the real image and their comparative study. In [8], a survey was presented on various kinds of digital image forgeries detection methods, this survey focusing on the current methods for forged image. In [9], short review of CMFD demonstrate that the work is still state of art and there is plenty of room for future study. In [10], a state-of-the-art review and analysis of recent CMFD techniques are presented. In [11], a survey offers an overview of common forms of image tampering, published datasets of image tampering and recent approaches to detect tampering. In [12], A research on recent developments in CMFD methods was presented to identify factors that hinder the detection of forgery and evaluate the accuracy of various methods proposed. However, they did not provides an extensive review of major IC-MFD algorithms developed for (1) hand-crafted features, (2) machine-crafted features. So they did not cover both of them. Therefore, the paper presented a comprehensive review of IC-MFD algorithms by collect various types of IC-MFD algorithms and group them according to their features used. Two groups, i.e. IC-MFD algorithms based hand-crafted features and IC-MFD algorithms based machine-crafted features. IC-MFD algorithms based hand-crafted features are the algorithms that detect the faked image depending on manual feature extraction while IC-MFD algorithms based machine-crafted features are the algorithms that detect the faked image automatically from image. Our hope that this presented survey will to keep up-to-date the researchers in the field of IC-MFD. The remainder of this paper is formulated as follows. In Section 2, classify the current IC-MFD Algorithms and group them

according to their features used. In Section 3, IC-MFD Algorithms based hand-crafted features are presented. In Section 4, IC-MFD Algorithms Based Machine- Crafted Features are presented. Finally, in Section 5, conclusions can be drawn.

2. EXISTING IC-MFD ALGORITHMS (IC-MFDs)

Many IC-MFD techniques are based on different types of features which are available in different domains. Such as many features that can be extracted in the spatial or transform domain. Generally speaking, the characteristics extracted in the spatial domain are relatively low in complexity, whereas those extracted in the transform domain better represent the multiscale and multi orientation characteristics of HVS; a fair combination of different features will effectively improve efficiency. Copy-move is the most widely used image tampering technique that attempts to keep hiding or modify the image content. Figure 3 shows the general taxonomy of image forgery detection techniques. Most conventional IC-MFDs depend on four stages such as: pre-processing (optional), feature extraction, matching and visualization (optional).

Here, collect various types of IC-MFDs algorithms and group them according to their features used. Two groups, i.e. IC-MFDs algorithms based hand-crafted features and IC-MFDs algorithms based non-hand crafted features. Most Conventional IC-MFDs algorithms rely on the extraction of certain features to differentiate the original image from the fake one. While IC-MFDs based deep learning, feature extraction and matching integrated into one optimization step as shown in Figure 4.

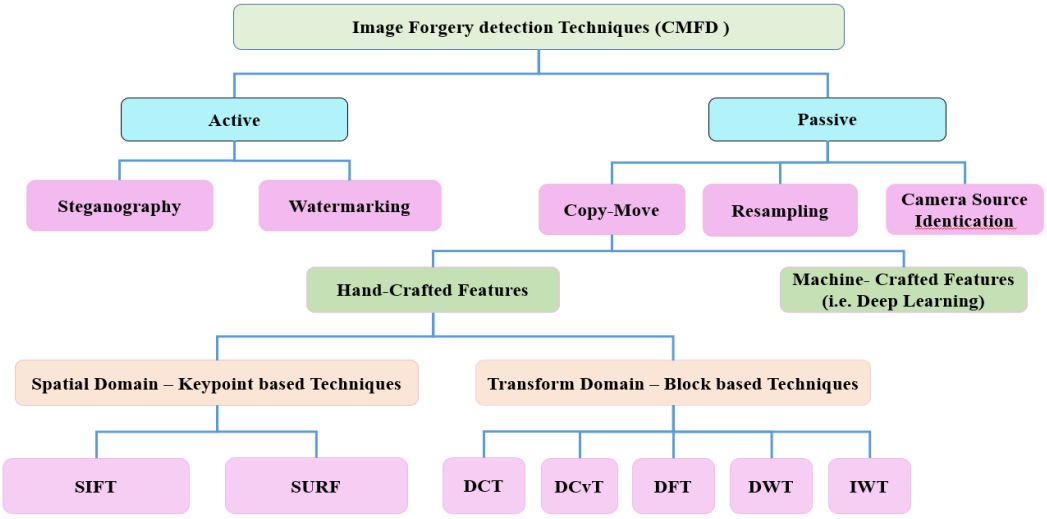

Figure 3. Image forgery detection techniques taxonomy

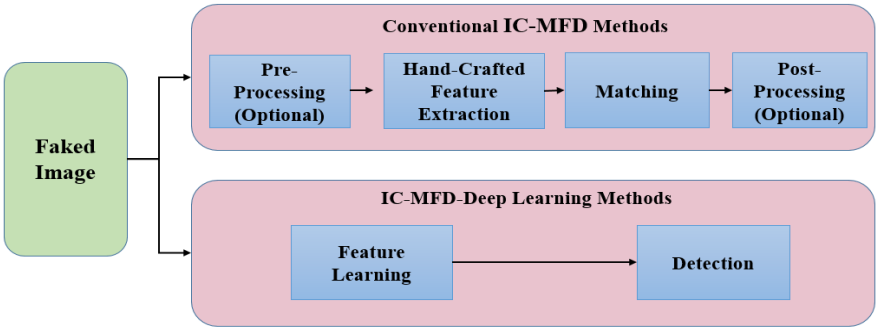

Figure 4. General architecture of image forgery detection techniques

2.1. Existing publicly databases

In order to validate the results of different image CMFD algorithms, different public image databases are used to test the performance of these algorithms. Table 1 provides information on these databases.

Table 1. Existing publically available image copy-move forgery datasets

Dataset	Year	Total Images No	Authentic Images No.	Tampered Images No.	Post-Processing Operations	Image Format	Resolution
MICC-F220 [13]	2011	220	110	110	No	JPEG	722×480 to 800×600
IMD [14]	2012	-	48	87	4	JPEG	1632 x 1224
MICC-F600 [15]	2013	600	440	160	yes	JPEG/ PNG	800×532 to 3888×2592
CoMoFoD [16]	2013	-	5200	5200	6	JPEG/ PNG	512 x 512
CASIA v1.0 [17]	2013	1721	800	921	No	JPEG	384×256
CASIA v2.0 [17]	2013	12614	7491	5123	yes	JPEG/ TIFF	240 × 160 - 900 × 600
MICC-F2000 [18]	2014	2000	1300	700	No	JPEG	2048x 1536
GRIP [19]	2015	80	80	-	6	-	768 ×1024
COVERAGE[20]	2016	-	100	-	No	TIFF	Various

2.2. Performance evaluation

CMFD evaluation at image level is performed after the images of the datasets are classified into two groups: faked and original. There is two metrics: true positive rate (TPR) and false positive rate (FPR) are used to evaluate the performance of different CMFD method. Typically these metrics are used to measure the accuracy. A successful detection method must establish a high TPR while a minimum FPR level should remain. Both the TPR and FPR equations are described in (2) and (3).

$$Accurcy = \frac{(TP+TN)}{(TP+TN+FN+FP)} \quad (1)$$

$$T_{PR} = \frac{TP}{(TP+FN)} \quad (2)$$

$$T_{NR} = \frac{TN}{(TN+FP)} \quad (3)$$

Where the number of forged images identified as forged is true positive (TP); the number of forged images identified as authentic is false negative (FN); the number of authentic images identified as authentic is true negative (TN); and the number of authentic images identified as forged ones is false positive (FP). TPR is the number of manipulated images correctly detected, and FPR refers to the percentage of the original images that are wrongly reported as manipulated.

3. IC-MFD ALGORITHMS BASED HAND-CRAFTED FEATURES

The IC-MFD approach is applied to detect the forgery image rely on the extracted features which are related to forgery detection. For an image, it is possible to capture the features either globally for the entire image or locally for regions or objects. Selecting good features can have a powerful impact on forgery image detection.

CMFD methods can be classified into three groups in terms of image dividing: block-based approaches [21], segmented region-based approaches [22], and local keypoint-based approaches [23]. In the block-based image is split into a variety of sub-blocks that are overlapping or non-overlapping blocking as shown in figure 5. Figure 5 shows that (my love image) divided into a variety of non-overlapping sub-blocks. Compared to an exhaustive search, the block division will minimize the processing time of the matching process to find a similar feature vector in an image. Similarly, the segmented-based approach attempts to segment the image into various areas that completely covered the forged objects in the image. In contrast, the keypoint based approach detects unique local characteristics including corners, blobs, and edge in the image (without any type of segmentation). The common types in the keypoint based approach are scale invariant feature transform (SIFT) [24] and speeded up robust features (SURF) [25].

Hand-crafted features is designed manually by human such as natural scene statistics (NSS), image gradients, image histogram, image entropies and image filter responses. CMFD methods are categorize into two groups, rely on the type of features: spatial domain and frequency domain methods. The previous IC-MFDs are classified depending on the form of domain in which the features are extracted.

3.1. IC-MFD algorithms based spatial domain

Techniques based on spatial domain rely on the original image data in spatial domain (i.e. an image plane). Unique local characteristics are detected by the keypoint based approach. The common types are scale invariant feature transform (SIFT) [24] and SURF (speeded up robust features) [25]. Table 2 lists the previous recently IC-MFD algorithms according to feature extracted from spatial domain

From Table 2, it can see that most of the existing methods rely on keypoint based approach. It also see that the most popular keypoint features technique in CMFD is scale invariant feature transform (SIFT) based technique. SIFT features have the power to geometric transformations that are constant to scaling and rotation. However these methods can fail when identifying small duplicate regions; also it can be fail to distinguish between copy-move areas versus naturally equivalent areas; few precise in labeling the exact forgery [26] There is another drawback of these methods, keypoint-based techniques cannot detect this forgery if the forgery process is performed with low contrast regions, since they are unable to get enough keypoints for these areas [27].

Any of the post-processing operations (JPEG compression, illumination change, noise, contrast change, blurring, and combined of them), and/or geometric transformations (translation, rotation, scaling) applied to the image make the forged image more realistic and more difficult to distinguish duplicated areas. The optimal CMFD can be measured in terms of the robust to all post processing operations, all geometric transformation, detect multiple forgeries, And High accuracy of detection. From Table 2, it can be see the following observations:

a) The CMFD that proposed in [28], [29], [30], [31], are very robust to most of post-processing operations. However, it fail for other operations especially contrast change.
b) The CMFD that proposed in [32], [29], [30], [33], [31] are very robust to most of the geometric transformation. However, it fail for other geometric transformation such as translation.
c) The CMFD that proposed in [32], [34], [35], [33], are robust to some of post processing operations.
d) The CMFD that proposed in [28], [35], [34] are robust to some of geometric transformation.
e) In [33], only geometric transformation are applied. In [35], only post processing operations are applied

3.2. IC-MFD algorithms based transform domain

In general, most prevalent feature extraction methods for block-based methods is Frequency transform. The two primary reasons are noise robustness and rotational and translational components separability [36]. Techniques based on transformation include converting the original image data from a spatial domain (i.e. an image plane) into a frequency or spatial frequency domain. Uses the Frequency Domain to classify regions that are likely to be tampered in images. Block-based techniques separate the image into overlapping or non-overlapping squares or blocks of circle shapes as shown in Figure 5. Then using an effective feature transform, features can be extracted from each block such as discrete cosine transform [37, 38], discrete wavelet transform [39], curvelet transform [40], fourier transform [41, 42, 43], fast walsh- hadamard transform (fwht), singular value decomposition [44], principal component analysis, intensity, zernike moments [45], and combinations of them. Some of multiscale decomposition transform (MSD) like pyramid and wavelet transform lacks directionality. However, multiscale geometrical analysis (MGA) transforms [46] were presented to resolve this issue. One of these transforms is curvelet transform (CT) which decomposes the initial image into a group of subband frequency coefficients under various sizes, orientation and position [47]. Curvelet has a common characteristics that distinguishes it from the other types of transforms are higher directional sensitivity and lower redundancy [48]. Table 3 lists the previous recently IC-MFD algorithms according to feature extracted from transform domain.

Figure 5. My love image is split into non-overlapping sub-blocks

Table 2. Previous of IC-MFDs classified according to feature extracted from spatial domain (2015-2020).

Ref. Year	Description	Features	Feature Matching	Database	CMFD Categories	Limitations
Diaa *et al.*, [32], 2015.	CMFD based on Hessian features and a center-symmetric local binary pattern (CSLBP) is proposed. **Findings**: • Robust to JPEG compression, translation, scale.	Hessian Features	Center-Symmetric Local Binary Pattern (CSLBP)	MICC-F220	Segmented - Based Methods	• Not Robust to Rotation, Blur and Contrast Change. • Small duplicated region not detected.
Guzin *et al.* [28], 2016.	CMFD technique based on AKAZE features and nonlinear scale space is proposed. **Findings:** • Robust to rotated, blurred, AWGN added, or JPEG compressed.	AKAZE Features	Hamming Distance	Google Image, CoMo FoD	Keypoint-Based Methods	• The Scaling and contrast change is not covered.
Fan *et al.* [29], 2017	A CMFD rely on hybrid features is proposed. **Findings:** • Robust to rotation, scaling, JPEG compression and adding noise.	KAZE & SIFT Features	Improved n-best Matching Strategy	IMD	Keypoint-Based Methods	• Blur and Contrast Change is not covered. .
Sajjad *et al.* [30], 2017.	CMFD with 3 levels of Ward linkage based clustering is proposed. **Findings:** • Robust to rotation, scale, multilevel forgeries, noise, and JPEG compression.	The Scale Invariant Feature Transform (SIFT)	Ward-based clustering	MICC-F220	Keypoint-Based Methods	• False positive still higher. • Cannot detect splicing forgeries. • Contrast Change is not covered
Hesham *et al.*, [33], 2018.	CMFD based SIFT and fuzzy c-means (FCM) clustering is proposed. **Finding:** • Minimal execution time. • Robust to rotation, scaling.	SIFT	Fuzzy C-means (FCM)	MICC-F220	Keypoint-Based Methods	• False positive still higher. • Blur and Contrast Change is not covered.
Priya *et al.*, [35], 2018.	CMFD based on combining the traditional block-based and keypoint-based techniques is proposed. **Finding:** • Minimal execution time. • Robust to Brightness changes, contrast adjustments, color reduction and blurring.	Binary Features	Binary Discriminative Features (BDF)	CoMo FoD, IMD	Keypoint-Based Methods & block-based methods	• True &False positive metrics is not covered. • Noise and JPEG compression is not covered.
Aya *et al.*, [31], 2019.	CMFD rely on density-based clustering and Guaranteed Outlier Removal algorithm is proposed. **Finding:** • Robust to rotation, scaling, JPEG compression and noise. • low false positive rate	SIFT	DBSCAN	MICC-F220, IMD	Keypoint-Based Methods	• Blur and Contrast Change is not covered.
Vaishnavi *et al.*, [34], 2019.	CMFD based on means of symmetry based local features are proposed. **Finding:** • Robust to JPEG compression and uncompressed.	Local symmetry	Random Sampling Consensus (RANSAC)	MICC-F220	Keypoint-Based Methods	• The results need to be enhanced. • Only tested with JPEG compression. • Blur, noise, Contrast Change, and translation are not covered.

Table 3. Previous of IC-MFDs classified according to feature extracted from transform domain

Ref. Year	Description	CMFD Categories	Features	Feature Matching	Data base	Limitations
Mahmood *et al.*, [40], 2016.	CMFD based on DCT and Gaussian RBF kernel PCA is proposed. **Finding:** • Robust to noise, compression, and blurring. • Lower feature length.	Block-Based Methods	DCT and KPCA	Euclidean distance	DVMM Columbia and Internet	• Contrast change and scaling is not covered. • The findings only refer to a few of the post processing operations.
Khizar and Qazi, [42], 2017.	CMFD based on the DWT as well as the DCT for feature reduction is proposed. **Finding:** • Reduced feature vector.	Block-Based Methods	DWT coefficients	Block Similarity Threshold	Image samples	• Post-processing operations are not covered. • The findings for Post-processing operations are not applied.
Toqeer *et al.*, [38], 2017.	CMFD based on local binary pattern variance (LBPV) and stationary wavelet transform is proposed. **Finding:** • Robust to translation, flipping, blurring, rotation, scaling, color reduction, brightness change, and JPEG compression. • Lower feature length and computational time.	Block-Based Methods	block-wise quantized DCT coefficients	Shift Distance Criterion	CoMoFoD, KLTCI	• Noise, Contrast change and scaling is not covered. • The findings for Noise, Contrast change and scaling are not applied.
Toqeer *et al.*, [39], 2018.	CMFD based on the stationary wavelet transform (SWT) and DCT is proposed. **Finding:** • Robust to translation, blurring, JPEG compression, color reduction, and, brightness change. • Lower feature vectors length and computational time.	Block-Based Methods	DWT coefficients	Block distance and block similarity threshold.	CoMoFoD and UCID	• Rotation, larger scaling, additive Noise, and Contrast change are not covered.
Badal *et al.*, [37], 2019.	CMFD based on hybrid local features extraction (SURF and MSER) is proposed. **Finding:** • Robust to Rotation and Scaling. • Lower Dimension Features.	Block-Based Methods	SURF features	Two nearest neighbors (2NN) procedure	MICC-F220, MICC-F2000 and MICC-F600	• False positive still higher. • Algorithm needs to enhance especially for highly similar regions. • Noise, Contrast change, blurring, and JPEG compression are not covered. • The findings only refer to a few of the post processing operations.
Kunj *et al.*, [26], 2020.	CMFD based on Tetrolet transform is proposed. **Finding:** • Robust to blurring, brightness adjustment, contrast, rotation, scaling, JPEG compression. • Detect very small duplicated regions.	Block-Based Methods	4 low-pass and 12 high-pass coefficients	Block Similarity Threshold and Euclidean distance	GRIP and CoMoFoD	• Noise is not covered. • True &False positive metrics is not covered.
Shilpa *et al.*, [36], 2020.	CMFD based on doubly stochastic model (dsm) is proposed. **Finding:** • Robust to blurring, noise, rotation, scaling, and JPEG compression. • Splicing and copy-move are used. • Use few features.	Block-Based Methods	block-wise quantized DCT coefficients	ELM/SVM	CASIA v1.0 and v2.0	• Contrast change is not covered. • True &False positive metrics is not covered.

There is relatively little complexity in the features derived in the spatial domain. However, as the computational power of computers increases over time, in spite of their relatively high complexity, features extracted in other domains become more common because the following interesting issue:

a) The multiscale and multi-orientation features of the human visual system (HVS) are better reflected by these transforms.

b) A very interesting issue can be noted when using the frequency domain, signatures for the image blocks are provided via signal transform, enabling duplicate regions to be identified.
c) In the block-based approach, popular techniques are frequency transform. The noise, blurring, and JPEG compression post-processing operations are invariant by frequency transform.

The following points can be observed from Table 3:

a) The CMFD that proposed in [26, 36, 49], are very robust to most of post-processing operations. However, it fail for other operations especially contrast change.
b) The CMFD that proposed in [37, 26, 36, 38] are very robust to most of the geometric transformation. However, it fail for other geometric transformation such as translation.
c) The CMFD that proposed in [38, 39] are robust to some of post processing operations. In the detection of manipulations, especially for JPEG compression, DCT is very common transform due to its high compact energy ability (most of the information in a minimal number of coefficients). Therefore, the finding robust to JPEG compression.
d) The CMFD that proposed in [40], are robust to some of geometric transformation.
e) In [37], only geometric transformation are applied.
f) In [36], only post processing operations are applied.
g) The CMFD that proposed in [26], are very robust to post-processing operations and geometric transformation. According to the literature survey, Tetrolet transform was first used in the field of image forgery detection. In contrast to other similar methods such as DWT and contourlet transform, the features derived using Tetrolet transform are more robust due to improved direction sensitivity. Another transform is Curvelet has a common characteristics that distinguishes it from the other types of Transforms are Higher directional sensitivity and lower redundancy [41]. There is a very significant and inspiring aspect, which is that the curvelet transform is invariant to post-processing operations, such as noise, blurring, and JPEG compression.

There is relatively little complexity in the features derived in the spatial domain. However, as the computational power of computers increases over time, in spite of their relatively high complexity, features extracted in other domains become more common because the following interesting issue:

a) The multiscale and multi-orientation features of the human visual system (HVS) are better reflected by these transforms.
b) A very interesting issue can be noted when using the frequency domain, signatures for the image blocks are provided via signal transform, enabling duplicate regions to be identified.
c) In the block-based approach, popular techniques are frequency transform. The noise, blurring, and JPEG compression post-processing operations are invariant by frequency transform.

The following points can be observed from Table 3:

a) The CMFD that proposed in [26], [36], [40], are very robust to most of post-processing operations. However, it fail for other operations especially contrast change.
b) The CMFD that proposed in [37], [26], [36], [38] are very robust to most of the geometric transformation. However, it fail for other geometric transformation such as translation.
c) The CMFD that proposed in [38], [39] are robust to some of post processing operations. In the detection of manipulations, especially for JPEG compression, DCT is very common transform due to its high compact energy ability (most of the information in a minimal number of coefficients). Therefore, the finding robust to JPEG compression.
d) The CMFD that proposed in [40], are robust to some of geometric transformation.
e) In [37], only geometric transformation are applied.
f) In [39], only post processing operations are applied.
g) The CMFD that proposed in [26], are very robust to post-processing operations and geometric transformation. According to the literature survey, Tetrolet transform was first used in the field of image forgery detection. In contrast to other similar methods such as DWT and contourlet transform, the features derived using Tetrolet transform are more robust due to improved direction sensitivity. Another transform is curvelet has a common characteristics that distinguishes it from the other types of Transforms are Higher directional sensitivity and lower redundancy [41]. There is a very significant and inspiring aspect, which is that the curvelet transform is invariant to post-processing operations, such as noise, blurring, and JPEG compression.

3.3. Comparison of IC-MFD techniques

The most of current CMFD techniques aim to obtain the following issues: robustness to post-processing operations, geometric transformations, detect multiple forgeries, High detection accuracy. For comparison, Table 4 displays the results of some IC-MFDs based on spatial/frequency domain. The detection performance of the 15 IC-MFDs methods in multiple domains in term of true & false positive metrics are

compared. It can be observed that IC-MFDs based on spatial domain [31] tends to low false positive rate than the rest methods. However, [29] tends to high false positive rate than the rest methods.

Table 4. The comparative results by detection accuracy for various IC-MFDs across different domains.

Domain	IC-MFD	CMFD Categories	Database	Accuracy		
				TPR (%)	FPR (%)	F1 (%)
Spatial	[35]	Keypoint-Based Methods	CoMoFoD, IMD	N/A	N/A	88:35
	[29]	Keypoint-Based Methods	IMD	78.33	9.79	87.04
	[31]	Keypoint-Based Methods	MICC-F220, IMD	100	3.63	97.56
	[34]	Keypoint-Based Methods	MICC-F220	83.64	5.45	90.2
	[33]	Keypoint-Based Methods	MICC-F220	99.09	9.09	N/A
	[30]	Keypoint-Based Methods	MICC-F220	97.8	5.6	N/A
	[32]	Segmented -Based Methods	MICC-F220	92	8	N/A
	[28]	Keypoint-Based Methods	Google image, CoMoFoD	0,80	0,02	N/A
Transform	[26]	Block-Based Methods	GRIP and CoMoFoD	N/A	N/A	0.97
	[36]	Block-Based Methods	CASIA v1.0 and v2.0	N/A	N/A	96.56
	[42]	Block-Based Methods	Various images	N/A	N/A	73.62
	[37]	Block-Based Methods	MICC-F220, MICC-F2000 and MICC-F600	97.55	8.40	N/A
	[43]	Block-Based Methods	CASIA v1.0 and v2.0	N/A	N/A	93
	[44]	Block-Based Methods	CoMoFoD	N/A	N/A	79.33
	[45]	Block-Based Methods	MICC-F2000 and MICC-F220	N/A	N/A	0.91

The image may be exposed to both or either of the post-processing operations and geometric transformations, which may disturb the correlation between copy-moved regions then make it more difficult to distinguish duplicated areas. In order to detect multiple forgeries present in the image and to detect precise forgery in extremely same areas, IC-MFDs in [37], [42] needs to some improvement. Nevertheless, selecting the best feature extraction methods and effective matching technique will easily unveil forgery.

It can also be observed that detection accuracy of IC-MFDs based on frequency domain based on Tetrolet transform [26] outperforms the other frequency domain including Wavelet, DCT, and Fourier. Based on all possible directions at each block level, an image can be represented very well by the Tetrolet transform. This motivates us to mention the curvelet transform. Curvelet has a common characteristics that distinguishes it from the other types of transforms are higher directional sensitivity and lower redundancy [41]. According to the above-mentioned distinguishing features, this makes the Curvelet transform is an interesting candidate for IC-MFDs. Many IC-MFD algorithms based on block-based methods have been proposed during the previous decade. Furthermore, their greatest drawback is the consumption of time and resources, undetectable big scaling distortion, which makes them inappropriate for applications such as social networks, where a large number of photos are exchanged every day.

4. IC-MFD ALGORITHMS BASED MACHINE- CRAFTED FEATURES

There are many techniques based on manual feature extraction. In order to reduce the use of manual feature extraction, a new term has emerged which is automatic feature extraction. deep learning is an automatic feature extraction conducted automatically to learn features from raw data (images). Many of the traditional IC-MFDs rely on four phases like pre-processing (optional), feature extraction, matching and visualization (optional), While IC-MFDs based deep learning, feature extraction and matching integrated into one optimization step as shown in Figure 4.

Conventional image forgery detection methods for the both block based and keypoint based methods use handcrafted features. however, the most of the conventional image manipulation detection techniques has weakness points such as: (i) high computational complexity, (ii) limited to define a particular kind of manipulation by identifying a particular features in the image, (iii) the smoothing forgery section cannot be covered by the keypoint-based technique. Deep learning approaches have lately been proposed for the image tampering detection. Because of it's a owing the capacity to extract complicated features from the image, it also consumes less time and energy needed to determine hand-crafted features, these methods achieved better performance than conventional methods.

The types of deep learning (DL) models are convolutional neural networks (CNN), deep neural network (DNN), recurrent neural network (RNN), deep belief network [56], and deep auto encoder [57]. Among these DL models, convolutional neural networks (CNN) [58] is common. Convolution layer is important CNN layer that is considered as distinguishing and feature extractor. Using the various layers, the CNN pipeline start the features extraction process to extract the best feature from the image and then inputs

them into the basic classifier to detect the copy-move forgery if it occur. Table 5 lists various previous recently of IC-MFDs classified based on machine-crafted features.

Table 5. Previous of IC-MFDs classified based on machine-crafted features

Ref. Year	Description	Deep Learning Method	Limitation	Layers No	DB
Rao and Ni, [46], 2016.	CMFD based on CNNs is proposed.	CNN	• The results still need to improve.	10	CASIA v1.0, CASIA v2.0, Columbia gray DVMM
Zhang *et al.*, [47], 2016.	CMFD based on Stacked-Autoencoders (SAE) is proposed.	Stacked-Autoencoders (SAE)	• The results still need to improve.	7	CASIA v1.0, CASIA v2.0, Columbia
Junlin *et al.*, [48], 2017.	CMFD based on CNNs is proposed.	CNN AlexNet	• Poor performance in various real scenarios. • The results need to improve.	8	UCID, OXFORD flower, and CMFD
Davide *et al.*, [49], 2017.	CMFD based on simple constrained CNN is proposed.	Constrained CNN	• Few training set, robust to median filtering, Gaussian blurring, noise, resizing, and JPEG compression.	-	Synthetic
Wu *et al.*, [50], 2018.	CMFD based on BusterNet an end to end deep neural network is proposed.	BusterNet (Deep Neural Network)	• Weak in pure texture image.	-	CASIA v2.0, CoMoFoD dataset
Yue *et al.*, [51], 2018	CMFD based on an end-to-end DNN is proposed.	Deep Neural Network	• The results still need to improve.	-	CASIA TIDE v2.0 Dataset
Younis *et al.*, [52], 2019.	CMFD based on scale variant convolutional neural networks (SVCNNs) is proposed.	CNN	• Overall effectiveness was relatively poor. • Post-processing operations not covered.	15	IMD MICC-F600 CIFAR-10 Caltech-101
Wang *et al.*, [53], 2019.	CMFD based on mask regional convolutional neural network (Mask R-CNN) is proposed.	Mask Regional CNN	• Only robust to JPEG compression and Resizing.	-	Cover, Columbia
Mohamed *et al.*, [54], 2020.	CMFD based on CNNs is proposed.	CNN	• Post-processing operations not covered.	14	MICC-F220, MICC-F2000, and MICC-F600
Jun-Liu and Pun, [55], 2020.	CMFD based on a Dense-InceptionNet is proposed.	Deep Neural Network (DNN)	• The results still need to improve.	24	FAU, CASIA CMFD, and Comofodnew

4.1. Convolutional neural networks (CNN) overview

CNN has lately become very successful based on its learning abilities to extract the characteristics of an image. These abilities make it CNN more suitable to be used in image recognition, processing tasks, and IC-MFDs. The components of many CNN models are (1) a combination of one input and output layer, (2) a few convolution layers, and (3) fully connected layers. Here a briefly explain the mechanism of the CNN are presented. Firstly, an image is described as pixel matrix and fed them to the input layer. The output matrix is generated by the summation of multiply the input matrix and filter values.

Afterwards, a pooling operation is performed. Max, average or global-pooling can be used for pooling. The feature map that is passed into the input and the output layer is generated by applying the activation function to the input. There are commonly used activation functions such as relu, sigmoid, and tanh. In CNN, the pooling layer that been used to minimize the data dimension. Then the output passed to the next input layer and solving the problem of overfitting by losing some information. After all these sequences of hidden and pooling layers, the data passes through a various fully connected layers when classification is done. Finally, the error is measured in the output layer, which is then propagated backward through the network to change the filter weights. Thus, to minimize the error and train the network, a sequence of feedforward and backpropagation is performed.

4.2. Comparison of ic-mfd techniques

For comparison, Table 6 displays the results for IC-MFDs rely on machine-crafted features. It can be noted that IC-MFDs rely on CNN Surpassed all previous state of the art IC-MFDs methods that relied on machine-

crafted features. Since image analysis and computer vision are so highly advanced in the CNN approach, CNN usually provides outstanding performance [59], [60] in image forgery detection, by the composition of simplistic non-linear and linear filtering operations (e.g., rectification and convolution) [61]. According to the promising findings and the special properties, this makes the CNN is an interesting candidate for IC-MFDs.

Table 6. The comparative results by detection accuracy for various recently IC-MFDs based on machine-crafted features

IC-MFD	Deep Learning Method	Database	Performance		
			TPR (%)	FPR (%)	F1 (%)
[46]	CNN	CASIA v1.0, CASIA v2.0, Columbia gray DVMM	N/A	N/A	**96.38**
[47]	Stacked-Autoencoders (SAE)	CASIA v1.0, CASIA v2.0, Columbia	N/A	N/A	87.51
[48]	AlexNet	UCID, OXFORD flower, and CMFD	N/A	3.56	N/A
[50]	BusterNet (Deep Neural Network)	CASIA v2.0, CoMoFoD	N/A	N/A	75.98
[51]	Deep Neural Network	CASIA TIDE v2.0	N/A	N/A	75.72
[52]	CNN	IMD, MICC-F600, CIFAR-10, Caltech-101	N/A	N/A	**90**
[53]	Mask Regional Convolution Neural Network (Mask R-CNN)	Cover, Columbia	N/A	N/A	**93**
[27]	AlexNet	GRIP	N/A	N/A	0.93
[62]	CNN	CoMoFoD, BOSSBase	N/A	N/A	**95.97**
[54]	CNN	MICC-F220, MICC-F2000, and MICC-F600	**100**	N/A	N/A
[55]	Deep Neural Network (DNN)	FAU, CASIA CMFD, and CoMoFoD	N/A	N/A	0.6429

Just several hundred or less may be included in most current copy-move forgery image databases. Fine-tuning technology can solve this problem. Due to the effort and time used in the training process, A variety of pre-trained CNN models have emerged, such as AlexNet [63], VGG-16, VGG-19 as well as Caffe, which could be used to extract feature. In order to highlight that these models have reduced the effort and time in the training process, several of the above mentioned models were trained on the subgroup of ImageNet dataset [64]. The ImageNet dataset includes one k object categories and 1.2 million training images. Consequently, pre-trained networks are full of feature representations of various natural images. For several image classification problems, learned features can be used by transfer learning and feature extraction. As shown in Table 5, pre-trained CNN models [48], [27] were successfully implemented in the design of IC-MFDs.

5. CONCLUSION

Although there are some of review papers. It is noted that most of the review papers published after 2015. However. They did not provides an extensive review of major CMFD algorithms developed for (1) hand-crafted features. (2) Deep leaning methods. So they did not cover both of them. Therefore, this paper presented a comprehensive review of IC-MFD algorithms by collect various types of IC-MFD algorithms and group them according to their features used. Two groups, i.e. IC-MFD algorithms based Hand-Crafted Features and IC-MFD algorithms based machine-Crafted Features. After surveying many existing IC-MFD algorithms, it appears that most of the existing CMFD algorithms based on Hand-crafted features are very robust to most of post-processing operations. However, it fail for other operations especially contrast change. It can noted that in the block-based approach, the most common method in the CMFD typical methods are frequency transform. This due to its appropriateness for different feature extraction methods and the ability to accomplish an elevated matching efficiency. The performance of these two types of algorithms is analyzed. The performance of various recently IC-MFD algorithms depends on hand-crafted features are compared. It should be noted that IC-MFD depends on transform domain appears to be higher than those depends on spatial domain. It can also be found that the Tetrolet transform-based CMFD surpasses the other transform domain including Wavelet. This motivates us to mention the Curvelet transform. Curvelet has a common characteristics that distinguishes it from the other types of transforms are higher directional sensitivity and lower redundancy. According to the above-mentioned distinguishing features, this makes the Curvelet transform is an interesting candidate for IC-MFDs. The performance of various recently IC-MFD algorithms based on Machine-crafted features are compared. It

should be noted that IC-MFD depends on machine-crafted features appears to be higher than those depends on hand-crafted features. It can also be found that the CNN-based CMFD surpasses all past state of the art IC-MFDs methods which depending on handcrafted features. Also, the computation testing process is more effective, which consume less resources. According to the promising findings and the special properties, this makes the CNN is an interesting candidate for IC-MFDs. Our hope that this presented survey will provide researchers a complete overview in the area of IC-MFD.

ACKNOWLEDGEMENTS

This research is supported by Uniten iRMC Research Publication Fund 2021.

REFERENCES

[1] A. Kuznetsov and V. Myasnikov, "A new copy-move forgery detection algorithm using image preprocessing procedure," *Procedia Eng.*, vol. 201, pp. 436–444, 2017.
[2] N. B. Abd Warif *et al.*, "Copy-move forgery detection: survey, challenges and future directions," *J. Netw. Comput. Appl.*, vol. 75, pp. 259–278, 2016.
[3] X. Lin, J.-H. Li, S.-L. Wang, F. Cheng, X.-S. Huang, and others, "Recent advances in passive digital image security forensics: A brief review," *Engineering*, vol. 4, no. 1, pp. 29–39, 2018.
[4] W. D. Ferreira, C. B. R. Ferreira, G. da Cruz Júnior, and F. Soares, "A review of digital image forensics," *Comput. Electr. Eng.*, vol. 85, p. 106685, 2020.
[5] M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques," *Signal Process. Image Commun.*, vol. 39, pp. 46–74, 2015.
[6] A. D. Warbhe, R. V Dharaskar, and V. M. Thakare, "A survey on keypoint based copy-paste forgery detection techniques," *Procedia Comput. Sci.*, vol. 78, no. C, pp. 61–67, 2016.
[7] R. Dhanya and R. K. Selvi, "A state of the art review on copy move forgery detection techniques," in *2017 IEEE International Conference on Circuits and Systems (ICCS)*, 2017, pp. 58–65.
[8] N. Kanagavalli and L. Latha, "A survey of copy-move image forgery detection techniques," in *2017 International Conference on Inventive Systems and Control (ICISC)*, 2017, pp. 1–6.
[9] A. U. Tembe and S. S. Thombre, "Survey of copy-paste forgery detection in digital image forensic," in *2017 international conference on innovative mechanisms for industry applications (ICIMIA)*, 2017, pp. 248–252.
[10] S. Teerakanok and T. Uehara, "Copy-move forgery detection: A state-of-the-art technical review and analysis," *IEEE Access*, vol. 7, pp. 40550–40568, 2019.
[11] L. Zheng, Y. Zhang, and V. L. L. Thing, "A survey on image tampering and its detection in real-world photos," *J. Vis. Commun. Image Represent.*, vol. 58, pp. 380–399, 2019.
[12] T. J. Shah and M. T. Banday, "A Comparative Study of Block-BasedCopy-Move Forgery Detection Techniques," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 2020, pp. 1–6.
[13] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy--move attack detection and transformation recovery," *IEEE Trans. Inf. forensics Secur.*, vol. 6, no. 3, pp. 1099–1110, 2011.
[14] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Trans. Inf. forensics Secur.*, vol. 7, no. 6, pp. 1841–1854, 2012.
[15] 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, 2013.
[16] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD-New database for copy-move forgery detection," in *Proceedings ELMAR-2013*, 2013, pp. 49–54.
[17] J. Dong, W. Wang, and T. Tan, "Casia image tampering detection evaluation database," in *2013 IEEE China Summit and International Conference on Signal and Information Processing*, 2013, pp. 422–426.
[18] V. S. Kulkarni and Y. V Chavan, "Comparison of methods for detection of copy-move forgery in digital images," *Spvryan's Int. J. Eng. Sci. Technol.*, vol. 1, no. 1, 2014.
[19] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy--move forgery detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 11, pp. 2284–2297, 2015.
[20] B. Wen, Y. Zhu, R. Subramanian, T.-T. Ng, X. Shen, and S. Winkler, "COVERAGE—A novel database for copy-move forgery detection," in *2016 IEEE International Conference on Image Processing (ICIP)*, 2016, pp. 161–165.
[21] T. Qazi *et al.*, "Survey on blind image forgery detection," *IET Image Process.*, vol. 7, no. 7, pp. 660–670, 2013.
[22] D. M. Uliyan, H. A. Jalab, A. Abuarqoub, and M. Abu-Hashem, "Segmented-Based Region Duplication Forgery Detection Using MOD Keypoints and Texture Descriptor," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, 2017, pp. 1–6.
[23] S. Sadeghi, H. A. Jalab, K. Wong, D. Uliyan, and S. Dadkhah, "Keypoint based authentication and localization of copy-move forgery in digital image," *Malaysian J. Comput. Sci.*, vol. 30, no. 2, pp. 117–133, 2017.
[24] D. G. Lowe, "Object recognition from local scale-invariant features," in *Proceedings of the seventh IEEE international conference on computer vision*, 1999, vol. 2, pp. 1150–1157.

[25] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (SURF)," *Comput. Vis. image Underst.*, vol. 110, no. 3, pp. 346–359, 2008.
[26] K. B. Meena and V. Tyagi, "A copy-move image forgery detection technique based on tetrolet transform," *J. Inf. Secur. Appl.*, vol. 52, p. 102481, 2020.
[27] G. Muzaffer and G. Ulutas, "A new deep learning-based method to detection of copy-move forgery in digital images," in *2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT)*, 2019, pp. 1–4.
[28] G. Ulutas and G. Muzaffer, "A new copy move forgery detection method resistant to object removal with uniform background forgery," *Math. Probl. Eng.*, vol. 2016, 2016.
[29] F. Yang, J. Li, W. Lu, and J. Weng, "Copy-move forgery detection based on hybrid features," *Eng. Appl. Artif. Intell.*, vol. 59, pp. 73–83, 2017.
[30] S. Dadkhah, M. Koppen, S. Sadeghi, K. Yoshida, H. A. Jalab, and A. A. Manaf, "An efficient ward-based copy-move forgery detection method for digital image forensic," in *2017 International Conference on Image and Vision Computing New Zealand (IVCNZ)*, 2017, pp. 1–6.
[31] A. Hegazi, A. Taha, and M. M. Selim, "An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal," *J. King Saud Univ. Inf. Sci.*, 2019.
[32] D. M. Uliyan, H. A. Jalab, and A. W. A. Wahab, "Copy move image forgery detection using Hessian and center symmetric local binary pattern," in *2015 IEEE Conference on Open Systems (ICOS)*, 2015, pp. 7–11.
[33] H. A. Alberry, A. A. Hegazy, and G. I. Salama, "A fast SIFT based method for copy move forgery detection," *Futur. Comput. Informatics J.*, vol. 3, no. 2, pp. 159–165, 2018.
[34] D. Vaishnavi and T. S. Subashini, "Application of local invariant symmetry features to detect and localize image copy move forgeries," *J. Inf. Secur. Appl.*, vol. 44, pp. 23–31, 2019.
[35] P. M. Raju and M. S. Nair, "Copy-move forgery detection using binary discriminant features," *J. King Saud Univ. Inf. Sci.*, 2018.
[36] S. Dua, J. Singh, and H. Parthasarathy, "Detection and localization of forgery using statistics of DCT and Fourier components," *Signal Process. Image Commun.*, vol. 82, p. 115778, 2020.
[37] B. Soni, P. K. Das, and D. M. Thounaojam, "Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features," *J. Inf. Secur. Appl.*, vol. 45, pp. 44–51, 2019.
[38] T. Mahmood, A. Irtaza, Z. Mehmood, and M. T. Mahmood, "Copy--move forgery detection through stationary wavelets and local binary pattern variance for forensic analysis in digital images," *Forensic Sci. Int.*, vol. 279, pp. 8–21, 2017.
[39] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," *J. Vis. Commun. Image Represent.*, vol. 53, pp. 202–214, 2018.
[40] T. Mahmood, T. Nawaz, A. Irtaza, R. Ashraf, M. Shah, and M. T. Mahmood, "Copy-move forgery detection technique for forensic analysis in digital images," *Math. Probl. Eng.*, vol. 2016, 2016.
[41] E. Candes, L. Demanet, D. Donoho, and L. Ying, "Fast discrete curvelet transforms," *Multiscale Model. Simul.*, vol. 5, no. 3, pp. 861–899, 2006.
[42] K. Hayat and T. Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms," *Comput. Electr. Eng.*, vol. 62, pp. 448–458, 2017.
[43] S. Dua, J. Singh, and H. Parthasarathy, "Image forgery detection based on statistical features of block DCT coefficients," *Procedia Comput. Sci.*, vol. 171, pp. 369–378, 2020.
[44] G. Gani and F. Qadir, "A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata," *J. Inf. Secur. Appl.*, vol. 54, p. 102510, 2020.
[45] H. Wang and H. Wang, "Perceptual hashing-based image copy-move forgery detection," *Secur. Commun. Networks*, vol. 2018, 2018.
[46] Y. Rao and J. Ni, "A deep learning approach to detection of splicing and copy-move forgeries in images," in *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2016, pp. 1–6.
[47] Y. Zhang, J. Goh, L. L. Win, and V. L. L. Thing, "Image Region Forgery Detection: A Deep Learning Approach.," *SG-CRC*, vol. 2016, pp. 1–11, 2016.
[48] J. Ouyang, Y. Liu, and M. Liao, "Copy-move forgery detection based on deep learning," in *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, 2017, pp. 1–5.
[49] D. Cozzolino, G. Poggi, and L. Verdoliva, "Recasting residual-based local descriptors as convolutional neural networks: an application to image forgery detection," in *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, 2017, pp. 159–164.
[50] Y. Wu, W. Abd-Almageed, and P. Natarajan, "Busternet: Detecting copy-move image forgery with source/target localization," in *Proceedings of the European Conference on Computer Vision (ECCV)*, 2018, pp. 168–184.
[51] Y. Wu, W. Abd-Almageed, and P. Natarajan, "Image copy-move forgery detection via an end-to-end deep neural network," in *2018 IEEE Winter Conference on Applications of Computer Vision (WACV)*, 2018, pp. 1907–1915.
[52] Y. Abdalla, M. T. Iqbal, and M. Shehata, "Convolutional Neural Network for Copy-Move Forgery Detection," *Symmetry (Basel).*, vol. 11, no. 10, p. 1280, 2019.
[53] X. Wang, H. Wang, S. Niu, and J. Zhang, "Detection and localization of image forgeries using improved mask regional convolutional neural network," *Math. Biosci. Eng.*, 2019.
[54] M. A. Elaskily *et al.*, "A novel deep learning framework for copy-moveforgery detection in images," *Multimed. Tools Appl.*, pp. 1–26, 2020.

[55] J.-L. Zhong and C.-M. Pun, "An End-to-End Dense-InceptionNet for Image Copy-Move Forgery Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2134–2146, 2019.
[56] H. Lee, C. Ekanadham, and A. Y. Ng, "Sparse deep belief net model for visual area V2," in *Advances in neural information processing systems*, 2008, pp. 873–880.
[57] H. Larochelle, Y. Bengio, J. Louradour, and P. Lamblin, "Exploring strategies for training deep neural networks.," *J. Mach. Learn. Res.*, vol. 10, no. 1, 2009.
[58] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, 1998.
[59] G. Giacinto and F. Roli, "Design of effective neural network ensembles for image classification purposes," *Image Vis. Comput.*, vol. 19, no. 9–10, pp. 699–707, 2001.
[60] K. Fukushima, S. Miyake, and T. Ito, "Neocognitron: A neural network model for a mechanism of visual pattern recognition," *IEEE Trans. Syst. Man. Cybern.*, no. 5, pp. 826–834, 1983.
[61] A. Vedaldi and K. Lenc, "Matconvnet: Convolutional neural networks for matlab," in *Proceedings of the 23rd ACM international conference on Multimedia*, 2015, pp. 689–692.
[62] R. Thakur and R. Rohilla, "Copy-Move Forgery Detection using Residuals and Convolutional Neural Network Framework: A Novel Approach," in *2019 2nd International Conference on Power Energy, Environment and Intelligent Control (PEEIC)*, 2019, pp. 561–564.
[63] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Commun. ACM*, vol. 60, no. 6, pp. 84–90, 2017.
[64] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, "Imagenet: A large-scale hierarchical image database," in *Computer Vision and Pattern Recognition, 2009. CVPR 2009. IEEE Conference on*, 2009, pp. 248–255.

BIOGRAPHIES OF AUTHORS

Ismail Taha Ahmed received his B.E. and M.Sc. degrees in Computer Science from College of Computer Science and Information Technology, University of Anbar, Anbar, in 2005 and 2009, respectively. He received his Ph.D. degrees in Computer Science from College of Computer Science and Information Technology, Universiti Tenaga Nasional, Putrajaya, Malaysia, in 2018. His research interests Include Image Processing, Image Quality Assessment, Deep Learning, and Computer Vision.

Baraa Tareq Hammad received her B.E. and M.Sc. degrees in Computer Science from College of Computer Science and Information Technology, University of Anbar, Anbar, in 2005 and 2012, respectively. She received her Ph.D. degrees in Computer Science from College of Computer Science and Information Technology, Universiti Tenaga Nasional, Putrajaya, Malaysia, in 2018. Her research interests Include Information Security, IoT and Network Security.

Norziana Jamil received her BSc (Information Technology), 2000, form Universiti Kebangsaan Malaysia, and she received her M.Sc. (Information Security), 2005, from Royal Holloway Universiti of London, UK, while she finish her PhD (Security in Computing), 2013, from UPM university, She is interested in cryptography, Authentication, SCADA system, wireless sensor network.