AI-enabled digital forgery analysis and crucial interactions monitoring in smart communities

Ahmed Sedik [a], Yassine Maleh [b], Ghada M. El Banby [c], Ashraf A.M. Khalaf [d], Fathi E. Abd El-Samie [c], Brij B Gupta [e,f,g,*], Konstantinos Psannis [h], Ahmed A. Abd El-Latif [i,j]

ARTICLE INFO

Keywords:
Forgery detection
Deep learning
IoT
Smart cities
Security analysis

ABSTRACT

Digital forgery has become one of the attractive research fields in today's technology. There are several types of forgery in digital media transmission, especially digital image transmission. A common type of forgery is copy-move forgery (CMF). The CMF may be encountered in streets, railway stations, underground stations, or festivals. This type of forgery may lead to hugger-mugger in some cases. Therefore, there is a need to find a sufficient countermeasure mechanism to detect image forgeries. This paper presents a new CMFD approach that depends on deep learning for IoT based smart cities. Two well-known deep learning models, namely CNN and ConvLSTM, are adopted for CMFD. The proposed models are tested on MICC-220, MICC-600 and MICC 2000 datasets for validation. Several tests are performed to verify the effectiveness of the proposed models. The simulation results reveal that the testing accuracy reaches 95%, 73%, and 94% for MICC-F220, MICC-F600 and MICC-F2000 datasets. In addition, the proposed approach achieves an accuracy of 85% for a combined set of all datasets.

1. Introduction

Manipulation alterations the contents of original data to create a new fabricated data. Unfortunately, manipulated data has become a growing interest concerning spreading misinformation via data sharing in smart communities. Image forgery detection has become one of the interesting fields that attract researchers in the field of image processing. Image forgery is involved in several fields such as access control systems, identity spoofing, biometrics forensics, and cyber security. Image forgery also affects the sustainable development of business(Bustos-Contell et al., 2019; Tewari and Gupta, 2020). Digital image forgery detection can be performed by looking up the disorders in such a suspicious image or similarities between the image blocks based on the features extracted from them. These disorders distinguish between the original and the tampered images (Xiang et al., 2018). Image forgery detection is mainly involved in security applications(Peng et al., 2015; Ribeiro-Navarrete et al., 2021a; Jha et al., 2021). There are several types of forgery in digital images. These types can be divided into image splicing, morphing, retouching, resampling, as well as CMF (Elaskily et al., 2017). Splicing can be generated by image fusion between several images, including objects, while the fused image includes both objects from all images (Prajapati and Desai, 2015; Ribeiro-Navarrete et al., 2021b). Image morphing can be performed by merging shapes from different images to evaluate other shapes different from the original ones (Thajeel and Sulong, 2014), while image retouching is based on hiding some features of the image using enhancement by applying a filtering process on the image (Lassala et al., 2021; Shah et al., 2013). Image resampling means resizing such an object in the image to give another meaning (Kirchner and Böhme, 2008). The CMF is based on copying a particular region or object from the image and pasting it into another place in the

same image (Birajdar and Mankar, 2013). This type is difficult to detect because the moved part has the same image characteristics, including contrast, brightness, and colors. Fig. 1 includes different kinds of image forgery. The CMF is common in images, and it is difficult to be detected. This difficulty is based on the limited effects in the tampered image. The copied regions have the exact nature of the whole image. So, the copy-move tampered image includes a homogeneous context. Image forgery detection is carried out without knowing the original image, which is commonly known as blind detection. The CMFD algorithms can be classified into traditional modalities and deep learning modalities. Traditional modalities are the algorithms in which the features are extracted from the images in order to detect the forgery occurrence in the image (Benrhouma et al., 2016; Farid, 2009; Jing et al., 2014; Shafiq et al., 2020). On the other hand, deep learning(Nguyen et al., 2021) modalities are extract features first from images and then perform classification and detection (Y. Zhan et al., 2017).

Traditional CMFD techniques are divided into block-based techniques and non-block-based techniques. The block-based techniques include segmentation the image into blocks, where these segmented blocks may be circular or rectangular in shape. The main idea of these techniques is to extract the features from the blocks. There are several feature extraction techniques by which the features can be collected, including invariant moments, image texture and intensity, as well as frequency transformations (Warif et al., 2016). After that, it is required to distinguish the similarities between blocks based on the extracted features (Nanda et al., 2014; Pineiro-Chousa et al., 2019).

Fridrich *et al.* (Fridrich et al., 2003) proposed a forgery detection algorithm based on Discrete Cousin Transform (DCT) for CMFD. This algorithm obtains the DCT for the image blocks. The coefficients of the DCT resulting from each block are considered as the features of the image. These features are used to discriminate the similarities between blocks. The work in (Boz and Bilge, 2016) depends on Local Binary Patterns (LBPs) as well as DCT for CMFD. This technique segments the images for feature extraction and detection to detect blocks. All blocks are transformed to the LBP domain. Then, the DCT is performed on each LBP block. The resulting feature map from this process is ordered lexicographically to detect similarities between blocks. All these feature matrices are sequentially sorted. Another CMFD algorithm is proposed in (Kang et al., 2012). This algorithm is based on the DCT and the SVD to discriminate the locations of CMFs. This algorithm comprises segmentation of the image into blocks, DCT of blocks to extract features, and SVD to enhance the noise immunity and allow dimensionality reduction. The techniques of (Leng et al., 2010a) and (Leng et al., 2010b) have been adopted to enhance the discrimination ability in the DCT domain. Additionally, texture and intensity techniques have been carried out for feature extraction and detection of similarities between the tampered images.

Sharma et al. (Sharma and Ghanekar, 2015) proposed another forgery detection algorithm, converts the color images to a grey-scale images. Then, these images are segmented to blocks. Center Symmetric Local Binary Patterns (CSLBP) technique is carried out to extract the features of these blocks. The similarity of the blocks is detected using thresholds, which are calibrated by Euclidean distance and shift frequency (Kang et al., 2012).

In the block-based approach, the non-block-based CMFD techniques are carried out on the whole image rather than each block. Invariant key point techniques are used for feature extraction, such as edges, blobs, and corners from the image. Several vital points descriptors are involved in CMFD such as SIFT and SURF (Leng et al., 2010a). The algorithm by (Leng et al., 2010b) adopted SIFT for CMFD. The algorithm in (Leng et al., 2010b) is based on the best-bin-first nearest neighbor methodology and it faces a lake of a low performance of detection of small-size

forgeries. The work in (Amerini et al., 2011) adopting a CMFD system can detect forgeries using image scaling, transition, and rotating. It consists of four steps: the first step is SIFT feature extraction, the second step is key point vectors construction, the third step is key point clustering, and the last step is estimating geometric transformation.

The work in (Costanzo et al., 2014) is based on SIFT key points removal and injection and deploys three detectors to determine which SIFT key points are removed. These detectors include SVMa, CHI-square distance, and key points to evaluate ratio. The discrimination is based on the consistency of the feature map generated from the key points. In addition, these detectors are acquired to detect the injected fake key points. The simulation results reveal that the deployed detectors appear to have high performance prior to injection and removal of fake key points.

Other forgery detection techniques are based on detecting the boundaries of objects in the image and performing image segmentation. The segmentation process is carried out according to the relationship of neighboring pixels such as the algorithms in (Alghamdi et al., 2020; Elaskily et al., 2018; Hosny et al., 2018; 2019; Yan et al., 2013; Yu et al., 2018). Benrhouma *et al.* (Alghamdi et al., 2020) proposed a forgery detection approach based on chaotic watermark. This approach can detect the occurrence of the forgery as well as focus on the tampered areas and is carried out on several images under a set of attacks. The simulation results reveal that the proposed methodology achieved a true positive rate (TPR) of 46.7657%.

Deep learning is involved in several fields, such as medical image analysis (Gupta et al., 2021; Haggag et al., 2019; Peraković et al., 2021; Wang et al., 2019), human being identification (Elgendy et al., 2021; Sallam et al., 2019), agriculture(AlZu'bi et al., 2019), and security (Liu et al., 2016; Peng et al., 2021). Deep learning is also involved in the detection of image forgeries (Al Azrak et al., 2020; Chu et al., 2018; Elaskily et al., 2020; Kim and Lee, 2017; Wu et al., 2018). Dep learning modality is based on constructing a model that extracts features from a certain image in a hierarchy of feature maps. One of the standard deep learning techniques is CNNs. This type of deep learning model contains convolutional and pooling layers (Ouyang et al., 2017).

A deep learning approach based on CNN has been represented in (Wu et al., 2018). This approach deploys a pre-trained deep learning model. Then, fine-tuning is performed on the architecture of the network via a small training set of CMF images. This method represents a high performance prior to computer generated forgeries. The performance of CMF method seems to be not sufficient. In addition, the authors of (Wu et al., 2018) performed CNN by deconvolutional layers (DeConnv.). This algorithm is based on image segmentation into blocks. CNN is carried out on these blocks in order to extract the features from them. After that, similarities between blocks are computed and the matched patterns are localized. Then, a forgery mask is evaluated using the (DeConv.). Deep learning techniques are involved in images splicing (Kim and Lee, 2017), but it is still not deeply involved in CMFD research field. Image forgery detection based on deep learning can be carried out by several methodologies such as Multi-layer Convolution Feature Fusion (MCFF) and Online Hard Example Mining (OHEM) (Chu et al., 2018). Additionally, the pandemic of COVID-19 has quickly changed the behaviors of people allowing new opportunities for fabricating.

Therefore, in this paper, we propose a new forgery detection with a deep learning model (DLM) in smart cities. The proposed strategy utilized two well-known models, namely CNN, and ConvLSTM. The proposed DLMs are designed in order to have high performance with the lower complexity of the whole detection method. The proposed model is carried out on MICC-220, MICC-600, and MICC 2000 data sets in order to validate the model. Several tests and statistical analyses are conducted to verify the effectiveness of the new detection approach. Results of all tests show the superiority of our algorithm over some robust state-of-art methods.

This paper is organized into five sections. The first section introduces the main idea of this paper and includes a brief explanation of the works in the literature. The second section consists of a discussion of benchmark models which are carried out on the same datasets of the proposed modality. The third section shows the proposed framework and the explanation of the proposed deep learning model. In addition, section four presents the simulation results and a brief comparison between the proposed model and the benchmark models. Finally, section five concludes the proposed work in this paper.

2. Benchmark models

This section reviews the two most important benchmarks models related to our proposed approach. The first benchmark model in (Elaskily et al., 2020) discussed the effect of number of epochs on the performance of the proposed DLM. Another benchmark DLM in (Al

		Predicted	
		Tampered	Original
True	Tampered	T_P	F_N
	Original	F_P	T_N

Fig. 8. The confusion matrix.

Table 1
The details of MICC-F220, MICC-F2000 and MICC-F600 datasets .

Dataset	Composition	Size of Images
MICC-F220	110 Original images 110 Tampered images	722 × 480 to 800 × 600 pixels
MICC-F2000	700 tampered images 1300 original images.	2048 × 1536 pixels
MICC-F600	152 tampered images 448 original images.	800 × 532 to 3888 × 2592 pixels

to "total ignorance" of the future.

- *The convolutional layer*

The convolutional layer contains a set of two-dimensional digital filters. Each filter in this set is convoluted to the input images. This convolution process's outputs are considered the feature maps of the input images, as shown in Fig. 5. Assume an RGB image with a depth of 3, and the number of the two-dimensional digital filters equals 16. The output feature map from the convolution process between the input image and the digital filters would be 16 instead of 3. The convolution process leads to an increment of the dimensions of images. Thus, there is a need for dimension decrement which is performed by the pooling layer.

. The value of a pixel which is generated (p_{new}) is obtained as:

$$p_{new} = \sum_{i \in a} p_i . w_i \tag{6}$$

The activation function carries out an important role. This role is represented to obtain the convolutional layer's output. The activation function used in this paper is Rectified Linear Unint (ReLU) activation function. It is represented as a linear function that allows the positive values to be the same, while the negative values will be zeros. The output of the activation function to the neuron output is shown in Eq. 7.

$$f(x) = max(0, x) \tag{7}$$

- *Pooling layer*

The pooling layer is considered as a kind of feature extraction beside the convolutional layer. The role of the pooling process is to adjust the output of the convolutional layer. The pooling process is carried out on the image by segmenting the image into windows with a window size of $n \times n$. A single value represents these windows. There are two types of pooling, mean and max. pooling. The mean pooling is performed by obtaining the mean value of each window, while the max. pooling is achieved by getting the maximum value of the window as shown in Fig. 6.

- *Classification network*

The classification network consists of a fully connected layer and classification layer. The fully connected layer is responsible for handling the output from the feature extraction network and the input of the classification layer. While the classification layer is responsible for evaluating the binary output.

The fully connected layer converts the data from the feature map generated from the feature extraction network to a 1-D vector. The generated vector would be the input of the classification layer.

The classification layer is considered as the last layer of DLM. This layer is able to obtain the decision of the model. It can be a binary decision of multiclass decision. A dense layer implements the classification process. The activation function of this layer is the softmax activation function. The probability $p(x)$ of a certain input x can be calculated by:

$$\mathbf{P}(\mathbf{y} = \mathbf{j}|\mathbf{x}) = \frac{e^{\mathbf{x}^T \mathbf{w}_j}}{\sum_{k=1}^{K} e^{\mathbf{x}^T \mathbf{w}_k}} \tag{8}$$

Table 3
The accuracy comparison between all trigometric transformation images.

Cases [Transformations]	TPR	FPR	FNR	TNR	Accuracy (%)	TT
1D-DCT & DWT	100	0	0	100	100%	1.815
2D-DCT & DWT	100	0	0	100	100%	1.981
1D-DFT	97.22	0	27.78	100	99%	2.098
1D-DFT & DWT	100	0	0	100	100%	2.132
2D-DFT	36.1	0	63.9	100	68%	2.165
2D-DFT & DWT	58.33	0	41.67	100	79%	2.066
DST	91.6	8.4	0.7	99.3	95%	1.572
DST & DWT	100	4	0	96	98%	2.323

- **Detection accuracy**

The accuracy of detection $Accuracy_{detection}$ can be calculated as follows:

$$Accuracy_{detection} = \frac{No.\ of\ correctly\ detected\ images}{Total\ No.\ of\ images} \times 100 = \frac{(T_N + T_P)}{(T_P + F_P + T_N + F_N)} \times 100 \quad (9)$$

where;

4.2. Datasets

The proposed DLM is validated by three datasets, MICC-F220, MICC-F600 and F2000 (Amerini et al., 2011), and a combination set of whole of them. MICC-F220 dataset consists of 110 original and 110 tampered images, while MICC-F600 consists of 448 original and 152 tampered images. MICC-F2000 contains 1300 original and 700 tampered images. Table 1 shows a summary of these datasets. Fig. 9 shows samples of the copy-move forgery datasets.

4.3. Results of forgery detection without transformations

This paper proposed a hybrid DLM based on ConvLSTM and CNNs. The proposed model is carried out on both MICC-F220, MICC-F600 and MICC-F2000 datasets. The simulation experiments are performed by python 3.5, Keras and TensorFlow on local machine with the following specifications:

CPU → Intel Core i7 8th edition.
RAM: 16 GB (DDR4).
GPU: NVIDIA 4 GB (DDR4) supporting CUDA.

The input data is split into training and testing subsets. The training subset represents 80% of the input dataset, while the testing subset represents 20% of the input data. This percentage is commonly known as 80-20 splitting. In addition, the training subset is split by k-fold technique to evaluate a sufficient cross validation process. The k-fold technique is based on shuffle and splits the data into k and 1-k subsets, where k is a real value between 0 and 1. Here, this paper performs the k-fold technique with k equals 0.1. Fig. 10 (a), (c), (e), and (g) show the training and validation curves of the accuracy during the training epochs. The training process is performed with fifteen epochs and the input data is fragmented into batches with batch size of 10. The simulation results from the accuracy curves reveal that the training process is performed without overfitting as the curves seem to be stable in most of the curve epochs with a sufficient increment during the training process. In addition, the loss curves in Fig. 10(b), (d), (f), and (h) seem to be stable and decrease during the training process. The testing process carried out on the remaining 20% of the datasets reveals that the testing accuracy achieves 95%, 73%, and 94% for MICC-F220, MICC-F600 and MICC-F2000, respectively. In addition, the proposed model achieved an accuracy of 85% for the combined set of whole datasets. So, the proposed cannot be considered a sufficient model for CMFD, until a modification to enhance its performance. The area can represent a visualized accuracy under curve (auc) and ROC curve as shown in Fig. 11(a), (b), (c), and (d). The proposed DLM is validated by (Elaskily et al., 2020), which is carried out on the same datasets. A brief comparison is shown in Table 2.

4.4. Results of trigometric transformations

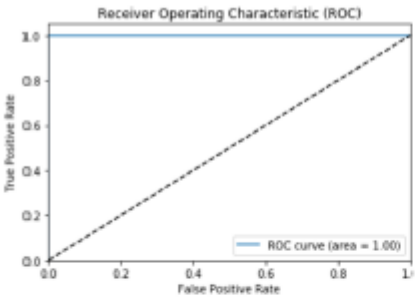
The enhancement of the proposed deep learning model is represented by adding a trigometric transformations to the feature extraction module. Here, we proposed several trigometric transformations such as Discrete Cousin Transform (DCT) in one-dimensional (1D-DCT)and two-dimensional (2D-DCT) modalities cascaded by Discrete Wavelet Transform (DWT) (1D-DCT & DWT, 2D-DCT & DWT). Discrete Fourier Transform (DFT) is also included in the form of one-dimensional (1D-DFT) and two-dimensional (2D-DFT) modalities. Both of 1D-DFT and 2D-DFT are carried out on the image with and without DWT addition. Discrete Sin Transform (DST) is also performed with and without DWT. Fig. 12 shows the accuracy and loss curves of the training and validation for the proposed model at each case of trigometric transformation technique. Table 3 shows the testing accuracy of each technique. In addition, the accuracy achieved 100% at most of the cases. The simulation results reveal that the proposed approach can be considered as an efficient CMFD system. In addition, a visualization of the testing accuracy of the proposed DLM is represented in Fig. 13. Table 4 shows a comparison between the results of the proposed approach and Ref. (Al Azrak et al., 2020) based on CNN. The results of the comparison reveal that the proposed approach presents a high-performance compared to the one in (Al Azrak et al., 2020). Additionally, the proposed approach performs well in digital watermarked images.

5. Results discussion

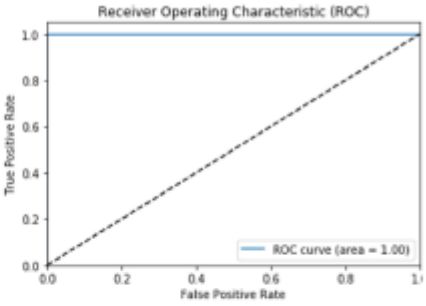
Deep learning is investigated in several security issues including splicing detection (Rao and Ni, 2016) and steganalysis (Wang et al., 2015). This paper aims to achieve an efficient CMFD system based on trigometric transforms and ConvLSTM. For this purpose, several transformations are carried out on both MICC-F220, MICC-F600, MICC-F2000 and a combined dataset of whole of these datasets. This section provides a comparison between the proposed modality and the state-of-the art methods in the literature. Table 5 shows a comparison between the proposed CMFD system based on ConvLSTM and the works in the literature based on traditional and deep learning methods. This comparison includes accuracy and testing time. The simulation results reveal that the proposed modalities including ConvLSTM with both 1D-DCT & DWT, 2D-DCT & DWT, and 2D-DFT & DWT can be considered efficient CMFD systems in the presence of real time applications as they achieved an accuracy of 100% and testing time of 1.8 seconds.

6. Conclusions

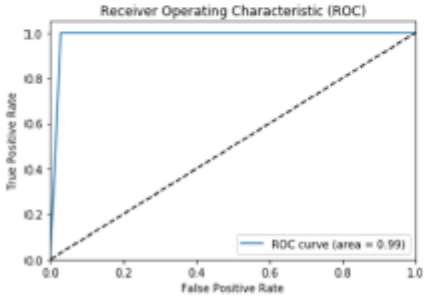
This paper presented a CMFD system based on deep learning. This system can be deployed by IoT technology in smart cities. The proposed deep learning model is based on convolutional neural networks and a convolutional long short term memory. The proposed system has been implemented on MICC-F220, MICC-F600 and MICC-F2000 datasets for validation. In addition, the proposed model is combined with a



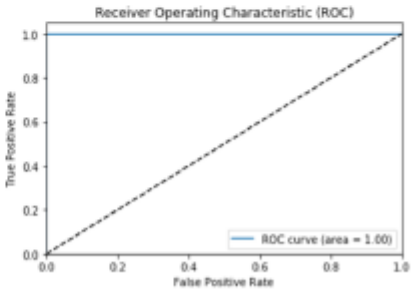
(a) ROC Curve for DCT-1D with DWT



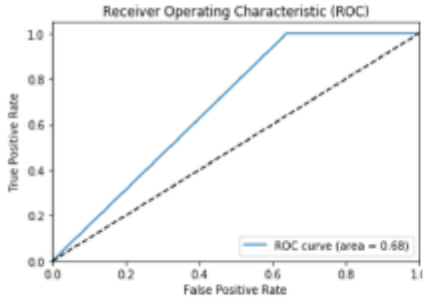
(b) ROC Curve for DCT-2D with DWT



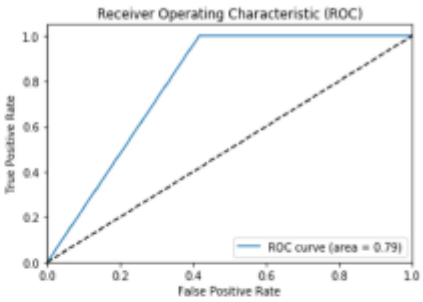
(c) ROC Curve for DFT-1D



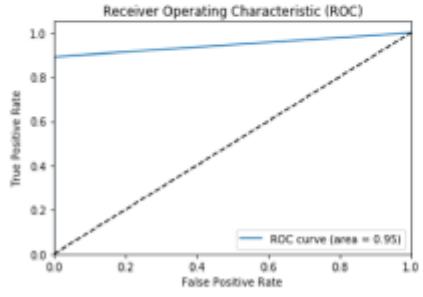
(d) ROC Curve for DFT-1D with DWT



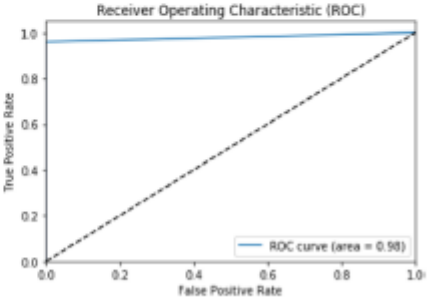
(e) ROC Curve for DFT-2D



(f) ROC Curve for DFT-2D with DWT



(g) ROC Curve for DST



(h) ROC Curve for DST with DWT

Fig. 13. ROC curves of the proposed DLM with trigometric transformations.

Table 4
The accuracy comparison between the proposed algorithm and the state-of-the-art algorithms.

Cases [Transformations]	Accuracy (%)	
	Algorithm Based on CNN [40]	Proposed Model
1D-DCT & DWT	90%	100%
2D-DCT & DWT	100%	100%
1D-DFT	60%	99%
1D-DFT & DWT	95%	100%
2D-DFT	60%	68%
2D-DFT & DWT	100%	79%
DST	60%	95%
DST & DWT	94.4%	98%

Table 5
Comparison between the proposed models and the state-of-the art methods. Moreover, the proposed model can be utilized by a hardware implementation. This trend needs a special type of IC testing (Ali et al., 2009).

Model	Year	Description	Accuracy (%)	Testing Time Min. : sec.
Proposed	2020	ConvLSTM + 1D-DCT + DWT	100	0:1.815
		ConvLSTM + 2D-DCT + DWT	100	0:1.981
		ConvLSTM + 1D-DFT	99	0:2.098
		ConvLSTM + 1D-DFT + DWT	100	0:2.132
		ConvLSTM + DST	95	0:1.572
		ConvLSTM + DST + DWT	98	0:2.323
(Al Azrak et al., 2020)	2020	CNN	100	0:14
(Nishanth and Karthik, 2015)	2020	CNN + 1D-DCT + DWT	90	0:20
		CNN + 2D-DCT + DWT	100	0:22
		CNN + 2D-DFT + DWT	100	0:25
(Amerini et al., 2011)	2011	SIFT + Keypoint Vector Construction	96	24:13
(Costanzo et al., 2014)	2014	SIFT + Keypoint Removal and Injection	97	17:05
(Mishra et al., 2013)	2013	SURF + HAC	85	0:2.85
(Kaur et al., 2015)	2015	Simulative Comparison	95	N/A
(Elaskily et al., 2018)	2019	ROI + Correlation	99	2:48
(Wankhade et al., 2019)	2020	HDBSCAN	98.2	N/A

trigometric transformation technique to reduce the system complexity. Several trigometric transformation techniques were adopted in order to obtain the optimum performance. The simulation results reveal that the proposed model shows a high performance prior to image classification and distinguishes between original and tampered images. In addition, the proposed model achieves an accuracy of 100%. Hence, it can be considered as an efficient CMFD system in IoT technology.

Availability of data and material

The datasets generated during and analysed during the current study are available from the corresponding author upon reasonable request.

Authors' contributions

Ahmed Seddik and Ahmed A. Abd El-Latif developed the idea of the study, participated in its design and coordination and helped to draft the manuscript. Yassine Maleh and Brij B. Gupta contributed to the acquisition and interpretation of data. Ghada M. El Banby, Ashraf A. M. Khalaf and Fathi E. Abd El-Samie provided critical review and substantially revised the manuscript. All authors commented on previous versions of the manuscript and all authors read and approved the final manuscript.

Declaration of Competing Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at 10.1016/j.techfore.2022.121555

References

Al Azrak, F.M., Sedik, A., Dessouky, M.I., Banby, E., M, G., Khalaf, A.A., Elkorany, A.S., El-Samie, F.E.A., 2020. An efficient method for image forgery detection based on trigonometric transforms and deep learning. Multimedia Tools and Applications 79 (25), 18221–18243.

Alghamdi, A., Hammad, M., Ugail, H., Abdel-Raheem, A., Muhammad, K., Khalifa, H.S., Ahmed, A., 2020. Detection of myocardial infarction based on novel deep transfer learning methods for urban healthcare in smart cities. Multimedia tools and applications 1–22.

Ali, L., Sidek, R., Aris, I., Ali, M.A.M., 2009. Design of a testchip for low cost ic testing. Intelligent Automation & Soft Computing 15 (1), 63–72.

AlZu'bi, S., Hawashin, B., Mujahed, M., Jararweh, Y., Gupta, B.B., 2019. An efficient employment of internet of multimedia things in smart and future agriculture. Multimedia Tools and Applications 78 (20), 29581–29605.

Amerini, I., Ballan, L., Caldelli, R., Bimbo, A.D., Serra, G., 2011. A sift-based forensic method for copy–move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security 6, 3.

Benrhouma, O., Hermassi, H., El-Latif, A.A.A., S. Belghith, C., 2016. Watermark for blind forgery detection in images". Multimedia Tools and Applications 75, 8695–8718.

Birajdar, G.K., Mankar, V.H., 2013. Digital image forgery detection using passive techniques: a survey. Digital Investigation 10, 226–245.

Box, A., Bilge, H.S., 2016. Copy-move image forgery detection based on lbp and dct, 24, 16–19.

Bustos-Contell, E., Labatut-Serer, G., Ribeiro-Navarrete, S., Climent-Serrano, S., 2019. Beyond subsidies: a study of sustainable public subordinated debt in spain. Sustainability 11 (4), 1049.

Chu, J., Guo, Z., Leng, L., 2018. Object detection based on multi-layer convolution feature fusion and online hard example mining. IEEE Access 6, 19959–19967.

Costanzo, A., Amerini, I., Caldelli, R., Barni, M., 2014. Forensic analysis of sift keypoint removal and injection. IEEE Transactions on Information Forensics and Security 9 (9), 1450–1464.

Elaskily, M.A., Aslan, H.K., Elshakankiry, O.A., Faragallah, O.S., El-Samie, A., E, F., Dessouky, M.M., 2017. Comparative study of copy-move forgery detection techniques. 2017 Intl Conf on Advanced Control Circuits Systems (ACCS) Systems & 2017 Intl Conf on New Paradigms in Electronics & Information Technology (PEIT). IEEE, pp. 193–203.

Elaskily, M.A., Elnemr, H.A., Dessouky, M.M., Faragallah, O.S., 2018. Two stages object recognition based copy-move forgery detection algorithm. Multimedia Tools and Applications.https://doi.org/10.1007/s11042-018-6891-7

Elaskily, M.A., Elnemr, H.A., Sedik, A., Dessouky, M.M., et. al, G.M.E.B., 2020. A novel deep learning framework for copy-moveforgery detection in images. Multimedia Tools and Applications 1–26.

Elgendy, I.A., Zhang, W.Z., He, H., Gupta, B.B., Abd El-Latif, A.A., 2021. Joint computation offloading and task caching for multi-user and multi-task mec systems: reinforcement learning-based algorithms. Wireless Networks 27 (3), 2023–2038.

Farid, H., 2009. Image forgery detection a survey. IEEE Signal Processing Magazine 26 (2), 16–25.

Fridrich, J., Soukal, D., Lukáš, J., 2003. Detection of copy-move forgery in digital images. In: Cleveland, U.S.A. (Ed.), Proceedings of DFRWS 2003.

Gupta, B.B., Li, K.C., Leung, V.C., Psannis, K.E., Yamaguchi, S., 2021. Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. IEEE/CAA Journal of Automatica Sinica.

Haggag, N.T., Sedik, A., Elbanby, G.M., El-Fishawy, A.S., et. al, A.M.K., 2019. Classification of corneal pattern based on convolutional lstm neural network. Menoufia Journal of Electronic Engineering Research, 28(ICEEM2019-Special Issue) 158–162.

Hosny, K.M., Hamza, H.M., Lashin, N.A., 2018. Copy-move forgery detection of duplicated objects using accurate pcet moments and morphological operators. The Imaging Science Journal 66 (6), 330–345.

Hosny, K.M., Hamza, H.M., Lashin, N.A., 2019. Copy-for-duplication forgery detection in colour images using qpcetms and sub-image approach. IET Image Processing 13, 1437–1446.

Jing, H., He, X., Han, Q., El-Latif, A.A.A., Niu, X., 2014. Saliency detection based on integrated features. Neurocomputing 129, 114–121.