Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.025766
Article

Tech Science Press

Metaheuristics with Optimal Deep Transfer Learning Based Copy-Move Forgery Detection Technique

C. D. Prem Kumar[1,*] and S. Saravana Sundaram[2]

[1]Department of Information Technology, Hindusthan College of Engineering and Technology, Coimbatore, 641032, Tamilnadu, India
[2]Department of Electrical and Electronics Engineering, Hindusthan College of Engineering and Technology, Coimbatore, 641032, Tamilnadu, India
*Corresponding Author: C. D. Prem Kumar. Email: premk.research@gmail.com
Received: 03 December 2021; Accepted: 23 January 2022

Abstract: The extensive availability of advanced digital image technologies and image editing tools has simplified the way of manipulating the image content. An effective technique for tampering the identification is the copy-move forgery. Conventional image processing techniques generally search for the patterns linked to the fake content and restrict the usage in massive data classification. Contrastingly, deep learning (DL) models have demonstrated significant performance over the other statistical techniques. With this motivation, this paper presents an Optimal Deep Transfer Learning based Copy Move Forgery Detection (ODTL-CMFD) technique. The presented ODTL-CMFD technique aims to derive a DL model for the classification of target images into the original and the forged/tampered, and then localize the copy moved regions. To perform the feature extraction process, the political optimizer (PO) with Mobile Networks (MobileNet) model has been derived for generating a set of useful vectors. Finally, an enhanced bird swarm algorithm (EBSA) with least square support vector machine (LS-SVM) model has been employed for classifying the digital images into the original or the forged ones. The utilization of the EBSA algorithm helps to properly modify the parameters contained in the Multiclass Support Vector Machine (MSVM) technique and thereby enhance the classification performance. For ensuring the enhanced performance of the ODTL-CMFD technique, a series of simulations have been performed against the benchmark MICC-F220, MICC-F2000, and MICC-F600 datasets. The experimental results have demonstrated the improvised performance of the ODTL-CMFD approach over the other techniques in terms of several evaluation measures.

Keywords: Copy move detection; image forgery; deep learning; machine learning; parameter tuning; forensics

1 Introduction

With the advancement in the imaging techniques, digital images have become a concrete data source. In the meantime, a considerable amount of image editing mechanisms have placed the authenticity of the

images in danger [1]. An objective behindhand image forgery has implemented the manipulation in such a way that it appears to be difficult to view with a naked eye and apply this creation for the malware purposes [2]. However, the forensic investigation has identified the tigers termed as the "paper tigers" [3]. In the same way, in 2008, official images of four Iranian ballistic weapons were proved to be forged as one of the missiles was exposed to be counterfeited [4]. Hence, methods that could guarantee the integrity of images particularly from the evidence centred application are thus required. Recently, the digital image forensics sector has emerged as an interesting field of research that defines the evidence of forgery from that of the digital image [5]. The main objective of digital image forensics is to examine the existence of forgeries in the concerned images by means of employing the passive or active (blind) approaches. The active methodologies such as the digital signatures and the watermarking strategies depend on the data embedded a priori in the image. But, the inaccessibility of the data might restrict the use of active approaches in real life [6]. Therefore, the passive methodologies have been utilized for authenticating the images that don't need any previous knowledge about them [7]. Image forgery technique consists of image re-sampling, Copy Move forgery, and Image splicing methods respectively [8]. The only objective of the copy-move forgery is to bring further details in the image that wasn't present initially. This forgery approach can be employed for covering the new data of the images by pasting the copied parts over it. This processing in the image changes the message reflected by the image [9]. Mostly, these transformed images would be applied in the courts of law as an evidence for proving the innocent as guilty. The recognition of copy move image forgery is not an easier task as the copied part is from the original image, hence the features such as; texture, colour, and noise patterns appears to be suitable for the remaining images. Along with this, some post-processing operation could also be employed to the copied segment before pasting it to original image that would make the forgery detection difficult. Different approaches for the copy-move forgery detection have been explained in this work [10].

This study has developed an optimal deep transfer learning based copy move forgery detection (ODTL-CMFD) technique for classifying the target images into the original and the forged/tampered followed by the localization of the copy moved regions. Besides, the ODTL-CMFD technique involves the design of the political optimizer (PO) with the Mobile Networks (MobileNet) model for generating a set of useful vectors. Moreover, an enhanced bird swarm algorithm (EBSA) with least square support vector machine (LS-SVM) model has been applied to the classification process. The parameters (kernel and penalty variables) involved in the LS-SVM model can be adjusted by the use of EBSA. The performance validation of the ODTL-CMFD technique has been carried out using the benchmark MICC-F220, MICC-F2000, and MICC-F600 datasets.

2 Literature Survey

Huang et al. [11], proposed a key point-based image forensics method based on the super pixel segmentation and the Helmert transformation algorithms. The primary objective was to identify the CMFD images and attain the forensic data. Initially, the descriptors and the key points were extracted by utilizing the SIFT approach. Next, based on the descriptors, the matching pair was attained by evaluating the similarities among the key points. Then, this matching pair was grouped based on the spatial distance and the geometric constraint through the Helmert transformation for attaining the coarse forgery region. Later, the isolated areas or the mistakes were removed and the coarse forgery region was well refined. In Meena et al. [12], a strong copy-move image forgery approach with that of the Gaussian-Hermite Moment (GHM) has been proposed. The presented strategy splits the input images into over-lapping blocks of fixed sizes and removes the GHM from the entire set of blocks. A similar block matching can be performed by arranging the individual features lexicographically. In Jindal [13], Image forgery was localized and detected by utilizing the semantic segmentation and the Deep Convolutional Neural Network (DCNN) system. Color illumination was employed for colouring the map after the completion

of the pre-processing stage. For training VGG-16, the DCNN-Transfer Learning (TL) method was employed. This technique categorizes the image pixels with that of the forgeries. This categorized image with the colour pixel labels were trained by utilizing the semantic segmentation for limiting the forged pixels. Goel et al. [14], proposed a DL based passive CMFD method which employs a Convolutional Neural Network (CNN) for categorizing the images as forged and original. The CNN method extracts the multi scale features using the distinct kernel sizes. Then, the Combination of the extracted multi scale features was implemented for achieving better recall, accuracy, and precision scores. Abbas et al. [15] aims at utilizing the two advanced DL methods; MobileNetV2 and Smaller VGGNet (inspired from VGGNet). Both these methods appear as time and Eco-friendly DL architectures for detecting the digital image forgeries on the embedded devices. After the completion of a comprehensive review, a modified form of MobileNetV2 that appears to be very efficient on the CMFD that caters for the inconsistencies performed post-forgery was considered. Elaskily et al. [16] examined a novel technique for the CMFD based techniques mainly on the DL approach. The presented method was based on the utilization of the Convolutional Long Short Term Memory (CovLSTM) and the CNN systems. This approach extracts the image features by a sequential number of Convolutional (CNV), ConvLSTM, pooling layers, and matching features. The use of deep learning-based extractors instead of the traditionally handmade ones were considered as an alternative to the more traditional approach. Conventional forensic detectors, on the other hand, are often not real-world accurate in a number of ways, such as the feature extraction strength and the answer to tampering location.

3 The Proposed System

In this study, an effective ODTL-CMFD technique has been developed for the detection and classification of digital images. The ODTL-CMFD technique intends to accomplish the classification of the target images into the original and the forged/tampered using different sub processes such as the MobileNet based feature extraction, the PO based hyper parameter tuning, the LS-SVM based classification, and the EBSA based parameter optimized. Fig. 1 shows the flow of the proposed system.

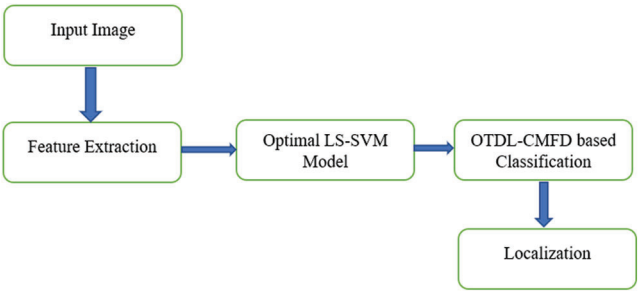

Figure 1: Flow of the proposed system

The detailed functioning process of these modules have been elaborated in the following sections.

3.1 Feature Extraction Using PO with the MobileNet Model

During the feature extraction procedure, the MobileNet model would be applied for deriving a collection of the feature vectors. The CNN generally comprises of the convolution, pooling, and the fully connected (FC) layers [17]. Primarily, the features would be removed by more than one convolutional and a pooling layer. Afterwards, the individual feature maps in the ending convolutional layer would be changed from the 1D vector to the FC. Eventually, the resultant layer would classify the n input images. The network would then alter the weight parameter as the BP and minimize the square variance amongst the classifier

outcomes and the predictable outcomes. The neuron in all the layers have been ordered in the 3 dimensional formats: width, height, and depth, whereas the width and the height represent the size of the neurons, and the depth indicates the channel amount of the input picture or the amount of the input feature maps. The framework dependent upon the convolution and the pooling layers has enhanced the robustness of the network model. The CNN has been obtained deeper with that of the multilayer convolutional. With the amount of layers improving, the features attained with learning have been further developed globally. The global feature map that has been learned at the end can be converted to vectors for linking the FC layer. The MobileNet comprises of a lesser framework, minimum computation, and superior precision that can be utilized at the mobile terminals and the embedding devices [18]. According to the depth wise separable convolutional, MobileNets utilize 2 global hyper parameters for maintaining a balance between the efficacy and the accuracy levels. Essential knowledge of the MobileNet is decomposed of convolutional kernels. By means of utilizing the depth wise separable convolutional, the typical convolutional has been observed to be decomposed as the depth wise convolutional and the point wise convolutional with a 1×1 convolutional kernel. The depth wise convolutional filter has been found to carry out the convolutional for all the channels, and a 1×1 convolutional has been utilized for combining the outcomes of the depth wise convolutional layers. During this manner, N typical convolutional kernels have been modified as the M depth wise convolutional kernels and the N pointwise convolutional kernels. The typical convolution filter joins the input with that of a novel group of outputs, but the depthwise separable convolutional separates an input to 2 layers, one appears to be the filter and the other would be merged suitably.

In addition, the hyper parameters of the MobileNet model can be optimally adjusted by the use of the PO. The PO algorithm is a metaheuristic optimization approach presented in 2020 and is dependent on the multiphase political approach [19]. This PO method stimulates the performance of the politician for achieving the ultimate objective of the optimized. PO implements five sequences of stages for enhancing the provided problem. Similar to the other metaheuristic approaches, the process can be initiated by the population initialization attribute P of size NP. Every row under the population comprises of the number of constituencies and the political parties. The number of input parameters of the problem has been represented by D.

$$P = \{P_{i,1},\ \ P_{i,2} \ldots P_{i,D}\},\ \ i = 1,\ 2,\ \ \ldots NP \tag{1}$$

Furthermore, the party member appear to be a political solution that acts as a selective candidate:

$$\begin{aligned} C &= \{\ C_1,\ \ C_2,\ \ \ldots C_n) \\ C_j &= \{P_i^j,\ P_2^j,\ \ \ldots P_n^j\} \end{aligned} \tag{2}$$

As previously mentioned, “n” amount of constituencies have been assumed here, where “n” represents the total number of parties competing from all the constituencies C. The optimal member of the party-based fitness has been assumed to be the leader of the party. The process involved in the selection of the party leader has been demonstrated below:

$$q = arg\min\ f(P_i^j),\ \forall i \in \{1,\ 2,\ 3,\ \ \ldots n\} and\ 1 \le j \le n \tag{3}$$

$$P_i^* = P_i^q$$

In which $P^* = \{P_1^*,\ P_2^*,\ \ \ldots,\ \ P_n^*\}$ denotes the group of the individual political party leaders. Where C_i^* indicates the constituency i won by the candidate, the group of the winning candidate’s procedure, the parliamentarian C^*, has been represented below:

$$C^* = \{C_1^*,\ C_2^*,\ \ldots,\ C_n^*\} \tag{4}$$

In the Election Campaigning stage, every candidate can enhance their majority by assuming the following aspects (1) influencing the constituency members by mentioning about the leader of the party and by itself, (2) candidate can learn from the former elections, and (3) by improving the relative analysis with the constituency winner. The campaigning of the candidate can follow these 3 stages and update their location with that of the preceding location, that is, when the fitness of the candidate is enhanced, the location can be upgraded by utilizing Eq. (5); or else, it can be upgraded by utilizing Eq. (6):

$$p_{i,k}^j(t+1) = \begin{cases} m^* + rand \cdot (m* - p_{i,k}^i(t)), & if\ p_{i,k}^i(t-1) \le p_{i,k}^i(t) \le m^*\ or\ p_{i,k}^i(t-1) \ge p_{i,k}^i(t) \ge m^* \\ m^* + (2 \times rand - 1) \cdot |m* - p_{i,k}^j(t)|, & if\ p_{i,k}^j(t-1) \le m^* \le p_{i,k}^j(t) or\ p_{i,k}^j(t-1) \ge m^* \ge p_{i,k}^j(t) \\ m^* + (2 \times rand - 1) \cdot |m* - p_{i,k}^j(t-1)|, & if\ m^* \le p_{i,k}^j(t-1) \le p_{i,k}^j(t) or\ m^* \ge p_{i,k}^j(t-1) \ge p_{i,k}^j(t) \end{cases} \tag{5}$$

$$p_{i,k}^i(t+1) = \begin{cases} m^* + (2 \times rand - 1) \cdot |m* - p_{i,k}^i(t)|, & if\ p_{i,k}^i(t-1) \le p_{i,k}^i(t) \le m^*\ or\ p_{i,k}^i(t-1) \ge p_{i,k}^i(t) \ge m^* \\ p_{i,k}^i(t-1) + rand(p_{i,k}^i(t) - p_{i,k}^i(t-1)), & if\ p_{i,k}^i(t-1) \le m^* \le p_{i,k}^i(t) or\ p_{i,k}^i(t-1) \ge m^* \ge p_{i,k}^i(t) \\ m^* + (2 \times rand - 1) \cdot |m* - p_{i,k}^i(t-1)|, & if\ m^* \le p_{i,k}^i(t-1) \le p_{i,k}^i(t)\ or\ m^* \ge p_{i,k}^i(t-1) \ge p_{i,k}^i(t) \end{cases} \tag{6}$$

In the party switching stage, a member of the party P_i^j can be elected with respect to the adoptive variable λ and can be swapped to another party P_r possessing the minimum fit member P_r^q. The index q can be calculated by using the following relationship,

$$q = \ \text{argmax}\ f(p_r^j),\ \ 1 \le j \le n \tag{7}$$

At the election stage, a candidate is supposed to selectively win according to the fitness as follows

$$q = \ \text{argmin}\ f(p_r^j),\ \ 1 \le j \le n \tag{8}$$

$$c_j^* = p_q^j \tag{9}$$

Now, the candidate can be stated as the winner of the constituency by means of upgrading the party leader. During the parliament affairs phase, the government can be formed after the election process. The leader of the parliamentarians and that of the party appears to be categorical; every parliamentarian can upgrade their location by electing the other parliamentarians when there is an enhancement in the fitness level.

3.2 Copy Move Detection Using the Optimal LS-SVM Model

At the time of the copy move detection process, the LS-SVM technique had been used for classifying the target images into the original and the forged/tampered ones. The LSSVM is a well-arranged ML approach dependent upon the statistical learning methodology presented by Vapnik [20]. The LSSVM resolves the high dimension non-linear and the local minimal issues effectively. It can be developed by the SVM technique with 2 additional features. Primarily, the inequality constraint by the equality constraint and secondly it transfers the 2 programming issues to the linear formulas directly. These features have been found to speed up the calculation time of the LSSVM on the SVM technique. The learning procedure of the LSSVM has been illustrated below. The group of instances data sets has been represented as: ($x_i y_i$), $i = 1, 2, \ldots, n$, where x_i refers to the i^{th} predictor variables and the $y_i i^{th}$ represents the outcome variable. Eq. (10) illustrates the linear regression function.

$$f(x) = w^T g(x) + b \tag{10}$$

where w, b defines the weight vector as well as the deviation correspondingly.

The optimized regression function can be attained by utilizing Eq. (11).

$$\min \ J(\omega, \ \zeta) = \frac{1}{2} w^T w + \frac{1}{2} C \sum_{i=1}^{m} \zeta^2 \tag{11}$$

where C, ζ_i signifies the error penalty as well as the slack variable correspondingly. The kernel purpose chosen appears to be dependent upon the Mercer's condition:

$$K(x_i, \ x_j) = \phi(x_i)^T \phi(x_j) \tag{12}$$

The last LSSVM technique has been computed using Eq. (13).

$$f(x) = \sum_{i=1}^{m} a_i K(x, \ x_i) + b \tag{13}$$

where a_i implies the Lagrangian multiplier.

The fundamental tuning parameter of the LSSVM technique appears to be the kernel parameter and the penalty C. This analysis possesses the Radial Basis Function (RBF) as the kernel function for training the method. The parameters (kernel and penalty variables) involved in the LS-SVM model can be adjusted by the use of the EBSA. BSA [20] is an effective optimized technique with features of easy procedure, optimum extensibility, and so on. Here N virtual bird flies and forage to food has been assumed here. Supposing $x_i^t (i \in [1, \ 2, \ \ldots, \ N])$ reveal the place of i^{th} bird at t. The bird performances can be explained as:

Foraging performance has been defined as:

$$x_{i,j}^{t+1} j = x_{i,j}^t + (p_{i,j} - x_{i,j}^t) \times C \times rand(0, \ 1) + (g_{i,j} - x_{i,j}^t) \times S \times rand(0, \ 1) \tag{14}$$

Vigilance performance has been determined as:

$$x_{i,j}^{t+1} = x_{i,j}^t + A_1 (mean_j - x_{i,j}^t) \times rand(0, \ 1) + A_2 (p_{i,j} - x_{i,j}^t) \times rand(-1, \ 1) \tag{15}$$

where, A_1 and A_2 are defined mathematically as:

$$A_1 = a_1 \times \ \exp \left(- \frac{p_{Fit_i}}{sumFit + \varepsilon} \times N \right) \tag{16}$$

$$A_2 = a_2 \times \ \exp \left(\left(\frac{p_{Fit_l} - p_{Fit_k}}{|p_{Fit_k} - p_{Fit_l}| + \varepsilon} \right) \times \frac{N \times p_{Fit_k}}{sumFit + \varepsilon} \right) \tag{17}$$

a_1 and a_2 can be the constants from zero and two. ε refers to the smaller constant. Flight performance has been defined as:

$$x_{i,j}^{t+1} = x_{i,j}^t + randn(0, \ 1) \times x_{i,j}^t \tag{18}$$

$$x_{i,j}^{t+1} = x_{i,j}^t + (x_{k,j}^t - x_{i,j}^t) \times FL \times randn(0, \ 1) \tag{19}$$

where FL is in 0 and 2. The chaotic method is a property of sensitivity pertaining to the primary condition. The chaotic signal created by the deterministic methods appears to be the quality of the genus-arbitrariness. Its curve has been defined as the primary value and the chaos mapping parameters. The logistic mapping was

utilized extremely practically. The logistic chaotic method is a complex dynamical performance, it could be explained as a variance as in Eq. (20).

$$\lambda_{i+1} = \mu \times \lambda_i \times (1 - \lambda_i) \tag{20}$$

$\lambda \in [0, 1]$, $i = 0, 1, 2, \ldots$, μ is in 1 and 4. According to the studies, μ implies the nearby 4, λ refers to the adjacent of the average distribution amongst the zero and the one. In the meantime, the method was entirely chaotic as μ is in 4. A primary population appears to be a vital part of the intelligently optimized technique that controls the convergence rate and the last solution quality [21]. The logistic chaotic mapping was utilized for initializing the population that generates the complete utilization of the data solution space for the purpose of improving the effectiveness of the technique.

The EBSA approach develops a Fitness Function (FF) for obtaining the enhanced classifier efficiency. It defines a positive integer for representing the optimum efficiency of the candidate solution. During this case, the minimal value of the classification error rate assumes the FF, as provided in Eq. (21). An optimum solution appears to be a lesser error rate and the worst solution gains a higher error rate.

$$fitness(x_i) = ClassifierErrorRate(x_i) = \frac{number\ of\ misclassified\ i,\ ages}{Total\ number\ of\ images} * 100 \tag{21}$$

4 Performance Validation

In this section, the simulation analysis of the ODTL-CMFD technique has been accomplished using the Python 3.6.5 tool. Besides, the results have been inspected under three benchmark datasets such as the MICC_F220, the MICC_F2000, and the MICC_F600 datasets [22]. Some of the sample test images have been displayed in Fig. 2.

Figure 2: Sample images

Fig. 3 illustrates the sample visualization result analysis of the ODTL-CMFD technique. The first column images portray the original input images and the forged images have been depicted in the second

column. Then, the localized forged regions have been showcased in the third column. These figures report the effectiveness of the ODTL-CMFD technique on the detection of the forged regions in the manipulated image.

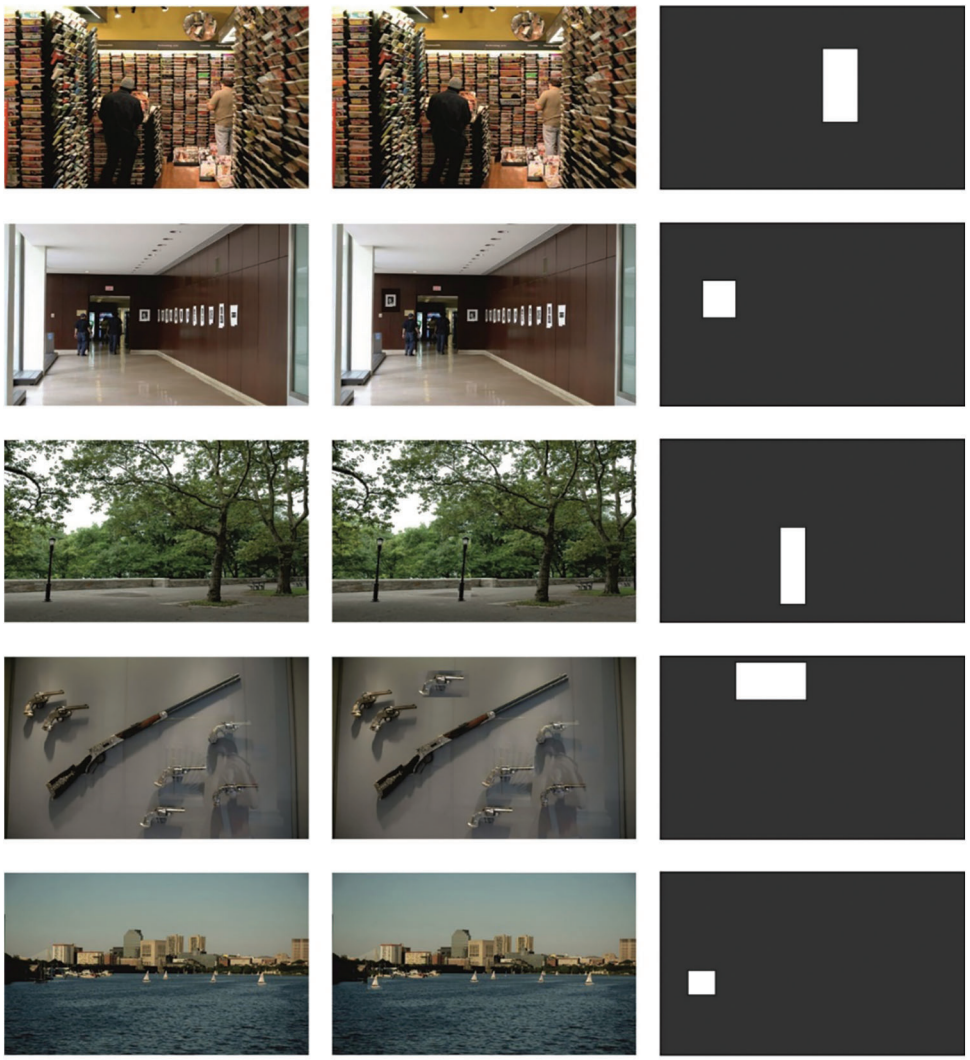

Figure 3: Sample results. a) Original Image b) Forgery Image c) Localization Image

Tab. 1 offers a brief copy move detection performance analysis of the ODTL-CMFD technique under distinct epochs on the MICC_F220 dataset. The experimental values thus point out that the ODTL-CMFD technique has reached the maximum detection performance level under all epochs. For instance, in 10 epochs, the ODTL-CMFD technique has provided accuracy, True positive Rate (TPR_, False Positive Rate (FPR), False Negative Rate (FNR), and True Negative Rate (TNR) of 0.973, 0.955, 0, 0.045, and 1.000. Eventually, with 50 epochs, the ODTL-CMFD technique has attained accuracy, TPR, FPR, FNR, and TNR of 1.000, 0.977, 0, 0.023, and 1.000 respectively.

Table 1: Result analysis of the ODTL-CMFD approach on the MICC_F220 dataset

No. of epochs	Accuracy	Log loss	TPR	FPR	FNR	TNR	Computational Time (CT) (s)
Epoch-10	0.973	0.027	0.955	0.000	0.045	1.000	14.44
Epoch-20	0.990	0.011	0.978	0.000	0.022	1.000	13.85
Epoch-30	0.969	0.031	0.952	0.000	0.048	1.000	13.92
Epoch-40	1.000	0.000	1.000	0.000	0.000	1.000	11.01
Epoch-50	1.000	0.000	1.000	0.000	0.000	1.000	12.41
Average	0.986	0.014	0.977	0.000	0.023	1.000	13.13

The performance analysis of the ODTL-CMFD approach in terms of the training and the validation accuracy under dissimilar epochs on the MICC_F220 dataset has been illustrated in Fig. 4. The figure illustrates the improved performance of the ODTL-CMFD technique with higher values of training and validation accuracy. It is also ensured that the ODTL-CMFD technique has resulted in increased values of validation accuracy compared with that of the training accuracy.

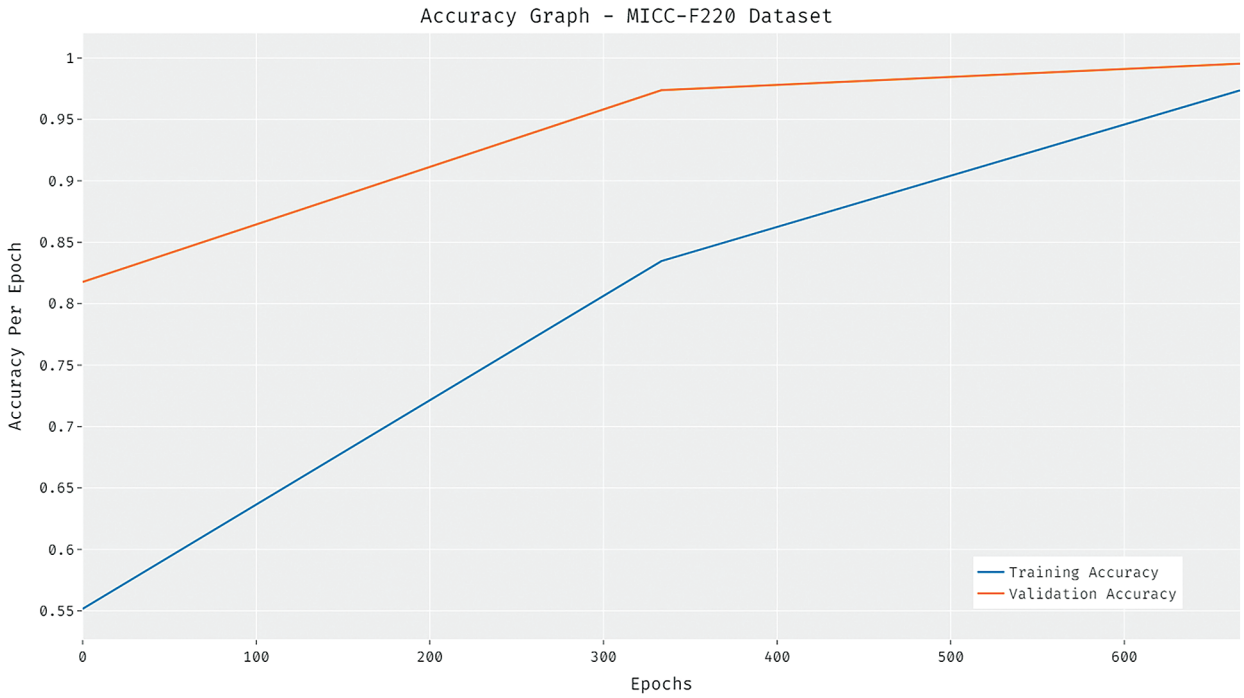

Figure 4: Accuracy analysis of ODTL-CMFD approach on MICC_F220 dataset

Next, the result analysis of the ODTL-CMFD technique with respect to the training and the validation loss under distinct epochs on the MICC_F220 dataset has been illustrated in Fig. 5. The results thus demonstrate that the ODTL-CMFD technique has reached the least training and the validation loss.

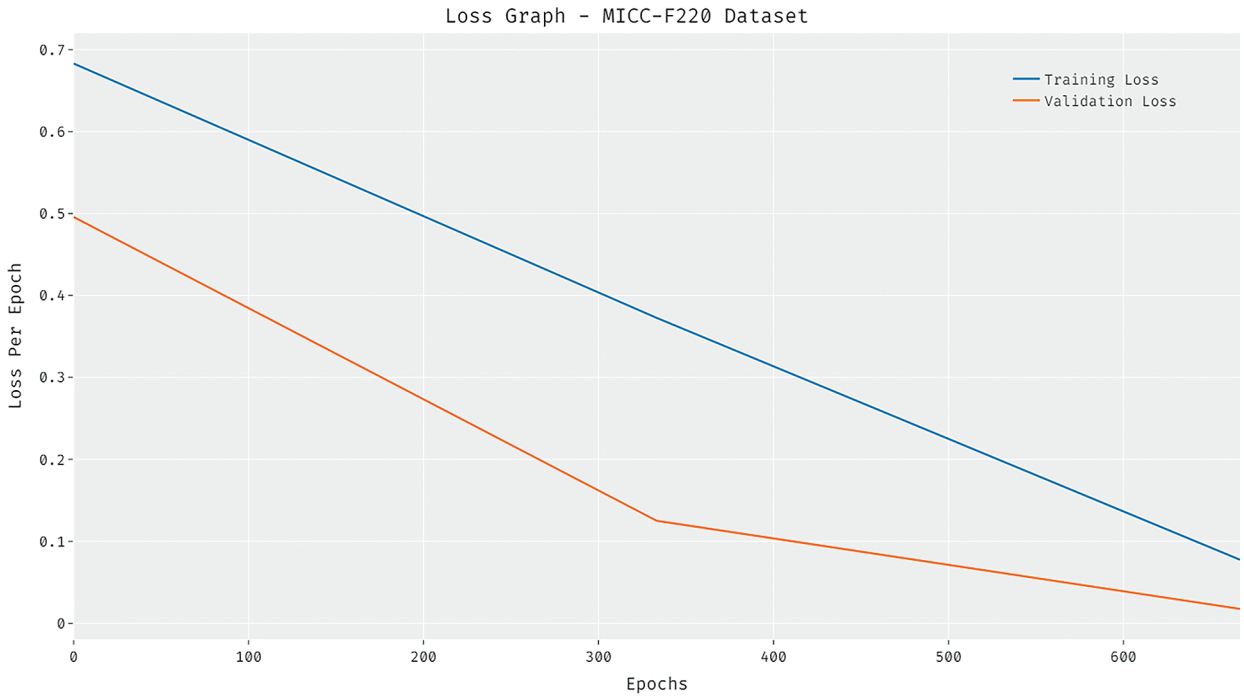

Figure 5: Loss analysis of the ODTL-CMFD approach on the MICC_F220 dataset

Here, an extensive Receiver Operating Characteristics (ROC) analysis of the ODTL-CMFD approach on the MICC_F220 dataset has been portrayed in Fig. 6. The results demonstrate the enhanced classification performance of the ODTL-CMFD approach with the higher ROC of 99.9578 on the test MICC_F220 dataset. Tab. 2 provides a comparative copy move detection performance analysis of the ODTL-CMFD method under varying epochs on the MICC_F2000 dataset. The experimental values thus point out that the ODTL-CMFD approach has attained the maximal detection performance level under all epochs. For instance, in 10 epochs, the ODTL-CMFD methodology has provided accuracy, TPR, FPR, FNR, and TNR of 0.953, 0.938, 0.067, 0.062, and 0.933. Finally, with 50 epochs, the ODTL-CMFD system has attained accuracy, TPR, FPR, FNR, and TNR of 1.000, 1.000, 0, 0, and 0.972 correspondingly.

The performance analysis of the ODTL-CMFD method with respect to the training and the validation accuracy under dissimilar epochs on the MICC_F2000 dataset has been illustrated in Fig. 7. The figure portrays the improved performance of the ODTL-CMFD method with superior values of training and validation accuracy. It can be also stated that the ODTL-CMFD algorithm has resulted in improved values of validation accuracy related to that of the training accuracy. Afterwards, the outcome analysis of the ODTL-CMFD approach in terms of the training and the validation loss under different epochs on the MICC_F2000 dataset has been illustrated in Fig. 8. The results thus demonstrate that the ODTL-CMFD approach has obtained minimum training and validation loss. An extensive ROC analysis of the ODTL-CMFD method on the MICC_F2000 dataset has been displayed in Fig. 9. The outcomes exhibit the improved classification performance level of the ODTL-CMFD approach with the superior ROC of 99.9731 on the test MICC_F2000 dataset.

Tab. 3 suggests a detailed copy move detection performance analysis of the ODTL-CMFD approach under various epochs on the MICC_F600 dataset. The experimental values state that the ODTL-CMFD methodology has achieved a higher detection performance level under all epochs. For instance, in 10 epochs, the ODTL-CMFD approach has offered accuracy, TPR, FPR, FNR, and TNR of 0.946, 0.952,

0.031, 0.049, and 0.969. At last, with 50 epochs, the ODTL-CMFD system has gained accuracy, TPR, FPR, FNR, and TNR of 1.000, 1.000, 0, 0, and 1.000 respectively.

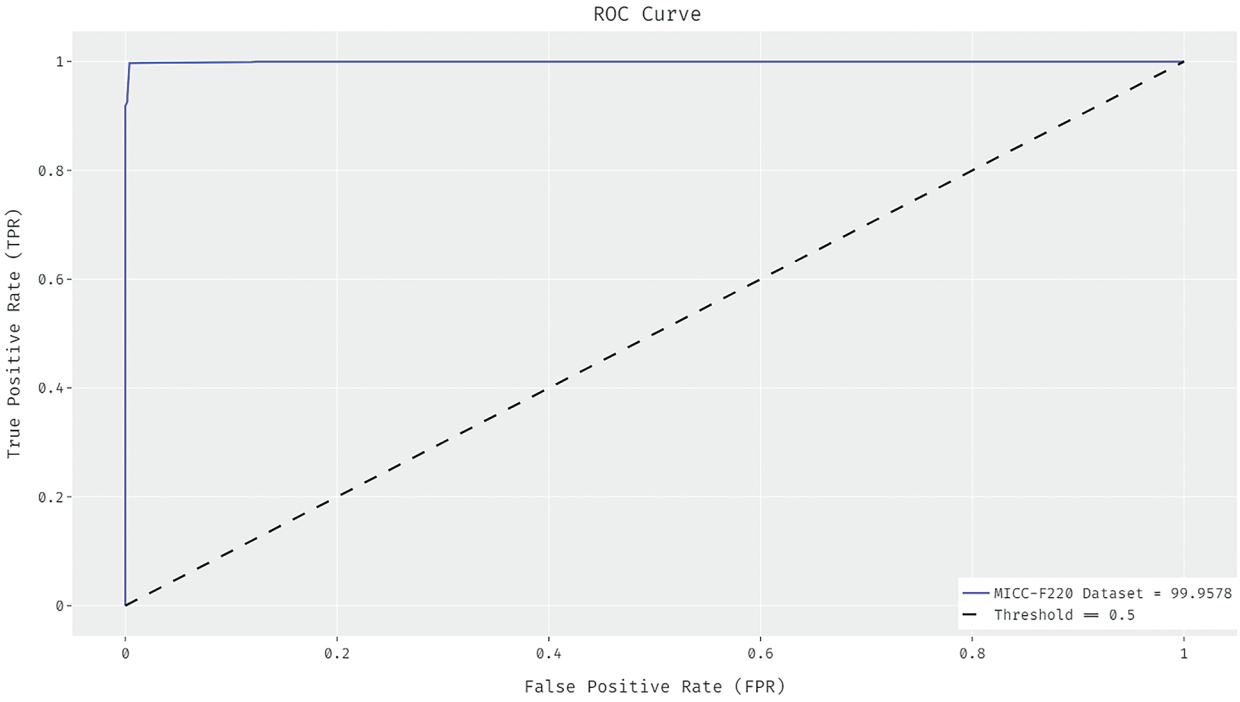

Figure 6: ROC analysis of the ODTL-CMFD approach on the MICC_F220 dataset

Table 2: Result analysis of the ODTL-CMFD approach on the MICC_F2000 dataset

No. of epochs	Accuracy	Log loss	TPR	FPR	FNR	TNR	CT (s)
Epoch-10	0.953	0.047	0.938	0.067	0.062	0.933	96.89
Epoch-20	0.982	0.018	0.973	0.059	0.027	0.941	84.77
Epoch-30	0.997	0.003	0.980	0.012	0.020	0.988	97.39
Epoch-40	1.000	0.000	1.000	0.000	0.000	1.000	66.66
Epoch-50	1.000	0.000	1.000	0.000	0.000	1.000	72.07
Average	0.986	0.014	0.978	0.028	0.022	0.972	83.56

The performance analysis of the ODTL-CMFD system with respect to the training and the validation accuracy under dissimilar epochs on the MICC_F600 dataset has been illustrated in Fig. 10. The figure depicts the increased performance level of the ODTL-CMFD algorithm with higher values of training and validation accuracy. It is also to make sure that the ODTL-CMFD approach has resulted in maximum values of validation accuracy against that of the training accuracy. Then, the outcome analysis of the ODTL-CMFD approach with respect to the training and the validation loss under varying epochs on the MICC_F600 dataset has been presented in Fig. 11. The results thus portray that the ODTL-CMFD method has attained minimal training and validation loss.

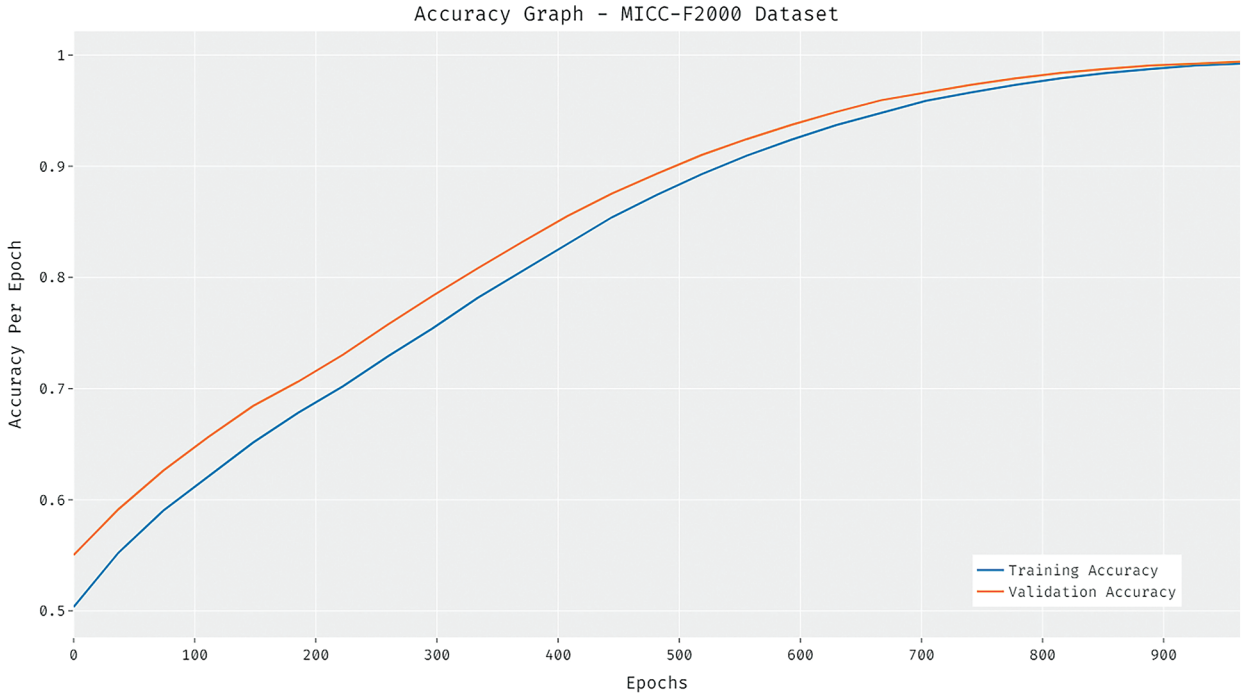

Figure 7: Accuracy analysis of the ODTL-CMFD approach on the MICC_F2000 dataset

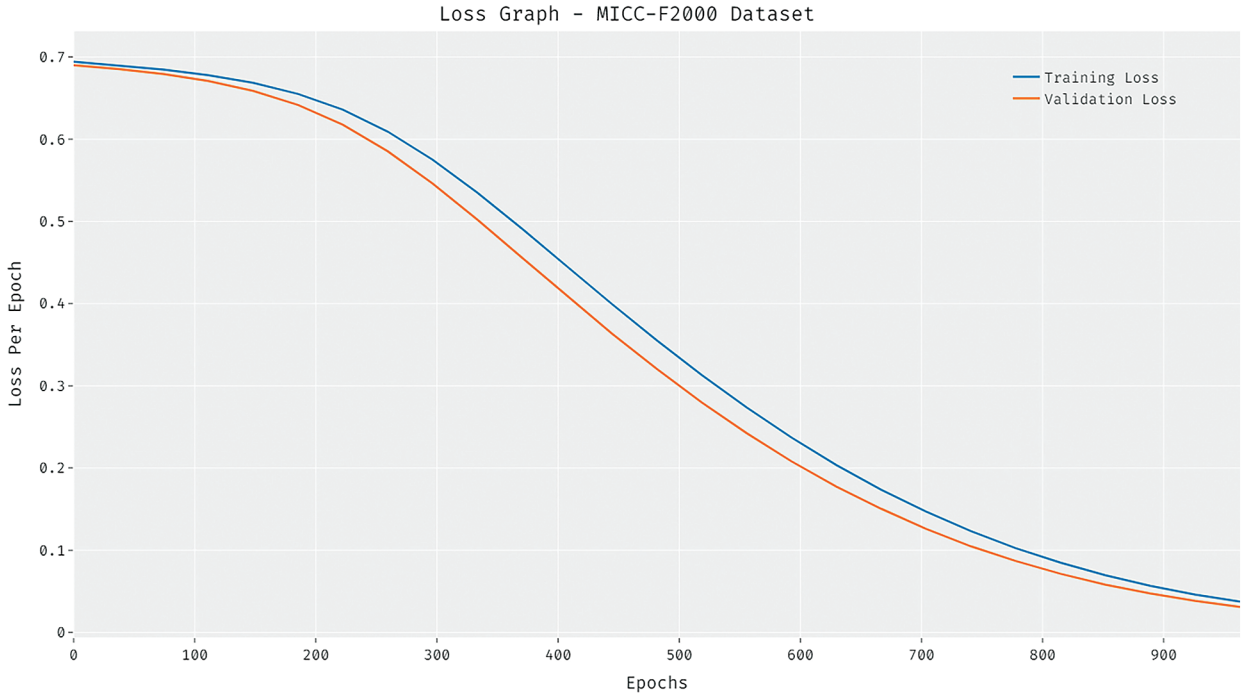

Figure 8: Loss analysis of the ODTL-CMFD approach on the MICC_F2000 dataset

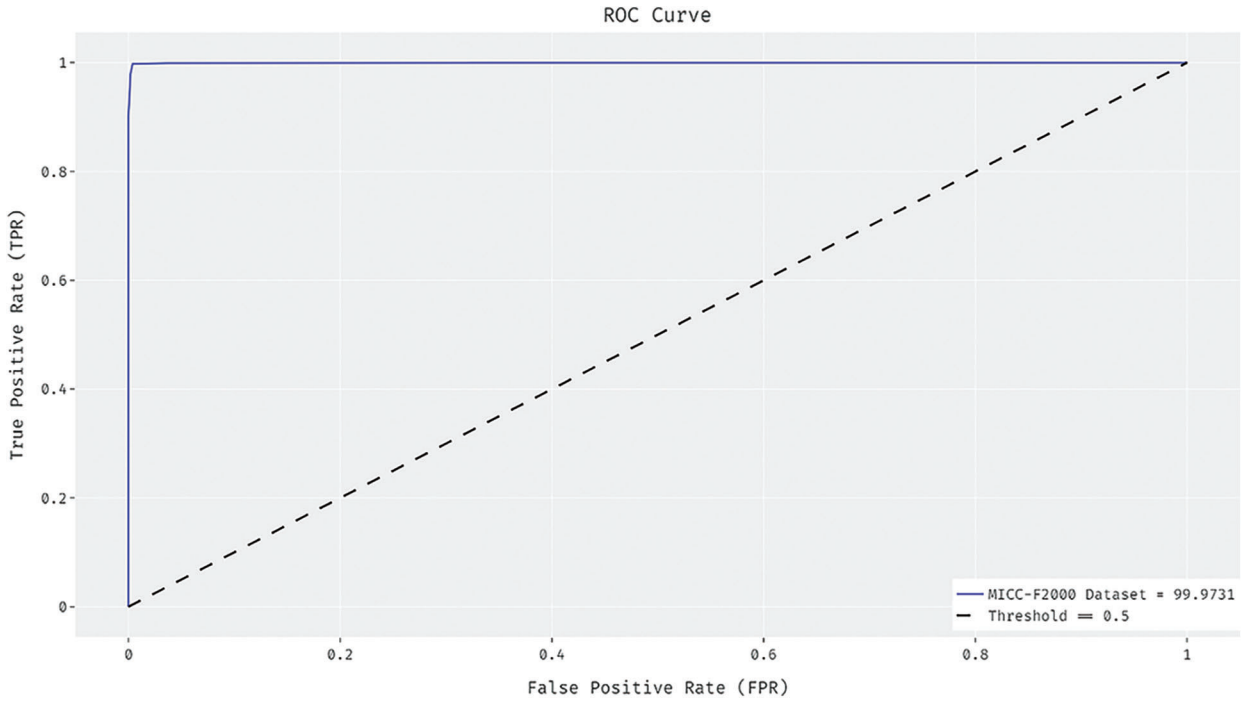

Figure 9: ROC analysis of the ODTL-CMFD approach on the MICC_F2000 dataset

Table 3: Result analysis of the ODTL-CMFD approach on the MICC_F600 dataset

No. of epochs	Accuracy	Log loss	TPR	FPR	FNR	TNR	CT (s)
Epoch-10	0.946	0.054	0.952	0.031	0.049	0.969	30.92
Epoch-20	0.989	0.011	0.969	0.020	0.031	0.980	32.11
Epoch-30	0.981	0.020	0.985	0.015	0.015	0.985	30.91
Epoch-40	1.000	0.000	1.000	0.000	0.000	1.000	18.15
Epoch-50	1.000	0.000	1.000	0.000	0.000	1.000	20.66
Average	0.983	0.017	0.981	0.013	0.019	0.987	26.55

At this time, a wide ROC analysis of the ODTL-CMFD approach on the MICC_F600 dataset has been portrayed in Fig. 12. The outcomes display the improved classification performance level of the ODTL-CMFD methodology with the superior ROC of 99.9979 on the test MICC_F600 dataset.

Finally, the detailed comparative detection performance of the ODTL-CMFD approach takes place using four datasets as in Tab. 4 [23–25]. The experimental values thus portray that the Scale Invariant Feature Transform Technique (SIFTT)-CMFD and SIFTT approaches exhibit least copy move detection performance level whereas the SIFTT approach has reached the moderate classification performance level. However, the ODTL-CMFD technique has resulted in the maximum performance level over the other methods on the test datasets. For instance, with the MICC_F220 dataset, the ODTL-CMFD technique has resulted in the TPR of 100%, FPR of 0%, FNR of 0%, and TNR of 100%. Similarly, on the MICC_F2000 dataset, the ODTL-CMFD technique has gained effective outcomes with the TPR of 100%, FPR of 0%, FNR of 0%, and TNR of 100%. Likewise, the ODTL-CMFD technique has accomplished the maximum performance level on the MICC_F600 dataset.

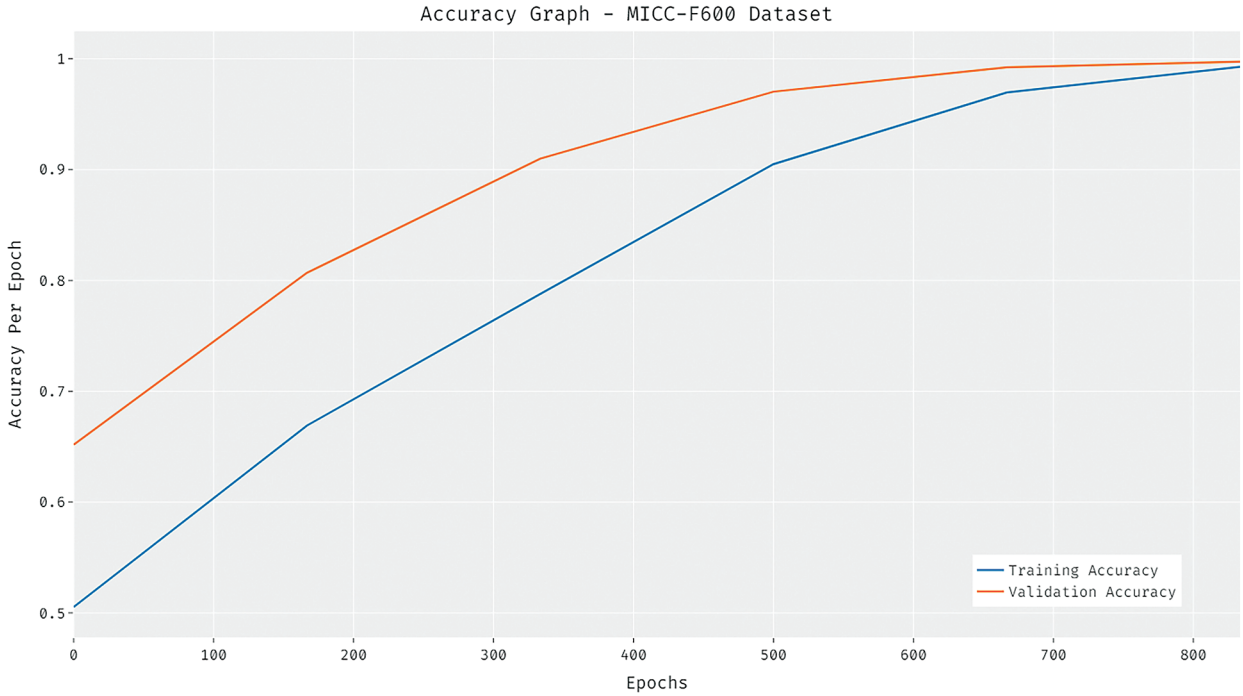

Figure 10: Accuracy analysis of the ODTL-CMFD approach on the MICC_F600 dataset

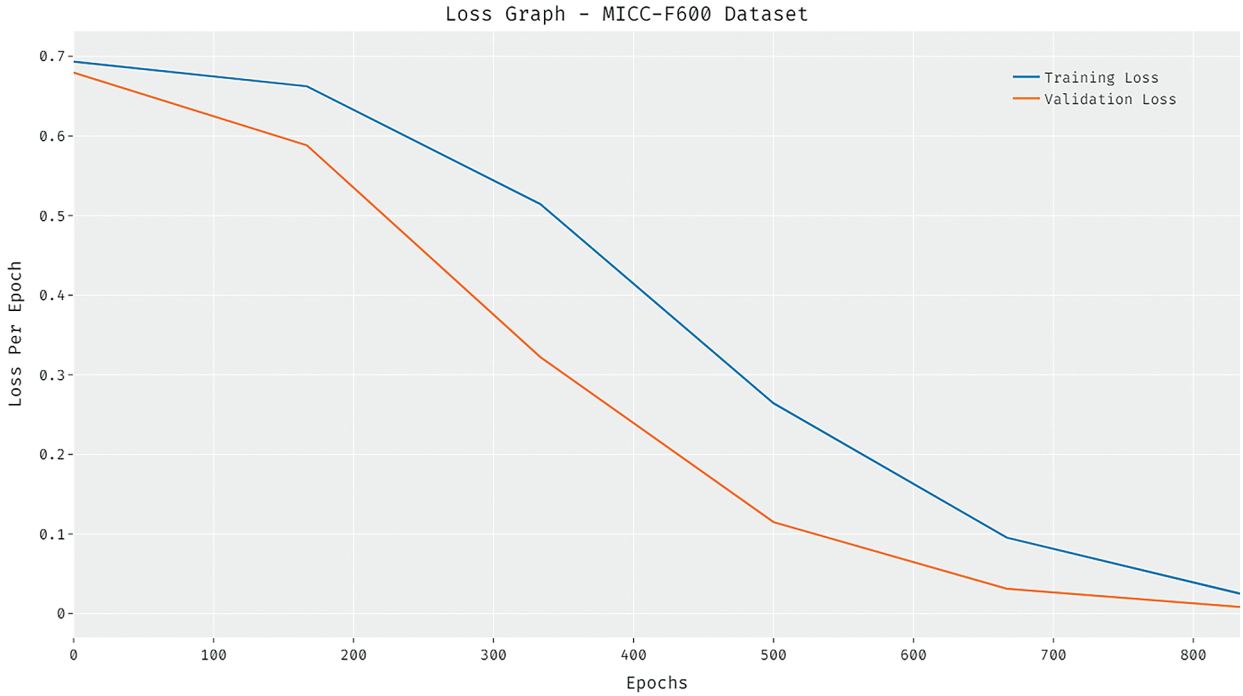

Figure 11: Loss analysis of the ODTL-CMFD approach on the MICC_F600 dataset

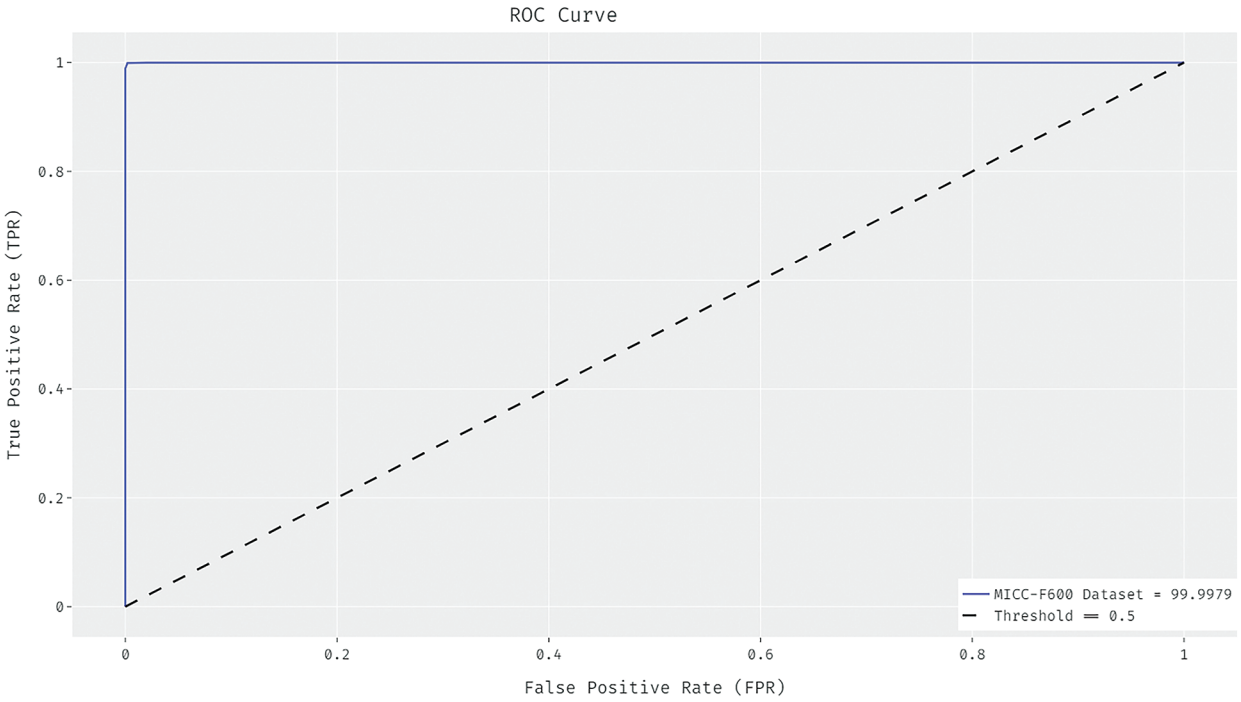

Figure 12: ROC analysis of the ODTL-CMFD approach on the MICC_F600 dataset

Table 4: Comparative analysis of the ODTL-CMFD technique with that of the existing approaches with respect to various measures

Measures	ODTL-CMFD	SIFTT-CMFD	SIFTT	CMFDT
MICC_F220 dataset				
TPR %	100.00	100.00	100.00	100.00
FPR %	0.00	6.00	8.00	1.80
FNR %	0.00	0.00	0.00	0.00
TNR %	100.00	94.00	92.00	98.20
CT (min)	0.187	17.05	24.13	2.48
MICC_F2000 dataset				
TPR %	100.00	94.86	93.42	98.40
FPR %	0.00	9.15	11.61	6.35
FNR %	0.00	5.14	6.58	1.60
TNR %	100.00	90.85	88.39	93.65
CT (min)	1.201	180.15	312.18	46.58
MICC_F600 dataset				
TPR %	100.00	81.60	69.20	94.50
FPR %	0.00	7.27	12.50	11.35
FNR %	0.00	18.40	30.80	5.50
TNR %	100.00	92.73	87.50	88.65
CT (min)	0.303	76.21	115.00	17.37

Fig. 13 provides a clear CT analysis of the ODTL-CMFD technique with the recent methodologies on the test MICC_F220 dataset. The results show that the SIFTT technique has required a higher CT of 24.13 min. At the same time, the SIFTT-CMFD technique has demonstrated a slightly decreased CT of 17.05 min whereas even the reduced CT of 2.48 min has been desired by the CMFDT technique. However, the ODTL-CMFD technique has offered the least CT of 0.187 min. Fig. 14 exhibits a comparative CT analysis of the ODTL-CMFD technique with the recent methods on the test MICC_F2000 dataset. The experimental values thus report that the SIFTT technique has depicted an increased CT of 312.18 min. Moreover, the SIFTT-CMFD technique has established a somewhat reduced CT of 180.15 min whereas even the reduced CT of 46.58 min has been desired by the CMFDT technique. But the ODTL-CMFD technique has surpassed the other techniques with a minimum CT of 1.201 min.

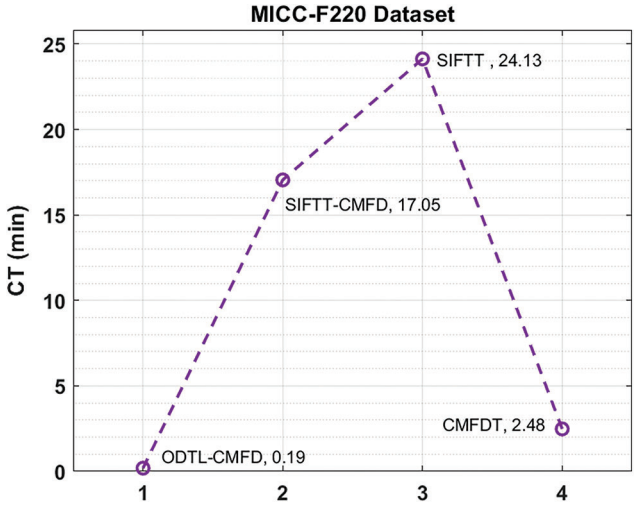

Figure 13: CT analysis of the ODTL-CMFD technique on the MICC_F220 dataset

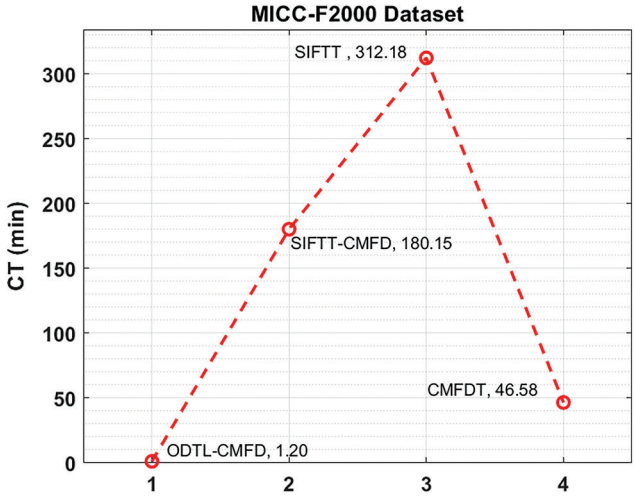

Figure 14: CT analysis of the ODTL-CMFD technique on the MICC_F2000 dataset

Fig. 15 illustrates a detailed CT analysis of the ODTL-CMFD technique with that of the recent methods on the test MICC_F600 dataset. The results thus reveal that the SIFTT technique has demonstrated a superior

CT of 115.00 min. Eventually, the SIFTT-CMFD technique has exhibited a certainly decreased CT of 76.21 min whereas even the reduced CT of 17.37 min has been desired by the CMFDT technique. However, the ODTL-CMFD technique has offered the least CT of 0.303 min.

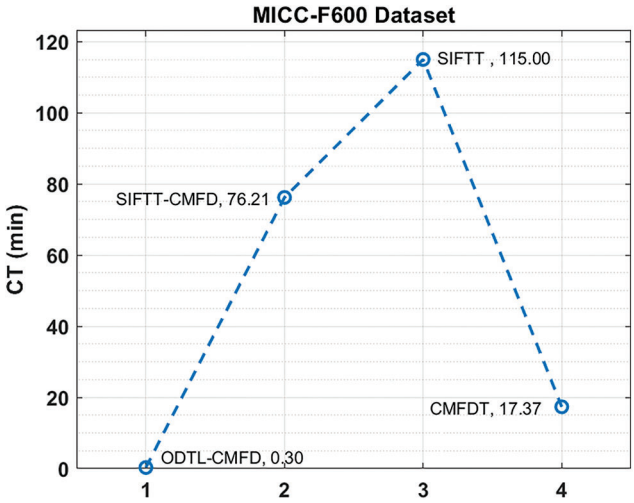

Figure 15: CT analysis of the ODTL-CMFD technique on the MICC_F600 dataset

By looking into the above mentioned results and discussions, it has been confirmed that the ODTL-CMFD technique has the ability to effectively detect and classify the copy move forgery compared with that of the recent methods.

5 Conclusion

This paper has introduced an effective ODTL-CMFD technique for the detection and classification of the digital images. The ODTL-CMFD technique intends to accomplish the classification of the target images into the original and the forged/tampered, followed by the localization of the copy moved regions. In addition, the ODTL-CMFD technique employs the MobileNet based feature extraction and the PO based hyper parameter tuning process. Moreover, the EBSA with the LS-SVM model has been applied for the classification of the images into the actual or the forged images. The performance validation of the ODTL-CMFD technique has been carried out using the benchmark MICC_F220, MICC_F2000, and MICC_F600 datasets. The experimental results thus state the better performance of the ODTL-CMFD technique over the recent approaches with respect to various evaluation measures. Therefore, the ODTL-CMFD technique can be utilized as an effective tool for the copy move forgery detection and classification. In future, the hybrid DL models can be utilized instead of the MobileNet and the LS-SVM models for enhancing the detection performance levels.

Funding Statement: The authors received no specific funding for this study.

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

References

[1] J. Zhao and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic Science International*, vol. 233, no. 1–3, pp. 158–166, 2013.

[2] N. Krawetz, "A pictures worth digital image analysis and forensics," in *Hacker Factor Solutions, Black Hat Briefings*, First Edition, Las Vegas, United States of America, 2007.

[3] F. M. Al_Azrak, A. Sedik, M. I. Dessowky, G. M. El Banby, A. A. Khalaf *et al.,* "An efficient method for image forgery detection based on trigonometric transforms and deep learning," *Multimedia Tools and Applications*, vol. 79, no. 25, pp. 18221–18243, 2020.

[4] A. Thakur and N. Jindal, "Hybrid deep learning and machine learning approach for passive image forensic," *IET Image Processing*, vol. 14, no. 10, pp. 1952–1959, 2020.

[5] S. P. Chalamalasetty and S. R. Giduturi, "Research perception towards copy-move image forgery detection: Challenges and future directions," *International Journal of Image and Graphics*, vol. 21, no. 4, pp. 1–18, 2021.

[6] R. Agarwal and O. P. Verma, "An efficient copy move forgery detection using deep learning feature extraction and matching algorithm," *Multimedia Tools and Applications*, vol. 79, no. 11, pp. 7355–7376, 2020.

[7] Z. J. Barad and M. M. Goswami, "Image forgery detection using deep learning: A survey," in *Proc. IEEE 6th Int. Conf. on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, pp. 571–576, 2020.

[8] M. M. Islam, G. Karmakar, J. Kamruzzaman and M. Murshed, "A robust forgery detection method for copy–Move and splicing attacks in images," *Electronics*, vol. 9, no. 9, pp. 500–1524, 2020.

[9] Y. Zhu, C. Chen, G. Yan, Y. Guo and Y. Dong, "AR-Net: Adaptive attention and residual refinement network for copy-move forgery detection," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6714–6723, 2020.

[10] G. Gani and F. Qadir, "A robust copy-move forgery detection technique based on discrete cosine transform and cellular automata," *Journal of Information Security and Applications*, vol. 54, pp. 102510–102524, 2020.

[11] H. Y. Huang and A. J. Ciou, "Copy-move forgery detection for image forensics using the superpixel segmentation and the helmert transformation," *EURASIP Journal on Image and Video Processing*, vol. 2019, no. 1, pp. 1–16, 2019.

[12] K. B. Meena and V. Tyagi, "A copy-move image forgery detection technique based on Gaussian-hermite moments," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 33505–33526, 2019.

[13] N. Jindal, "Copy move and splicing forgery detection using deep convolution neural network, and semantic segmentation," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 3571–3599, 2021.

[14] N. Goel, S. Kaur and R. Bala, "Dual branch convolutional neural network for copy move forgery detection," *IET Image Processing*, vol. 15, no. 3, pp. 656–665, 2021.

[15] M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O'Neill *et al.,* "Lightweight deep learning model for detection of copy-move image forgery with post-processed attacks," in *Proc. IEEE 19th World Symp. on Applied Machine Intelligence and Informatics (SAMI)*, Herl'any, Slovakia, pp. 125–130, 2021.

[16] M. A. Elaskily, M. H. Alkinani, A. Sedik and M. M. Dessouky, "Deep learning based algorithm (ConvLSTM) for copy move forgery detection," *Journal of Intelligent & Fuzzy Systems*, vol. 40, no. 3, pp. 4385–4405, 2021.

[17] X. B. Meng, X. Z. Gao, L. Lu, Y. Liu and H. Zhang, "A new bio-inspired optimization algorithm: Bird swarm algorithm," *Journal of Experimental & Theoretical Artificial Intelligence*, vol. 28, no. 4, pp. 673–687, 2015.

[18] W. Wang, Y. Hu, T. Zou, H. Liu, J. Wang *et al.,* "A new image classification approach via improved MobileNet models with local receptive field expansion in shallow layers," *Computational Intelligence and Neuroscience*, vol. 2020, no. 8817849, pp. 1–10, 2020.

[19] V. Basetti, S. S. Rangarajan, C. K. Shiva, H. Pulluri and R. Kumar, "Economic emission load dispatch problem with valve-point loading using a novel quasi-oppositional-based political optimizer," *Electronics*, vol. 10, no. 21, pp. 2596–2612, 2021.

[20] D. J. Armaghani, D. Kumar, P. Samui, M. Hasanipanah and B. Roy, "A novel approach for forecasting of ground vibrations resulting from blasting: Modified particle swarm optimization coupled extreme learning machine," *Engineering with Computers*, vol. 37, no. 4, pp. 3221–3235, 2021.

[21] D. Zhang, J. Yang and P. Yang, "An improved chaos bird swarm optimization algorithm," *Journal of Physics: Conference Series*, vol. 1176, no. 2, pp. 1–9, 2019.

[22] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo and G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, 2011.

[23] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, L. D. Tongo *et al.,* "Copy-move forgery detection and localization by means of robust clustering with J-linkage," *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 659–669, 2013.

[24] 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 Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, 2011.

[25] M. A. Elaskily, H. A. Elnemr, A. Sedik, M. M. Dessouky, G. M. E. Banby *et al.,* "A novel deep learning framework for copy-moveforgery detection in images," *Multimedia Tools & Applications*, vol. 79, pp. 19167–19192, 2020.