IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 July 2023, accepted 4 August 2023, date of publication 10 August 2023, date of current version 21 August 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3304237

RESEARCH ARTICLE

Modeling of Reptile Search Algorithm With Deep Learning Approach for Copy Move Image Forgery Detection

MASHAEL MAASHI[1], HAYAM ALAMRO[2], HEBA MOHSEN[3], NOHA NEGM[4], GOUSE PASHA MOHAMMED[5], NOURA ABDELAZIZ AHMED[5], SARA SAADELDEEN IBRAHIM[5], AND MOHAMED IBRAHIM ALSAID[5]

[1]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[2]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 11671, Saudi Arabia
[3]Department of Computer Science, Faculty of Computers and Information Technology, Future University in Egypt, New Cairo 11835, Egypt
[4]Department of Computer Science, College of Science and Art at Mahayil, King Khalid University, Abha 62529, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia

Corresponding author: Gouse Pasha Mohammed (g.mohammed@psau.edu.sa)

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Groups Project under grant number (RGP2/96/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R361), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2023R787), King Saud University, Riyadh, Saudi Arabia. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444).

ABSTRACT Copy-move (CM) forgery is a common type of image manipulation that involves copying and pasting a region within an image to conceal or duplicate content. Detection of such forgeries acts as an important part of digital image forensics. Deep learning techniques, such as convolutional neural networks (CNNs), are employed to extract informative features from images. CNNs are known for their ability to capture complex patterns and structures, making them well-suited for image-related tasks like forgery detection. This paper introduces a reptile search algorithm with a deep transfer learning-based CM forgery detection (RSADTL-CMFD) approach. The presented model uses Neural Architectural Search Network (NASNet) for feature extraction in forgery detection which allows the network to effectively capture relevant and discriminative features from the input images. To enhance the performance of the NASNet model, we employ the reptile search algorithm (RSA) for hyperparameter tuning. This algorithm optimizes the network's hyperparameters, enabling the model to quickly adapt to different forgery detection tasks and achieve superior performance. Finally, extreme gradient boosting (XGBoost) effectively utilizes the extracted features from the deep learning network to classify regions within the image as genuine or manipulated/forged. The experimental result analysis of the RSADTL-CMFD model is tested using benchmark datasets. An extensive comparative study highlighted the enhanced outcomes of the RSADTL-CMFD method over recent techniques.

INDEX TERMS Cybersecurity, image forgery, copy move detection, machine learning, deep learning, parameter optimization.

I. INTRODUCTION

Currently, with the familiarity of digital media cameras, digital media plays a significant role in day-to-day life. But digital images were easily modified and manipulated without leaving any visual clues by digital image tools (e.g., 3D Max and Photoshop) [1]. This indicates a severe social issue of the degree of trust which could be positioned in the authenticity of digital contents, particularly when submitted as proof in a courtroom, to claim insurance, as well as in the scientific

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

community. Following a few statistical reports [2], most of the chronicle-approved manuscripts comprise figures with fraudulent and unsuitable operations. Several methodologies were advanced to counter forgery and tampering to assure the authenticity of an image [3].

Copy-move forgery (CMF) imaging was considered a specific kind of forgery which includes making a copy of a portion of the image and copied portion should be pasted to the same image [4], [5], [6], [7]. Therefore, image forensics linked with CMF identification made it very significant in the network-based community. The technologies utilized in image forensics were classified into two i.e. active detection and passive detection [8]. Firstly, the active detection technique demands previous details which are derivated from an image for identifying the authenticity of an image, namely watermarking. In contrast to active detection techniques, passive detection techniques need not attain prior data on an image. Passive detection approaches could use the benefits of detective tactics for finding the tampering areas [9]. But, a major part of image forgery detection methodologies implements passive-related tactics for executing the types of tampering recognition which is deliberated in this article. Fig. 1 illustrates AI in cybersecurity.

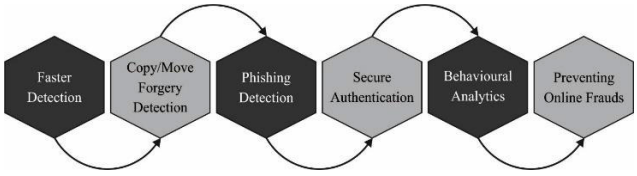

FIGURE 1. Artificial intelligence in cybersecurity.

Commonly, the major goal involved in forgeries is to hide a few of the doubtful items like guns by pasting other items or portions from that image [10]. With the help of modern hypermedia tools, digital images can be edited easily. A specialist forger could make a forged image where it is not possible to distinguish between authentic and fake images only by watching the image with the human eye. The authors have recommended several methods for identifying forgery in images.

This paper designs a reptile search algorithm with a deep transfer learning-based CM forgery detection (RSADTL-CMFD) model. The RSADTL-CMFD method identifies the availability of the CM region in the image. To attain this, the RSADTL-CMFD model initially derives a Neural Architectural Search Network (NASNet) model to generate feature vectors. For optimal tuning of the hyperparameter of the NASNet method, the RSA was used. The design of RSA helps to improve the performance of the NASNet model, showing the novelty of the work. To the best of our knowledge, the RSADTL-CMFD method never existed in the literature. At the final stage, the extreme gradient boosting (XGBoost) classification technique was utilized for allotting suitable class labels. The experimental result analysis of the RSADTL-CMFD method was tested with the benchmark datasets.

II. LITERATURE REVIEW

In [11], the authors developed an improved salient key point selection approach for CM forgery detection (CMFD). Scale-Invariant Feature Transform (SIFT) and KAZE keypoint features have been used and the salient keypoints have been chosen to improve the robust nature of the proposed model. The authors in [12] develop a novel deep learning (DL) concept for CMFD. Here, feature extraction, segmentation of the image, and localizing the area of forgery in an image have been performed using the Convolutional Block Attention Module (CBAM). Moreover, deep matching can be employed for determining feature map self-correlation, and Atrous Spatial Pyramid Pooling (ASPP) is employed for fusing the scaled correlation maps to create the coarse mask. At last, bilinear upsampling can be carried out for resizing the estimated outcomes to the same size as the input image.

Abbas et al. [13] investigated two DL models such as smaller VGGNet and MobileNetV2 for CM forgery detection. They are time-effective and resource-friendly to operate on embedded devices. A modified version of MobileNetV2 is considered to be highly efficient in CM detection. Ananthi et al. [14] developed an Advanced Fake Image-Feature Network (AFIFN) depending on DL methodologies. Here, Y Cr Cb and Discrete Cosine Transformation (DCT) based image preprocessing is applied. Furthermore, the AFIFN was enclosed by two-layered network architecture, attaining a pair-wise dataset as input. In [15], splicing was CMF recognition are simultaneously implemented on the similar data set CASIA v1.0 and CASIA v2.0. Firstly, suspicious images are taken and the feature is extracted by using block Discrete Cosine Transform (BDCT) and improved threshold methodology. The presented method agrees with whether the provided image is operated or not. Once it is manipulated the support vector machine (SVM) classifies the provided images via CMF or splicing forgery.

Alkawaz et al. [1] carry out the copy-move image forgery recognition via Discrete Cosine Transform (DCT) coefficients. Initially, based on the typical image transformation method, RGB image was converted to grayscale images. The two-dimensional DCT coefficient is evaluated and changed position into a feature vector by zig-zag scanning in all the blocks. At last, the lexicographic type is exploited for sorting the feature vector. Eventually, the duplicated block was situated using the Euclidean Distance. In [6], [16], and [17], proposed a hybrid mechanism by integrating the block-based technology with Fourier-Mellin Transform (FMT) and a keypoint-related approach with SIFT. Here, the inputs image are tested for forgery and are initially separated into smooth and texture areas. Next, the key point is abstracted from the texture portion of the images with the SIFT descriptors, as well as Fourier Mellin Transformation (FMT) is employed on the smoothest portion of the images. Later, the Extracted

feature is matched for detecting the duplicated region of images.

In [18], the authors examine the difficulty of identifying the CMF and define an effective and reliable passive-blind detection approach. In [19], a keypoint-based image forensics system dependent upon a superpixel segmentation technique and Helmert transformation were presented. The goal of this system is to identify CMF images and for obtaining forensic data. Tokas et al. [20] present a W-Net system-based technique to detect and localize areas of video forged utilizing the CMF approach. The presented approach was employed for the recognition of forged videos with a high degree of efficacy. Ganguly et al. [21] present a novel copy-move image forgery recognition system that depends on a texture feature descriptor termed Local Tetra Pattern (LTrP) for block-level image comparative utilized for localised tampered regions.

III. THE PROPOSED MODEL

In this work, an RSADTL-CMFD model was enhanced to identify the existence of CM regions in the image. The RSADTL-CMFD model initially derived a NASNet model to generate feature vectors. Followed by, the hyperparameters of the NASNet method are optimally altered by the use of RSA. Lastly, the XGBoost classification model is utilized to allot appropriate class labels.

A. LEVEL I: FEATURE EXTRACTOR

In this work, the RSADTL-CMFD model initially derived a NASNet model to generate feature vectors [22]. NASNet framework is made by a neural architecture search technique. The search technique named Neural Architectural Search (NAS) employs a control neural network (NN) to present the optimal CNN model for provided information. Two kinds of convolution cells are applied in this architecture, that is, the Standard cell and the Reduction cell. Where the Reduction cell decreases the region of the feature map through a factor of 2. Especially, NASNet is augmented for the ImageNet data that has images from each walk of life excel in extracting features. In this work, a pre-trained NASNet architecture (trained on ImageNet data) is presented. The shortage of large-scale data necessitates the usage of pre-trained architecture. Then, a dense layer of 128×1 replaces the classifier portion of the architecture that is 3×1 and 128×1, 2×1 for ternary and binary classifiers, correspondingly. Next, the pre-trained architecture attained is fine-tuned. During the fine-tuning process, NASNet is fed as an input image of $224 \times 224 \times 3$ dimensions. Later, the input goes through different reduction and Normal layers extracting the optimal feature. At last, the obtained feature is given into two dense layers of 128×1 and 3×1 dimensions for the classifier. Fig. 2 depicts the framework of the NASNet method. The above-mentioned procedure is continually performed in different iterations of backpropagation.

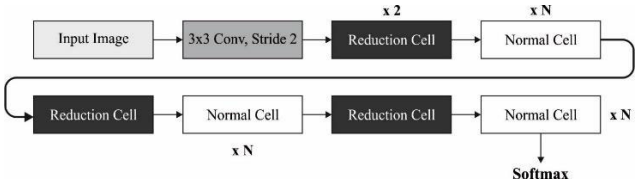

FIGURE 2. The architecture of the NASNet model.

B. LEVEL II: HYPERPARAMETER TUNING

At this stage, the hyperparameters of the NASNet method are optimally attuned by utilizing RSA [23]. RSA is another nature-simulated algorithm based on simulating crocodile surrounding and hunting performance. It can be a gradient-free technique which begins with creating arbitrary solutions as given in Eq. (1):

$$x_{i,j} = rand_{\in[0,1]} \times \left(UB_j - LB_j\right) + LB_j \; for \; i \in \{1, \ldots, N\} \; and \; j \in \{1, \ldots, M\} \tag{1}$$

whereas, $\chi_{i,j}$ implies the i^{th} solution for j^{th} input feature to entire N solutions including M feature, $rand_{\in[0,1]}$ represents the arbitrary number distributed uniformly from a range of zero and one, and the j^{th} feature is upper UB_j and lower LB_j boundaries.

Similar to the other nature-simulated MAs, RSA is assumed in 2 rules such as exploration and exploitation. These rules are enabled by crocodile movement but surrounding the target prey. The entire iterations of RSA were separated into 4 phases for taking benefit of the natural performance of the crocodiles. During the primary 2 phases, the RSA attains the exploration dependent upon the surrounding performance including the higher and belly walking movement. The crocodiles start their surrounding by searching the area, facilitating a further comprehensive search of solution space. It can be formulated using Eq. (2):

$$x_{i,j}(g+1) = \begin{cases} \left[-n_{i,j}(g)\,\gamma Best_j(g)\right] - \left[rand_{\in[1,N]} R_{i,j}(g)\right], \\ g \leq \dfrac{2T}{4} \\ \mathrm{ES(g)}.Best_j(g).\chi_{(rand_{\in[1,N]},j)} \\ \mathrm{g} \leq \dfrac{2T}{4} and g > \dfrac{T}{4} \end{cases} \tag{2}$$

whereas $Best_j(g)$ signifies the optimum solution to the j^{th} feature, $n_{i,j}$ signifies the hunting function to the j^{th} feature from the i^{th} solution (computed as in Eq. (3)), parameter γ controls the exploration accuracy throughout the length of iterations and is fixed as 0.1.

The decrease function $R_{i,j}$ was utilized for reducing the search area and is computed as in Eq. (6), $rand_{\in[1,N]}$ refers to the number amongst 1 to N utilized for arbitrarily choosing the most feasible candidate solutions, and evolutionary sense ES (g) indicates the probability ratio decreasing from

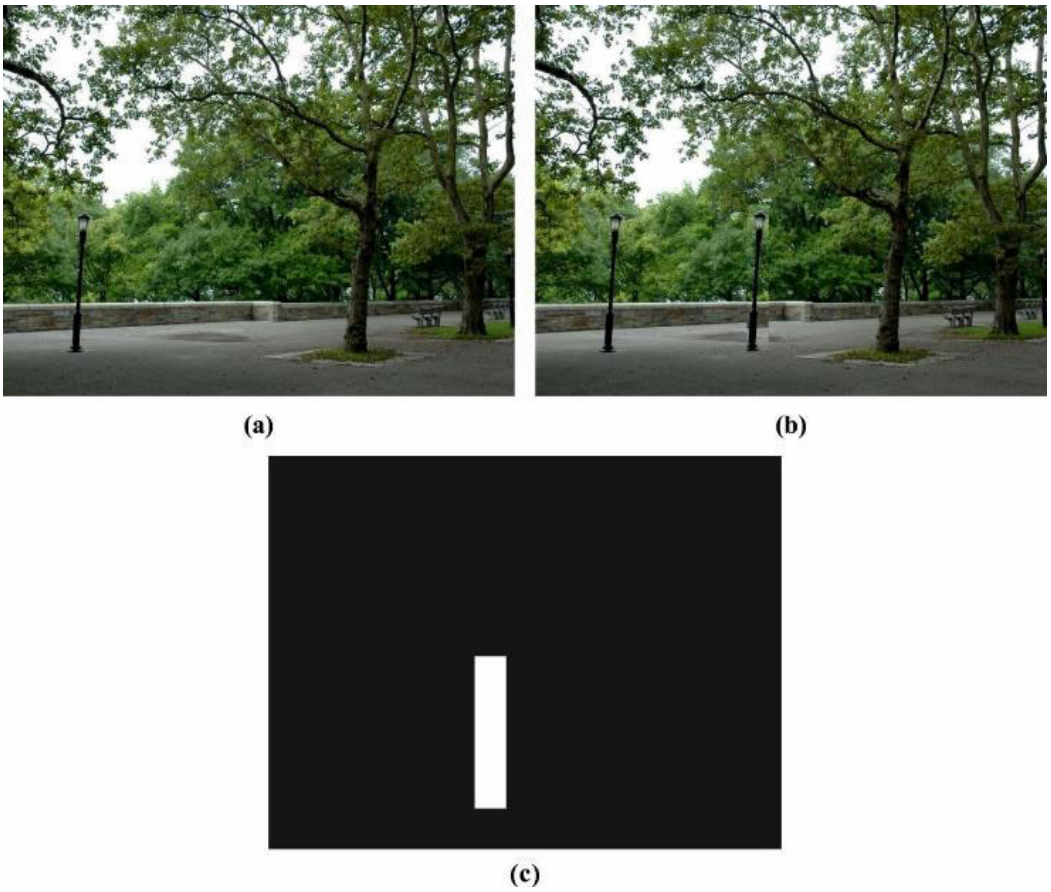

FIGURE 3. Sample test image a) Original image b) Tampered image c) Localization image.

2 to −2 over iteration, computed as in Eq. (3).

$$n_{i,j} = Best_j\,(g) \times P_{i,j} \tag{3}$$

In which, $P_{i,j}$ signifies the percentage variance amongst the j^{th} value of the optimum solution to their corresponding value from the existing solution and was computed in Eq. (4):

$$P_{i,j} = \theta + \frac{x - M(x)}{Best_j(g) \times (UB_j - LB_j) + e} \tag{4}$$

whereas θ indicates the sensitive parameter which controls the exploration efficiency, e implies the small floor value, and $M(x)$ represents the average solution and was demonstrated in Eqs. (5)-(7):

$$M\,(x_i) = \frac{1}{n}\sum_{j=1}^{n} x_{i,j} \tag{5}$$

$$R_{i,j} = \frac{Best_j(g) - \chi_{(rand_{\in[1,N]'}j)}}{Best_j(g) + e} \tag{6}$$

$$ES\,(g) = 2 \times rand_{\in[-1,1]} \times \left(1 - \frac{1}{T}\right) \tag{7}$$

where the value 2 performs as the multiplier for providing correlation value from the range in zero and two, and $rand_{\in[-1,1]}$ denotes the arbitrary integer number amongst −1 and 1. During the final 2 phases, the RSA executes the exploitation (hunting) for searching feature space to optimum solution utilizing 2 manners such as hunting coordination and cooperation. The solution is to upgrade their value under the exploitation utilizing Eq. (8):

$$x_{i,j}(g+1) = \begin{cases} rand_{\in[-1,1]}.Best_j(g).P_{i,j}(g), \\ g \leq \frac{3T}{4}\ and\ g > \frac{2T}{4} \\ [e.Best_j(g).n_{i,j}(g)] - [rand_{\in[-1,1]}.R_{i,j}(g)], \\ g \leq T\ and\ g > \frac{3T}{4} \end{cases} \tag{8}$$

The quality of candidate solutions at every iteration was measured utilizing the existing FF and this technique stop after T iteration and the candidate solution with minimal fitness value was chosen as OFS. The RSA approach intends to compute a fitness function for accomplishing superior classification accuracy. It described a positive value to characterize the effective performance of the candidate solution, as defined in Eq. (9). Here, the reduction of classification error rate was a fitness function. The worse solution attains an increased error rate and the best solution has the

least error rates.

$$fitness\,(x_i) = ClassifierErrorRate\,(x_i)$$

$$= \frac{number\ of\ misclassified\ samples}{Total\ number\ of\ samples} * 100 \qquad (9)$$

C. LEVEL III: IMAGE CLASSIFICATION

In the last phase, the XGBoost classification model is utilized to allocate applicable class labels [24]. It employs boosted tree and is utilized for regression and classification. Also, it is commonly employed for different predictive tasks and produces considerable results because of its speed and effective learning ability. XGB is an improved version of the XGB. The primary goal of the presented method is the optimization of the objective function by decreasing the difficulty, computation resource usage, and loss.

The difficulty can be minimized by regularization. Furthermore, normalization can be utilized for alleviating the over-fitting problem. The process works by adding the tree iteratively by splitting the features. In the following iteration, new rules are included, as well as the loss is decreased. This process continues until the model accomplished the optimum result. XGB employs the second-order derivative to the loss function.

Consider D indicates the dataset comprises n amount of features, as given in Eq. (10):

$$D = \{x_1, x_2, \ldots, x_n\} \qquad (10)$$

The XGB tree ensemble ($Tree_{Ens}$) is defined in Eq. (11)

$$Tree_{Ens} = \sum_{k=1}^{j} Loss\left(y_k, \sum_{n=1}^{N} f_n\,(x_k)\right) + \sum_{n=1}^{N} \Omega\,(f_n)\,, f_n \in F, \qquad (11)$$

where y characterizes the class attributes. The loss embodies loss function viz, the variance among the actual and the predicted. N signifies the tree count. F denotes the set of trees utilized in the model training. ω denotes the regularization term.

IV. EXPERIMENTAL VALIDATION

The proposed model is simulated using Python 3.6.5 tool on PC i5-8600k, GeForce 1050Ti 4GB, 16GB RAM, 250GB SSD, and 1TB HDD. The parameter settings are given as follows: learning rate: 0.01, dropout: 0.5, batch size: 5, epoch count: 50, and activation: ReLU. This section examines the experimental validation of the RSADTL-CMFD approach taking place using MNIST [25] and CIFAR-10 [26] datasets. The suggested method is simulated by the Python tool. A few sample images are portrayed in Fig. 3. The outcomes are examined for a set of ten iterations.

Fig. 4 presents detailed CM forgery detection outcomes of the RSADTL-CMFD method under distinct iterations on the MNIST dataset. The figure pointed out the RSADTL-CMFD approach has demonstrated reasonable outcomes

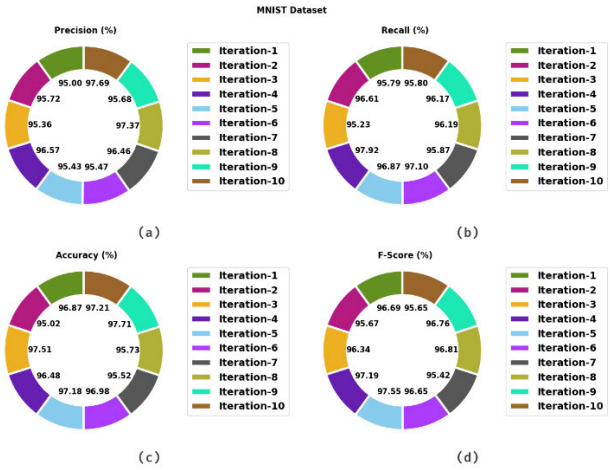

FIGURE 4. Result analysis of RSADTL-CMFD technique under various iterations on MNIST dataset (a) $prec_n$, (b) $reca_l$, (c) $accu_y$, and (d) F_{score}.

under each iteration. For example, with iteration-1, the RSADTL-CMFD model has offered $prec_n$, $reca_l$, $accu_y$, and F_{score} of 95%, 95.79%, 96.87%, and 96.69% correspondingly. Simultaneously, with iteration-5, the RSADTL-CMFD method has accessible $prec_n$, $reca_l$, $accu_y$, and F_{score} of 95.43%, 96.87%, 97.18%, and 97.55% correspondingly. Moreover, with iteration-10, the RSADTL-CMFD system has obtainable $prec_n$, $reca_l$, $accu_y$, and F_{score} of 97.69%, 95.80%, 97.21%, and 95.65% correspondingly.

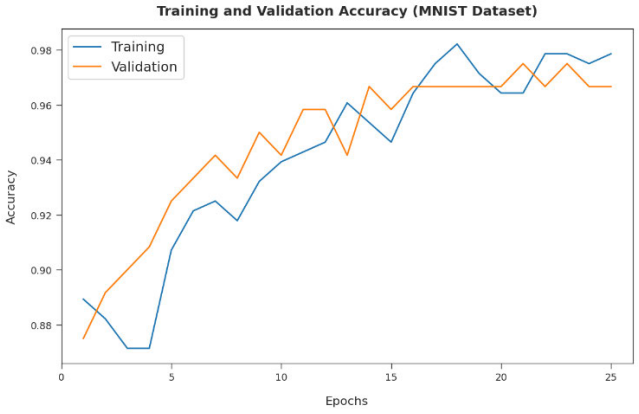

FIGURE 5. TA and VA outcome of RSADTL-CMFD method on MNIST dataset.

The training accuracy (TA) and validation accuracy (VA) reached by the RSADTL-CMFD approach on the MNIST database are seen in Fig. 5. The figure displayed that the RSADTL-CMFD method has obtained higher values of TA and VA. The VA is greater than that of the TA.

The training loss (TL) and validation loss (VL) reached by the RSADTL-CMFD method on the MNIST dataset are seen in Fig. 6. The figure specified that the RSADTL-CMFD

approach has the least values of TL and VL. The VL is lesser than TL.

Fig. 7 portrays the receiver operating characteristic (ROC) analysis of the RSADTL-CMFD technology on the MNIST database. The figure exposed that the RSADTL-CMFD system has attained enhanced outcomes with a maximal ROC of 99.4369.

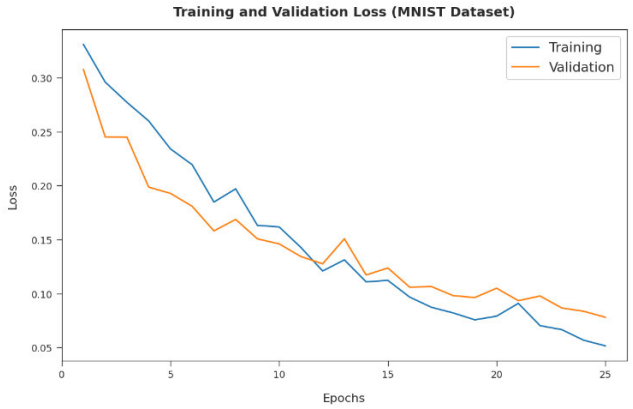

FIGURE 6. TL and VL outcome of RSADTL-CMFD method on MNIST database.

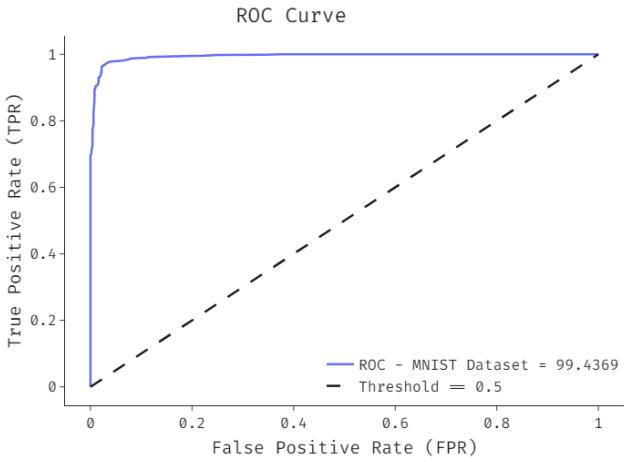

FIGURE 7. ROC curve outcome of RSADTL-CMFD method on MNIST database.

Fig. 8 provides detailed CM forgery detection outcomes of the RSADTL-CMFD method under various iterations on the CIFAR-10 dataset. The experimental outcome shows that the RSADTL-CMFD algorithm has reasonable outcomes under all iterations. For example, with iteration-1, the RSADTL-CMFD model has offered $prec_n$, $reca_l$, $accu_y$, and F_{score} of 97.67%, 97.59%, 96.06%, and 98.23% respectively. Simultaneously, with iteration-5, the RSADTL-CMFD approach has obtainable $prec_n$, $reca_l$, $accu_y$, and F_{score} of 96.54%, 97%, 96.31%, and 98.46% correspondingly. In addition, with iteration-10, the RSADTL-CMFD algorithm has accessible $prec_n$, $reca_l$, $accu_y$, and F_{score} of 97.42%, 97.65%, 96.86%, and 96.73% correspondingly.

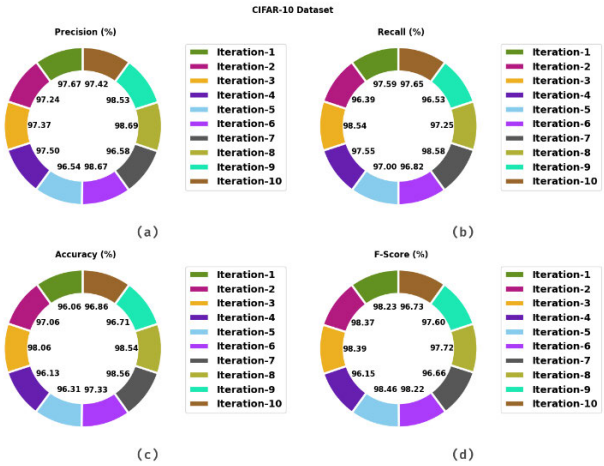

FIGURE 8. Result analysis of the RSADTL-CMFD method under various iterations on the CIFAR-10 dataset.

The TA and VA reached by the RSADTL-CMFD technique on the CIFAR-10 dataset were shown in Fig. 9. The figure pointed out that the RSADTL-CMFD algorithm has higher values of TA and VA. Especially the VA is comparatively lesser than TA.

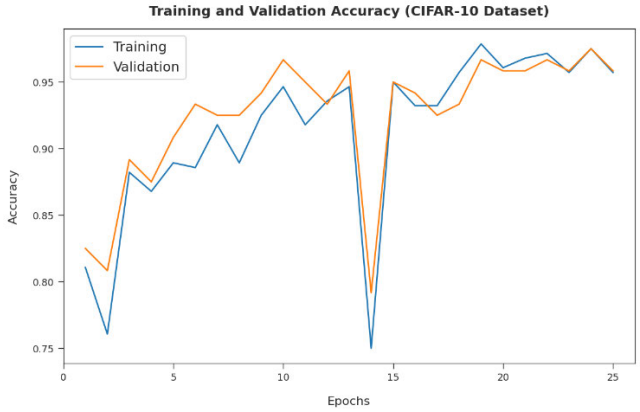

FIGURE 9. TA and VA outcome of RSADTL-CMFD methodology on CIFAR-10 database.

The TL and VL gained by the RSADTL-CMFD method on the CIFAR-10 database are displayed in Fig. 10. The figure displayed the RSADTL-CMFD model has the least values of TL and VL. The VL is comparatively lesser than TL.

Fig. 11 illustrates the ROC analysis of the RSADTL-CMFD system on the CIFAR-10 database. The figure revealed the RSADTL-CMFD approach reaches enhanced outcomes with the highest ROC of 99.8645.

Table 1 shows a brief analysis of the RSADTL-CMFD approach with current models [27], [28]. The experimental results indicated the IFD-AOS-FPM and CMFD-BMIF model has shown lower $prec_n$ values of 63.52% and 65.08%

Besides, the RSADTL-CMFD approach has reported a maximum F_{score} of 97.65%. The above-mentioned results

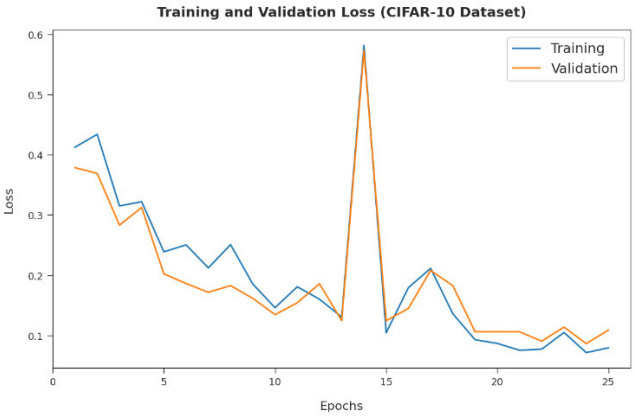

FIGURE 10. TL and VL outcome of RSADTL-CMFD methodology on CIFAR-10 database.

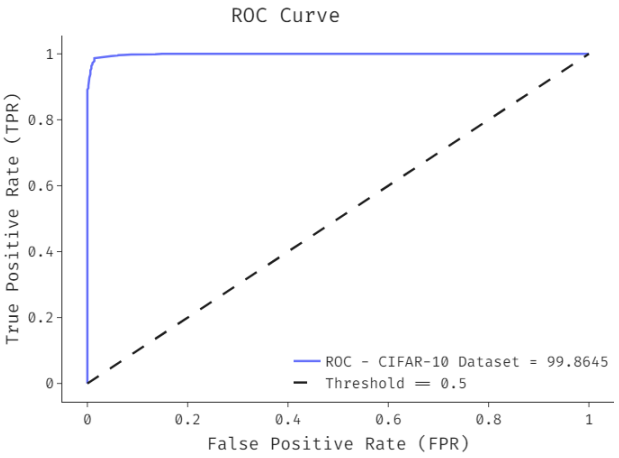

FIGURE 11. ROC curve analysis of RSADTL-CMFD method on the CIFAR-10 database.

TABLE 1. Comparative analysis of RSADTL-CMFD technique with recent algorithms [27], [28].

Methods	Precision	Recall	F-score
CMFD Model	68.28	78.97	65.05
IFD-AOS-FPM	63.52	83.35	64.45
CMFD-BMIF	65.08	80.68	69.42
BB-KB-ICMFD	68.40	79.68	70.94
CMFD-GAN-CNN	70.10	80.69	88.26
DLFM-CMDFC	96.96	96.90	96.87
RSADTL-CMFD	97.62	97.39	97.65

and discussion reported that the RSADTL-CMFD model has shown maximum outcomes over other models. Thus, the RSADTL-CMFD model can be employed for the detection of CM regions in the image.

V. CONCLUSION

In this study, an RSADTL-CMFD approach was formulated for identifying the existence of CM regions in the image. The RSADTL-CMFD model initially derived a NASNet model to generate feature vectors. Followed by, the hyperparameters of the NASNet technique are altered through RSA. Lastly, the XGBoost classification model is utilized to allot appropriate class labels. The experimental result analysis of the RSADTL-CMFD method is tested with the benchmark datasets. An extensive study pointed out the enhanced outcomes of the RSADTL-CMFD method over recent methods. Thus, the RSADTL-CMFD approach can be utilized to identify the CM regions in real time. In future, the outcome of the RSADTL-CMFD method has been enhanced by the use of hybrid DL methods. Besides, the presented method will be tested on real-time data in the upcoming years.

ACKNOWLEDGMENT

The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Groups Project under grant number (RGP2/96/44). Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R361), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. Research Supporting Project number (RSPD2023R787), King Saud University, Riyadh, Saudi Arabia. This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2023/R/1444).

REFERENCES

[1] M. H. Alkawaz, G. Sulong, T. Saba, and A. Rehman, "Detection of copy-move image forgery based on discrete cosine transform," *Neural Comput. Appl.*, vol. 30, no. 1, pp. 183–192, Jul. 2018.

[2] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," *Digit. Invest.*, vol. 9, no. 1, pp. 49–57, Jun. 2012.

[3] S. Sadeghi, S. Dadkhah, H. A. Jalab, G. Mazzola, and D. Uliyan, "State of the art in passive digital image forgery detection: Copy-move image forgery," *Pattern Anal. Appl.*, vol. 21, no. 2, pp. 291–306, May 2018.

[4] J. Zheng, Y. Liu, J. Ren, T. Zhu, Y. Yan, and H. Yang, "Fusion of block and keypoints based approaches for effective copy-move image forgery detection," *Multidimensional Syst. Signal Process.*, vol. 27, no. 4, pp. 989–1005, Oct. 2016.

[5] A. A. Albraikan, S. B. H. Hassine, S. M. Fati, F. N. Al-Wesabi, A. M. Hilal, A. Motwakel, M. A. Hamza, and M. Al Duhayyim, "Optimal deep learning-based cyberattack detection and classification technique on social networks," *Comput., Mater. Continua*, vol. 72, no. 1, pp. 907–923, 2022.

[6] M. A. Alohali, F. N. Al-Wesabi, A. M. Hilal, S. Goel, D. Gupta, and A. Khanna, "Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment," *Cognit. Neurodyn.*, vol. 16, no. 5, pp. 1045–1057, Oct. 2022, doi: 10.1007/s11571-022-09780-8.

[7] M. A. Hamza S. B. H. Hassine, I. Abunadi, F. N. Al-Wesabi, and H. Alsolai, "Feature selection with optimal stacked sparse autoencoder for data mining," *Comput., Mater. Continua*, vol. 72, no. 2, pp. 2581–2596, 2022.

[8] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Block-based copy–move image forgery detection using DCT," *Iran J. Comput. Sci.*, vol. 2, no. 2, pp. 89–99, Jun. 2019.

[9] A. K. Jaiswal and R. Srivastava, "Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model," *Neural Process. Lett.*, vol. 54, no. 1, pp. 75–100, Feb. 2022.

[10] A. B. Z. Abidin, H. B. A. Majid, A. B. A. Samah, and H. B. Hashim, "Copy-move image forgery detection using deep learning methods: A review," in *Proc. 6th Int. Conf. Res. Innov. Inf. Syst. (ICRIIS)*, Johor Bahru, Malaysia, Dec. 2019, pp. 1–6, doi: 10.1109/ICRIIS48246.2019.9073569.

[11] N. Kumar and T. Meenpal, "Salient keypoint-based copy–move image forgery detection," *Austral. J. Forensic Sci.*, vol. 55, no. 3, pp. 331–354, May 2023.

[12] M. Sabeena and L. Abraham, "Convolutional block attention based network for copy-move image forgery detection," *Multimedia Tools Appl.*, pp. 1–23, May 2023.

[13] M. N. Abbas, M. S. Ansari, M. N. Asghar, N. Kanwal, T. O'Neill, and B. Lee, "Lightweight deep learning model for detection of copy-move image forgery with post-processed attacks," in *Proc. IEEE 19th World Symp. Appl. Mach. Intell. Informat. (SAMI)*, Herl'any, Slovakia, Jan. 2021, pp. 125–130, doi: 10.1109/SAMI50585.2021.9378690.

[14] M. Ananthi, P. Rajkumar, R. Sabitha, and S. Karthik, "A secure model on advanced fake image-feature network (AFIFN) based on deep learning for image forgery detection," *Pattern Recognit. Lett.*, vol. 152, pp. 260–266, Dec. 2021, doi: 10.1016/j.patrec.2021.10.011.

[15] C. S. Prakash, A. Kumar, S. Maheshkar, and V. Maheshkar, "An integrated method of copy-move and splicing for image forgery detection," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26939–26963, Oct. 2018.

[16] K. B. Meena and V. Tyagi, "A hybrid copy-move image forgery detection technique based on Fourier-Mellin and scale invariant feature transforms," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 8197–8212, Mar. 2020.

[17] A. M. Hilal, M. A. Alohali, F. N. Al-Wesabi, N. Nemri, H. J. Alyamani, and D. Gupta, "Enhancing quality of experience in mobile edge computing using deep learning based data offloading and cyberattack detection technique," *Cluster Comput.*, vol. 26, no. 1, pp. 59–70, Feb. 2023, doi: 10.1007/s10586-021-03401-5.

[18] L. Kang and X.-p. Cheng, "Copy-move forgery detection in digital image," in *Proc. 3rd Int. Congr. Image Signal Process.*, Yantai, China, Oct. 2010, pp. 2419–2421, doi: 10.1109/CISP.2010.5648249.

[19] H.-Y. Huang and A.-J. Ciou, "Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation," *EURASIP J. Image Video Process.*, vol. 2019, no. 1, pp. 1–16, Dec. 2019, doi: 10.1186/s13640-019-0469-9.

[20] B. Tokas, V. R. Jakkinapalli, and N. Singla, "Video forgery detection and localization with deep learning using W-Net architecture," in *Computational Intelligence* (Lecture Notes in Electrical Engineering), 2023, pp. 31–38, doi: 10.1007/978-981-19-7346-8_3.

[21] S. Ganguly, S. Mandal, S. Malakar, and R. Sarkar, "Copy-move forgery detection using local tetra pattern based texture descriptor," *Multimedia Tools Appl.*, vol. 82, no. 13, pp. 19621–19642, May 2023, doi: 10.1007/s11042-022-14287-9.

[22] B. Zoph, V. Vasudevan, J. Shlens, and Q. V. Le, "Learning transferable architectures for scalable image recognition," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit.*, Salt Lake City, UT, USA, Jun. 2018, pp. 8697–8710, doi: 10.1109/CVPR.2018.00907.

[23] L. Abualigah, M. A. Elaziz, P. Sumari, Z. W. Geem, and A. H. Gandomi, "Reptile search algorithm (RSA): A nature-inspired meta-heuristic optimizer," *Expert Syst. Appl.*, vol. 191, Apr. 2022, Art. no. 116158, doi: 10.1016/j.eswa.2021.116158.

[24] Z. Chen, F. Jiang, Y. Cheng, X. Gu, W. Liu, and J. Peng, "XGBoost classifier for DDoS attack detection and analysis in SDN-based cloud," in *Proc. IEEE Int. Conf. Big Data Smart Comput. (BigComp)*, Shanghai, China, Jan. 2018, pp. 251–256, doi: 10.1109/BigComp.2018.00044.

[25] *The MNIST Database of Handwritten Digits*. Accessed: Feb. 14, 2023. [Online]. Available: http://yann.lecun.com/exdb/mnist

[26] *Cifar*. Accessed: Feb. 24, 2023. [Online]. Available: https://www.cs.toronto.edu/ kriz/cifar.htm

[27] N. Krishnaraj, B. Sivakumar, R. Kuppusamy, Y. Teekaraman, and A. R. Thelkar, "Design of automated deep learning-based fusion model for copy-move image forgery detection," *Comput. Intell. Neurosci.*, vol. 2022, pp. 1–13, Jan. 2022.

[28] Y. Abdalla, M. T. Iqbal, and M. Shehata, "Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network," *Information*, vol. 10, no. 9, p. 286, Sep. 2019.