Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

Research Article

Digital Image Forgery Detection and Localization using the Innovated U-Net

Nuha Majeed Saleh[1]
Informatics Institute for Postgraduate Studies,
Iraqi Commission for Computers and Informatics.
Baghdad
Iraq
ms202130663@iips.edu.iq

Sinan A. Naji [2]
University of Information Technology
and Communications,
Baghdad
Iraq
dr.sinannaji@uoitc.edu.iq

A R T I C L E I N F O
Article History
Received: 18/12/2023
Accepted: 29/1/2024
Published: 30/6/2024

ABSTRACT
A reliable image copy–move forgery detection approach adaptable to different scenarios of tampering with color images is crucial for many applications. Different methods and solutions have been effectively proposed, but they are still subject to false positive/negative detections and cannot handle the variety of copy–move forgeries. In this paper, a machine learning model that combines ResNet 50 and U-net architectures for automatic image forgery detection in color image(s) is presented. The proposed system is inspired by the ResNet 50 architecture as an encoder and the U-Net architecture as a decoder. The encoder function implies applying convolution and normalizing for feature extraction. Conversely, the decoder functions is locating the spatial features. The decoder in the U-Net network comprises multiple decoder blocks, which are connected to corresponding encoder blocks by employing concatenate layers. A binary mask is then produced to represent the tampered regions in the image. Quantitative experimental results on two standard public datasets and a comparison with state-of-the-art methods demonstrate the effectiveness and robustness of the proposed model.

Keywords: ***Deep Learning; U-Net; Encoder; Decoder; ResNet.***

1. INTRODUCTION

With the development of digital image processing software packages and other editing tools, image forgery has become simple and popular [1]. Image forgery can now imply many kinds of tampering and modifications to the visual contents of images in such a perfect way that they are unnoticeable to casual people. By altering the visual contents of an image, the new image is called a “forged” image [2]. In many instances, the purpose of this manipulation is to influence the attention and opinions of the recipient. As the world becomes more dependent on digital images for getting information, the need to verify the authenticity (i.e., originality) and dependability of these images’ increases. However, researchers and specialists are collaborating to develop computer-based systems to detect such forgeries automatically [3][1]. Using forged images for malicious purposes may have hazardous consequences in our society. These images are used in several application sectors, such as politics, investigations as forensic evidence, journalism, business, arts, and medical imaging. Generally, tampering images can be classified into two categories: tampering with innocent intent and tampering with noninnocent intent. The first category is employed to enhance the images and/or eliminate distortions while preserving the semantic content of the image. This category includes contrast enhancement, color enhancement, blurring, retouching, and red-eye correction. For example, the first category is widely used in fashion photographs, beauty care photos, truism, business, and marking. The second category involves malicious intentions and/or criminal activities. Generally, based on the type of content tampering, this type of manipulation has been classified into five categories: image splicing, copy–move forgery, geometric transformation forgery, text editing, and deep fake forgery [2]. Consequently, we have opted for the detection of manipulated images to provide efficient solutions employing various methods. To identify and detect an image forgery, the solutions can be broadly classified into two main categories: passive and active techniques. In active methods, some type of authentication data is embedded in the source image before distribution. The authentication data might be subsequently utilized to confirm

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

whether the image has been altered during a forensic examination. One potential constraint associated with this particular technique is its reliance on either specialized cameras or subsequent image processing procedures. Examples of active techniques commonly employed in the field of digital image security include digital image cryptography, digital signature implementation, and embedding a watermark into the original image prior to its utilization. Passive techniques are the most dominant methods in cases of forgery activities. These techniques are needed to determine whether an image has been tampered with, even in the absence of any pre-existing authentication data, such as a signature or watermark. Hence, passive forgery detection is regarded as a more appealing approach [4][5]. Copy–move is considered the most common method for image forgery. This technique involves replacing one or more image fragments with one or more image fragments from the same image to produce forged images. The main purpose of copy–move forgery is to either conceal object(s) or generate many duplicates of a certain object. Copy–move forgery detection (CMFD) is a challenging task. The technical complications with automatic CMFD can be related to the following issues [6]:

- Presence or absence of structural components: Tampering can alter the image's contents, causing some features to become partially or completely obscured.
- Geometric transformations: Object appearance can be changed by geometric transformations, such as rotation, scaling, and translation.
- Imaging retouching: When the image is captured, lighting and camera attributes can affect the visual representation of objects. Generally, image retouching may change the appearance of objects and consequently affect the feature-set extraction. This situation may lead to many false negative and/or false positive results.
- Intensity and color adjustment: These processes also affect the output of the feature extraction step and consequently may cause many false negative and/or false positive results

In this paper, a novel method for identifying and locating manipulated regions in digital images using machine learning-based semantic segmentation approach is presented. The proposed system is inspired by the ResNet50 model as an encoder and the U-Net architecture as decoder [7]. The encoder function implies applying convolution and normalizing for feature extraction. Conversely, the decoder function is locating the spatial features. The decoder in the U-Net network comprises multiple decoder blocks, which are connected to corresponding encoder blocks by employing concatenate layers. Then, a binary mask is generated to denote the manipulated regions in the image. Figure 1 shows the general architecture of the proposed model for automatic forgery detection.

The subsequent sections of this research study are structured as follows: In Section II, a brief overview of the recent related works is provided. Subsequently, the preprocessing and feature extraction procedures are delineated. In Section III, the machine learning techniques employed for predicting forged regions is discussed. In Section IV, the results are discussed.

2. RELATED WORKS

Generally, CMFD techniques can be classified into three primary categories: block-based, key point-based, and machine learning-based [8]. The block-based technique entails initially dividing the input image into overlapping or nonoverlapping blocks. Then, feature-sets are extracted for each block. The matching phase is employed to determine similar blocks based on their feature-sets [6]. The key point-based approach involves extracting local features from the whole image and representing them as a set of descriptors. Finally, the descriptors are compared to identify forged regions [9]. Deep learning algorithms depend on the creation of convolutional neural network (CNN) models, which possess high capacity for extracting meaningful information from the input images and other digital data [8]. Parveen et al. utilized a block-based method for CMFD [10]. The suggested approach encompasses a series of steps: converting the color image to grayscale and dividing the grayscale image into [8×8] overlapping blocks. DCT is for locating features, and finally the feature matching is conducted via the radix sort method. Yang et al. introduced a key point-based approach using the SIFT technique [11]. A formulation of a distribution strategy was devised to ensure the fair placement of key-points within an image. The enhanced SIFT descriptor was developed to depict key-points precisely within the context of the CMFD scenario, and the key-points were matched using the agglomerative hierarchical clustering (AHC) algorithm. Elaskily proposed an innovative model for CMFD based on deep learning [8]. Specifically, a CNN model was proposed to generate a representation of categorized descriptors. Following the training phase of the CNN, the system could classify images to identify instances of copy–move forgeries.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

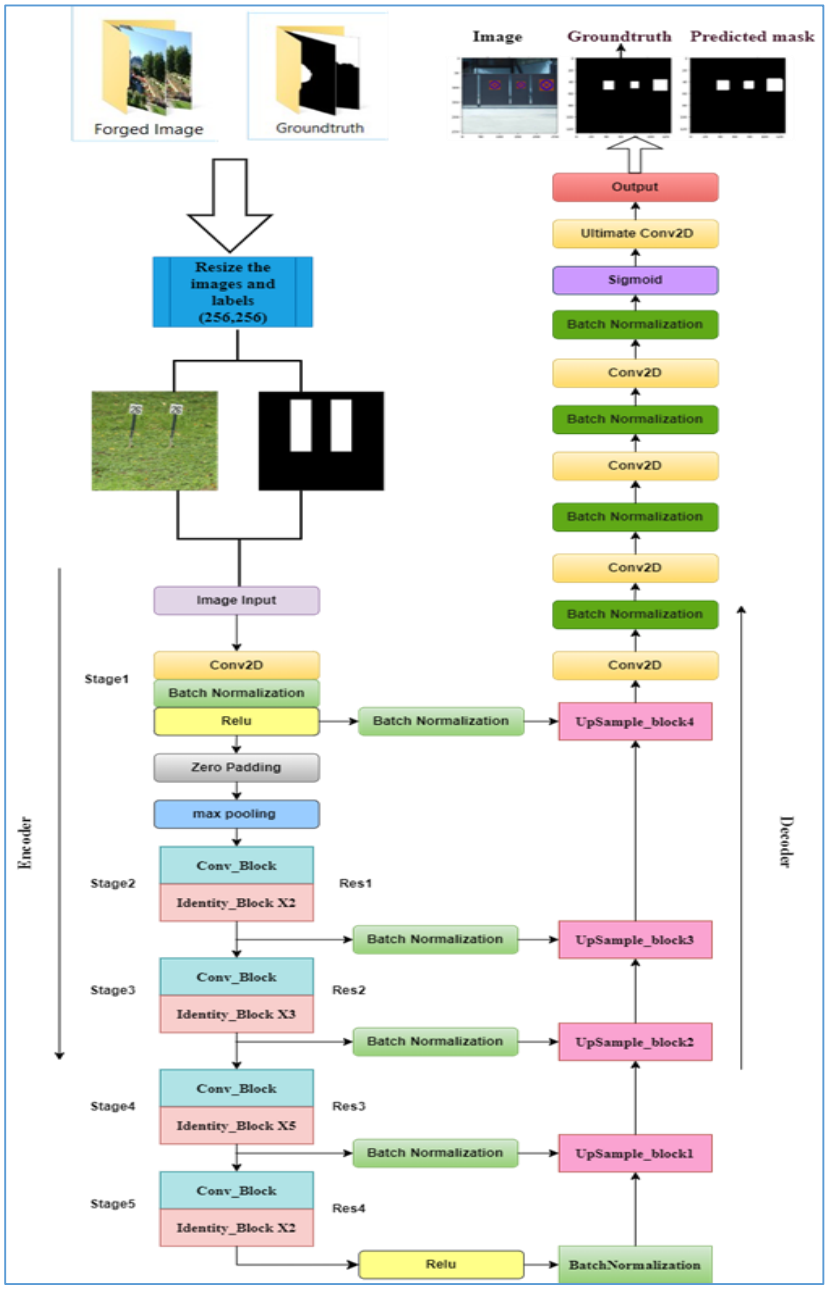


Fig. 1. General Architecture of The Proposed Model For Automatic Forgery Detection

Yao et al. presented a model based on deep learning for forgery detection in videos [12]. The proposed model utilizes CNNs for the extraction of features. To reduce temporal redundancy between video frames, the video frames undergo preprocessing in three stages. These stages include the implementation of a frame absolute difference layer. Additionally, data augmentation techniques are applied to prepare image patches for the training phase. Wu et al. presented an innovative deep learning model called BusterNet, for the purpose of CMFD [13]. BusterNet comprises two CNN architectures, followed by a fusion model. This remarkable model can accurately identify potential manipulated regions through the utilization of feature similarities. According to the author's statement, BusterNet surpasses existing cutting-edge models in terms of performance. Liu employed multiscale convolution for producing forgery probability maps and combined it with segmentation to obtain the final tampered maps [14]. Bi et al. introduced the ringed residual U-Net (RRU-Net) for splicing forgery detection [15]. The RRU-Net demonstrated enhanced utilization of contextual spatial details and effectively resolved the issue of gradient degradation in the detection of splicing forgery. Zhu et al. proposed an end-to-end neural network called AR-Net [16]. The network is based on adaptive attention and residual refinement, which it aims to enhance the representation of features by fusing position and channel attention features. Additionally, deep matching is employed to calculate the self-correlation between feature maps, and the atrous spatial pyramid pooling (ASPP) technique combines the scaled correlation maps to produce the mask. Finally, the mask is refined through the residual refinement module, which preserves the boundary structure of objects. Kumar et al. employed unsupervised domain adaptation to learn the

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

discriminative features from a large dataset and classify the forged images in new domains by feature space mapping [17]. Ahmed et al. introduced a novel deep learning technique for the identification of image forgeries, which remains effective even after post processing [18]. The suggested model is founded upon an encoder–decoder framework specifically devised to acquire discriminative attributes spanning the forged areas. Huang et al. [19] a dual-stream UNet named DS-UNet for CMFD and localization. The DS-UNet extracts the high-/low-level manipulated traces. The lightweight hierarchical fusion method enables the DS-UNet to perceive tampered objects at different scales because tampered objects always vary in shape and size. Weng et al. proposed a novel model named UCM-Net, which incorporates multilayer asymmetric connections between the feature extraction module (FEM) and the tampered region localization module (TRLM [20]. The FEM selectively processes large- or small-tampered regions by leveraging deep underlying networks. To eliminate irrelevant semantic information effectively while preserving multiscale tampered features, multiple cross-layer connections are established between two auto correlation and ASPP computation modules. Furthermore, TRLM employs multiple U-shaped residual block units to capture global and local information.

3. PROPOSED SYSTEM

Generally, CNNs are a sophisticated form of artificial neural networks that utilize convolutional kernels for successful pattern recognition and image processing tasks. In this paper, the proposed model is inspired by the ResNet50 model as an encoder within the U-Net architecture. The encoder function implies applying a set of operations, such as convolution and normalizing to extract features. Conversely, the decoder function is locating the spatial features by combining two inputs (one stemming from the preceding layer of the decoder and the other originating from the symmetrical residual stage output of the encoder).

The proposed model includes three basic stages:

A. Preprocessing

Enhancing the quality of the dataset and the corresponding ground truth masks is highly important for the purpose of training. This stage implies the following steps:

- **Splitting, resizing, and labeling:** The images are divided into three distinct sections, namely, 80% for training, 10% for validation, and 10% for testing. Subsequently, the images and ground truth masks are resized to standardize all inputs for the model, ensuring uniform dimensions. This standardization results in a reduction of the images to dimensions of 256 × 256. The manipulated images are similarly organized alongside the corresponding mask through the arrangement of the name syllable for each individual image.
- **Normalization:** Normalizing pixel values in the “image” and “mask” arrays. Normalization is a widely accepted practice in the fields of image processing and deep learning. This normalization aims to scale the pixel values to a range that typically falls between 0 and 1. Typically, pixel values in most images are initially represented within the range of 0 to 255 for each channel, assuming an 8-bit representation. By dividing these values by 255, normalization is achieved.

B. Architecture of the Innovated U-Net

The proposed model is partitioned into two distinct components: the encoder and the decoder:

- **Encoder**

Due to the inherent advantages possessed by ResNet [7], the utilization of ResNet50 as an encoder is deemed appropriate. First, ResNet50 enhances extracting features. Second, reducing the number of parameters makes the system more effective. Third, it offers the skip connections concept, which allows the model to preserve information from the earlier layer. Fourth, combining ResNet50 with other models shows excellent results, in which one model can overcome the weakness of the other. The proposed model accepts an image with dimensions of 256 × 256 × 3 as input. To commence, the initial block of the encoder executes convolutional operations utilizing a kernel size of 7 × 7 and a stride of 2. Following this, Max-Pooling is employed with a stride size of 2. Subsequently, four consecutive residual stages, namely, Res1, Res2, Res3, and Res4, are employed sequentially. Figure 2 shows the general architecture of ResNet50.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

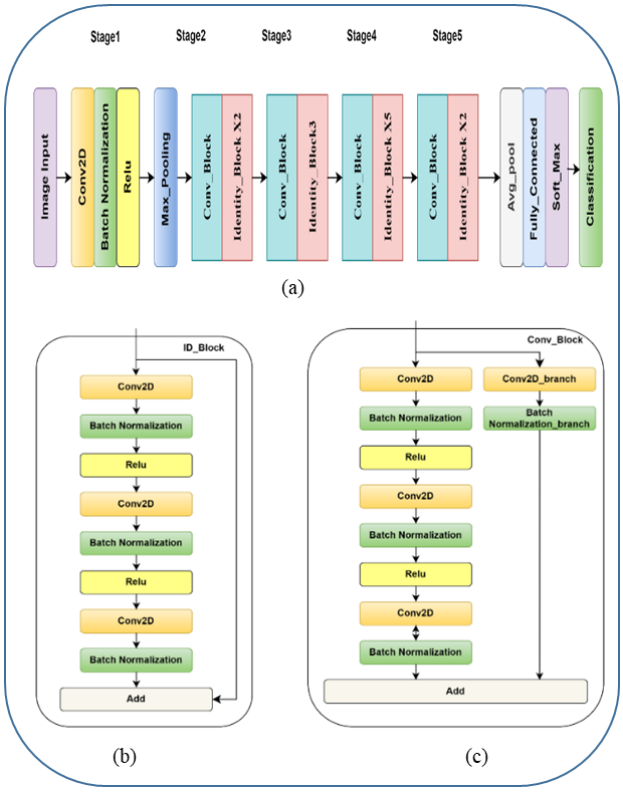


Fig. 2. Resnets50: (A) Architecture of Resnets50, (B) Design of the Identity Block, and (C) Design of The Convolutional Block

- **Decoder**

Generally, classic CNNs make no assumptions about the spatial correlations between the extracted features or spatial relations among pixels. In this work, the U-Net network architecture is used as a decoder, which comprises multiple decoder blocks. The U-Net is a powerful CNN model that can capture detailed features and spatial coherence with their neighbor's, which makes it highly suitable for image segmentation applications [19]. The main idea here is to take the whole image as an input and produce a full binary image as an output. In this work, the decoder in the U-Net network comprises multiple decoder blocks, which are connected to corresponding encoder blocks by employing concatenate layers. The decoder block engages in an upsampling procedure for the feature maps that are conveyed to it by the preceding block. This particular upsampling entails a convolutional operation using a kernel size of 3 × 3, which is subsequently followed by batch normalization. This upsampling procedure is reiterated four times. In the decoder section, four upSample blocks are respectively aligned with Res4, Res3, Res2, and Res1 of the encoder. Each upSample block is composed of feature maps with dimensions of (16×16×256), (32×32×128), (64×64×64), and (128×128×32). To predict the manipulated regions, the decoder network concludes with the utilization of the sigmoid pixel-wise classification function. The term P(TC) represents the likelihood of the two classes, namely, 0: forged and 1: original. This likelihood is determined through the utilization of the sigmoid function. Ultimately, binary masks are generated to denote the manipulated regions in the image.

4. PROBLEM OF IMBALANCED CLASSES

After Generally, researchers in machine learning have to deal with the imbalanced data sets. This problem arises when the number of samples in one class (i.e., pixels in the genuine regions) greatly exceeds those in other classes (i.e., pixels in the forged regions), resulting in inadequate to classify pixels [21]. Practically, traditional classifiers are likely to bias into the large class samples and ignore the class with small samples [21][22]. To tackle this issue, the probability of the forged and genuine regions is calculated by employing the statistical information obtained from ground truth samples. The weights exhibit a reciprocal correlation with the frequency at which each class occurs. Higher frequencies of appearance lead to lower weights. The class weights, denoted as class weights, are computed by employing the inverse ratio of the occurrence frequency of each class. The next is the all-encompassing expression used to determine the class weights. The class weight for each class is determined by the following [23]:

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

$$w_c = \frac{S}{C \cdot N_s}, \quad (1)$$

where S represents the entirety of the samples, C is the number of classes, Ns is the number of samples for a specific class, and Wc is the allocation of weight for class C. The strategy is to utilize the class weights parameter during the training procedure and the optimization by modifying the effect of each class on the overall loss. This approach enables the model to assign greater significance to classes that are under-represented, thus effectively tackling the problem of imbalanced classes.

5. DATA COLLECTION

To evaluate the proposed model, two datasets are used: CASIA [24] and COMOFOD [25]. The dataset is subdivided into three randomly chosen subsets: training (80%), validation (10%), and tests (10%).

Each image in the CoMoFoD dataset is coupled with its corresponding ground-truth mask that accurately outlines the forged regions. Five different categories of tampering are applied to the images: translation, rotation, scaling, combination, and distortion. Many post processing methods are used to modify the forged and original images, such as JPEG compression, blurring, noise addition, and color reduction. For the CASIA dataset, each image is coupled with its corresponding ground-truth mask.

TABLE I. DATASETS USED IN THIS PAPER

COMOFOD					
No. of Images	**Image size**	**Sub datasets**	**Image percentage**	**No. of Images**	**Ground-Truth**
4800	512×512	Training	80%	3840	YES
		Validation	10%	480	YES
		Testing	10%	480	YES
CASIA					
1309	384×256	Training	80%	1047	YES
		Validation	10%	131	YES
		Testing	10%	131	YES

6. PERFORMANCE MEASURES

Many parameters are utilized for evaluating the performance of the proposed model and may include the sensitivity, receiver operator characteristic (ROC), area Under the ROC curve (AUC), F1-score, the Matthews correlation coefficient (MCC), and the Jaccard similarity index or intersection over union (IoU) [26][27]:

- **Sensitivity** is the ratio of correct predictions, specifically true positives, to the total number of true positives and false negatives. Sensitivity is calculated as follows [26]:

$$Recall\ or\ Sensitivity\ = TP/(TP + FN) \quad (2)$$

- **ROC curve** is another metric to assess the performance of several different models. A curve that approximates the 45° diagonal of the ROC space suggests less precise examinations. In general, the closer the curve aligns with the top-left corner, the greater the precision of the examination [26].

- **F1-score** is an embodiment of the weighted average of recall and precision. As a result, the utilization of this specific metric involves the inclusion of false negatives and false positives. The F1-score possesses a higher degree of importance and usefulness compared with accuracy, especially when dealing with imbalanced classes, equation [26]:

$$F_1 = \frac{2TP}{2TP+FN+FP} \quad (3)$$

7. RESULTS

S The experimental results reveal the excellent performance of the proposed U-Net model in determining and locating copy–move forged regions in images. The performance metrics of the proposed model trained on the CoMoFoD and CASIA2 datasets, as summarized in Tables 2 and 3, respectively.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

TABLE II. RESULTS OF THE COMOFOD DATASET

Phase	Acc. %	Prec. %	Recall %	F1 %	AUC %	MCC %	IoU %
Training	97.83	80.45	100	89.17	99.32	89.05	65.66
Validation	98.05	77.12	99.8	87.01	98.97	86.84	67.67
Testing	91.83	73.34	99.71	84.52	99.19	84.87	60.10

TABLE III. RESULTS OF THE CASIA2 DATASET

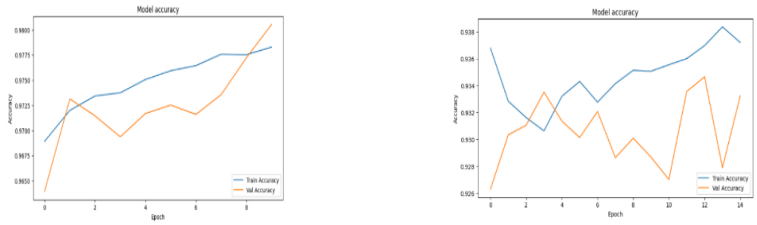
Phase	Acc. %	Prec. %	Recall %	F1 %	AUC %	MCC %	IoU %
Training	93.72	71.01	97.07	82.02	95.70	80.41	61.84
Validation	93.32	54.49	90.99	67.85	90.99	66.48	57.05
Testing	92.74	54.94	93.41	69.36	93.41	68.83	54.39

The proposed innovative U-Net model exhibited promising efficacy in detecting and locating of copy–move forgery within digital images. This model achieved notable levels of accuracy during the training and testing phases on the CoMoFoD and CASIA2 datasets. Specifically, on the CoMoFoD dataset, the model attained an accuracy of approximately 97.83% during the training phase and maintained similar levels of accuracy during the validation stage, up to 98.05% for validation, which correspondingly decreased during testing up to 91.83% for testing. On the CASIA2 dataset, the model achieved a slightly lower accuracy of around 93.72% during training, which correspondingly decreased during validation and testing up to 93.32% and 92.74% respectively.

The loss percentages indicate the disparity between the predicted values and the actual ground truth values. Lower loss percentages signify a greater agreement between the predicted and ground truth values, thus suggesting that the model effectively learned the underlying patterns within the training data. Figures 3 and 4 show the accuracy and loss function respectively.

F1-scores for the CoMoFoD and CASIA2 datasets indicate the overall accuracy of the U-Net model in correctly identifying forged regions in the images. MCC values reflect the overall performance of the U-Net model in accurately classifying forged regions, which is better across the CoMoFoD dataset than CASIA2.

AUC values are reported for both datasets during the testing phase, providing insights into the discriminatory power of the U-Net model in identifying forged regions, which is better across the CoMoFoD dataset than CASIA2. The ROC-AUC curve that reflects the model's performance is shown in Figure 5.



(a) (b)

Fig. 3. Accuracy of the Proposed Model: (a) Comofod Dataset and (b) CASIA2 Dataset

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

(a) (b)

Fig. 4. Loss Function of The Proposed Model: (a) Comofod Dataset and (b) CASIA2 Dataset

The visual representation of the model's output is highly important for qualitative evaluation, as shown in Figures 6 and 7. Columns (a), (b), and (c) show the input image, the ground truth mask, and (c) the model results, respectively. The examples of CMFD predicated output mask are highly similar to those of the ground truth mask. This finding implies that the proposed U-Net model exhibits robust performance in detecting and localizing manipulated regions in images.

For quantitative comparison with other works, Tables 4 and 5 provide a comprehensive overview of key performance metrics when applied on CoMoFoD and CASIA2, respectively. Moreover, the model achieves an impressive recall rate of 99.71%, implying that it successfully captures nearly all of the actual forged regions found within the dataset. This high recall rate ensures that the model effectively detects the majority of forged regions, thereby minimizing the occurrence of false negatives.

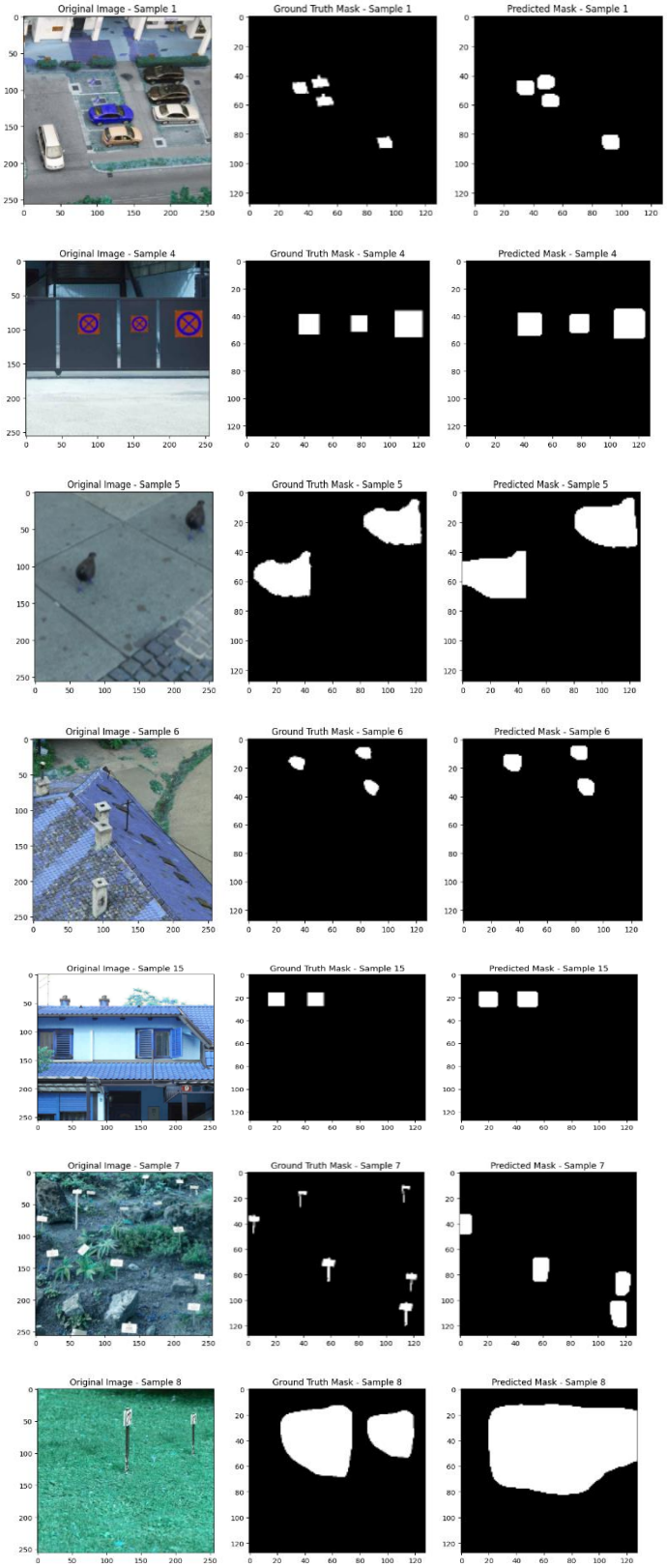
The visual representation of the model's output is highly important for qualitative evaluation, as shown in Figures 6 and 7. Columns (a), (b), and (c) show the input image, the ground truth mask, and (c) the model results, respectively. The examples of CMFD predicated output mask are highly similar to those of the ground truth mask. This finding implies that the proposed U-Net model exhibits robust performance in detecting and localizing manipulated regions in images.

For quantitative comparison with other works, Tables 4 and 5 provide a comprehensive overview of key performance metrics when applied on CoMoFoD and CASIA2, respectively. Moreover, the model achieves an impressive recall rate of 99.71%, implying that it successfully captures nearly all of the actual forged regions found within the dataset. This high recall rate ensures that the model effectively detects the majority of forged regions, thereby minimizing the occurrence of false negatives.

(a) (b)

Fig. 5. ROC-AUC Curve for the Proposed Model: (a) Comofod Dataset and (b) CASIA2 Dataset

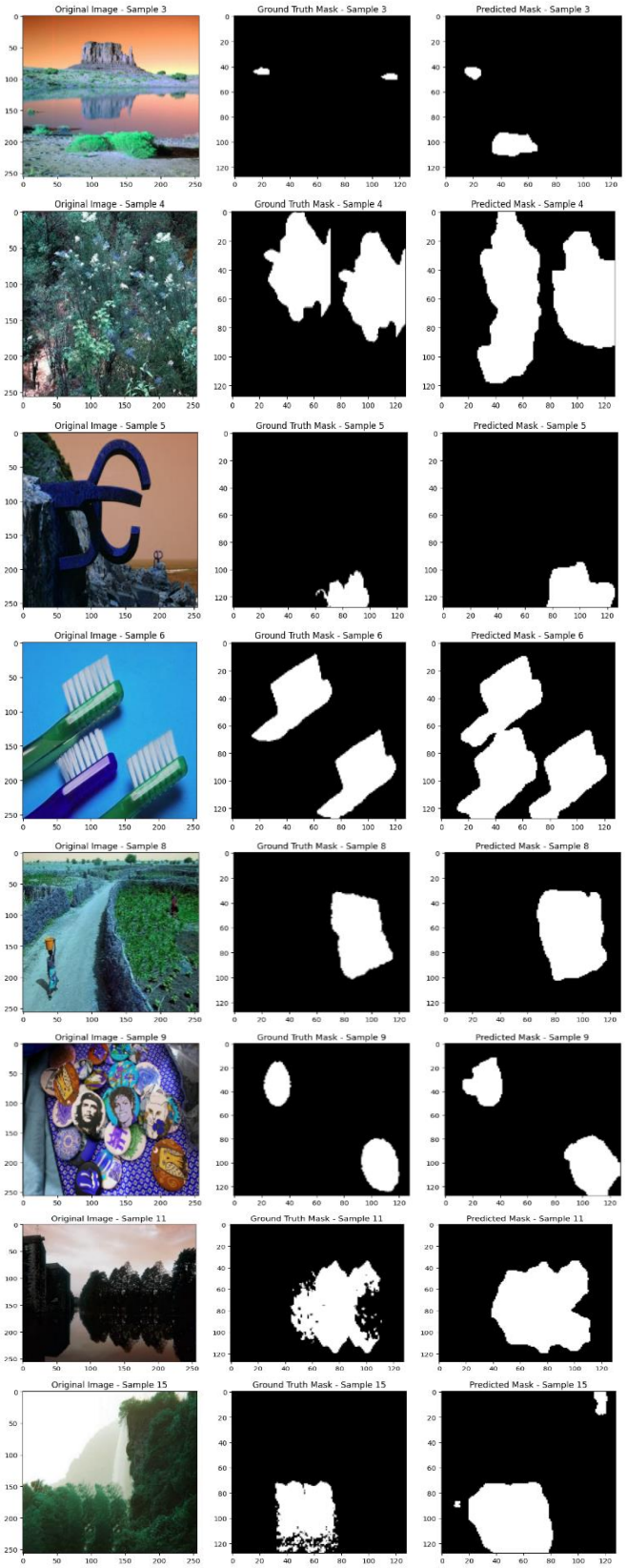
Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912



a b c

Fig. 6. Examples of CMFD Results using the Proposed Model Applied on Comofod Dataset: (a) Input Image, (b) Ground Truth Mask, and (c) Model Results

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912



(a) (b) (c)

Fig. 7. Results Of the U-Net Model Applied on CASIA2 Dataset: (a) Input Image, (b) Ground Truth Mask, and (c) CMFD Mask

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

TABLE IV. COMPARISON OF OUR U-NET WITH OTHER MODELS IN THE LITERATURE ON COMOFOD DATASET

Model	Dataset	Precision %	Recall %
Zernike Moments [28]	Only 12 images	83.59	76.63
Busternet [13]	CoMoFoD	57.34	49.39
Base [16]	CoMoFoD	47.68	38.11
Base-Ada-Atten [16]	CoMoFoD	46.61	40.75
AR-Net [16]	CoMoFoD	54.21	46.55
False-Unet [26]	CoMoFoD	NA	NA
Our Innovative Unet	CoMoFoD (480 images)	**73.34**	99.71

TABLE V. COMPARISON OF OUR U-NET WITH OTHER MODELS IN THE LITERATURE CASIA2 DATASET

Model	Acc. %	F1-Score %	AUC %	MCC %	IoU %
ManTra-Net [29]	NF	NF	81.7	NF	NF
Busternet [13]	76.84%	45.56%	93	NF	NF
FCN [30]	NF	67.58	NF	NF	NF
False-Unet [26]	NF	69.53	83.25	62.38	91.33
Our model	**92.74**	**69.36**	**93.41**	**68.38**	**54.39**

8. CONCLUSIONS

In this paper, an innovated machine learning-based model is proposed for the automatic detection of image forgery. The qualitative performance of this model is highly excellent in locating forged regions. Furthermore, the predicted mask shows that the predicted forged regions closely resemble the ground truth mask. For the quantitative evaluation, many metrics are used, such as accuracy, F1-scores, AUC values, MCC scores, and IoU metrics. The accuracy and effectiveness in identifying forged areas emphasize the potential of deep learning approaches to improve forgery detection methods and to eliminate human intervention completely. The proposed model is tested and evaluated on two different datasets, CoMoFoD and CASIA2 datasets, which offers various copy–move scenarios. The experimental results reveal that the model can detect forged images with high accuracy, reaching up to 92.74%.

References

[1] Y. Abdalla, M. Tariq Iqbal, and M. Shehata, "Copy-move forgery detection and localization using a generative adversarial network and convolutional neural-network," *Inf.*, vol. 10, no. 9, 2019, doi: 10.3390/info10090286.

[2] M. A. Elaskily, H. K. Aslan, O. A. Elshakankiry, O. S. Faragallah, F. E. A. El-Samie, and M. M. Dessouky, "Comparative study of copy-move forgery detection techniques," *ACCS/PEIT 2017 - 2017 Intl Conf Adv. Control Circuits Syst. 2017 Intl Conf New Paradig. Electron. Inf. Technol.*, vol. 2018-Febru, pp. 193–203, 2018, doi: 10.1109/ACCS-PEIT.2017.8303041.

[3] M. S. Mahdi and S. N. Alsaad, "Detection of Copy-Move Forgery in Digital Image Based on SIFT Features and Automatic Matching Thresholds," in *International Conference on Applied Computing to Support Industry: Innovation and Technology*, Springer, 2019, pp. 17–31.

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[4] I. A. Zedan, M. M. Soliman, K. M. Elsayed, and H. M. Onsi, "Copy Move Forgery Detection Techniques: A Comprehensive Survey of Challenges and Future Directions," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 7, 2021.

[5] X. Lin, J.-H. Li, S.-L. Wang, F. Cheng, and X.-S. Huang, "Recent advances in passive digital image security forensics: A brief review," *Engineering*, vol. 4, no. 1, pp. 29–39, 2018.

[6] B. Soni, P. K. Das, and D. M. Thounaojam, "CMFD: A detailed review of block based and key feature based techniques in image copymove forgery detection," *IET Image Process.*, vol. 12, no. 2, pp. 167–178, 2018, doi: 10.1049/iet-ipr.2017.0441.

[7] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2016-Decem, pp. 770–778, 2016, doi: 10.1109/CVPR.2016.90.

[8] M. A. Elaskily *et al.*, "A novel deep learning framework for copy-moveforgery detection in images," *Multimed. Tools Appl.*, vol. 79, no. 27–28, pp. 19167–19192, 2020, doi: 10.1007/s11042-020-08751-7.

[9] B. D. A. S. S. (PRADIP K.), *IMAGE COPY-MOVE FORGERY DETECTION: New Tools and Techniques*. SPRINGER VERLAG, SINGAPOR, 2023.

[10] 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, 2019, doi: 10.1007/s42044-019-00029-y.

[11] B. Yang, X. Sun, H. Guo, Z. Xia, and X. Chen, "A copy-move forgery detection method based on CMFD-SIFT," *Multimed. Tools Appl.*, vol. 77, no. 1, pp. 837–855, 2018, doi: 10.1007/s11042-016-4289-y.

[12] Y. Yao, Y. Shi, S. Weng, and B. Guan, "Deep learning for detection of object-based forgery in advanced video," *Symmetry (Basel).*, vol. 10, no. 1, p. 3, 2017.

[13] Y. W. B, W. Abd-almageed, and P. Natarajan, *BusterNet : Detecting Copy-Move Image Forgery with Source / Target Localization*, vol. 1. Springer International Publishing, 2018. doi: 10.1007/978-3-030-01231-1.

[14] Y. Liu, Q. Guan, X. Zhao, and Y. Cao, "Image forgery localization based on multi-scale convolutional neural networks," in *Proceedings of the 6th ACM workshop on information hiding and multimedia security*, 2018, pp. 85–90.

[15] X. Bi, Y. Wei, B. Xiao, and W. Li, "RRU-Net: The ringed residual U-Net for image splicing forgery detection," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 2019, p. 0.

[16] 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 Trans. Ind. Informatics*, vol. 16, no. 10, pp. 6714–6723, 2020, doi: 10.1109/TII.2020.2982705.

[17] A. Kumar, A. Bhavsar, and R. Verma, "Syn2real: Forgery classification via unsupervised domain adaptation," in *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops*, 2020, pp. 63–70.

[18] B. Ahmed, T. Aaron Gulliver, and S. alZahir, "Localization and Detection of Copy-Move Forgeries in Post-processed Images Using U-Net," *SN Comput. Sci.*, vol. 2, no. 6, 2021, doi: 10.1007/s42979-021-00893-1.

[19] Y. Huang, S. Bian, H. Li, C. Wang, and K. Li, "DS-UNet: A dual streams UNet for refined image forgery localization," *Inf. Sci. (Ny).*, vol. 610, pp. 73–89, 2022.

[20] S. Weng, T. Zhu, T. Zhang, and C. Zhang, "UCM-Net: A U-Net-like tampered-region-related framework for copy-move forgery detection," *IEEE Trans. Multimed.*, 2023.

[21] N. V Chawla, N. Japkowicz, and A. Kotcz, "Special issue on learning from imbalanced data sets," *ACM SIGKDD Explor. Newsl.*, vol. 6, no. 1, pp. 1–6, 2004.

[22] H. He and E. A. Garcia, "Learning from imbalanced data," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 9, pp. 1263–1284, 2009.

[23] K. Singh, "How to Improve Class Imbalance using Class Weights in Machine Learning." https://www.analyticsvidhya.com/blog/2020/10/improve-class-imbalance-class-weights/#

Iraqi Journal for Computers and Informatics
Information Technology and Communications University
Vol. 50, No. 1, 2024, pp. 195-207
DOI: https://doi.org/10.25195/ijci.v49i2.484
Print ISSN: 2313-190X, Online ISSN: 2520-4912

[24] J. Dong, W. Wang, and T. Tan, "Casia image tampering detection evaluation database," in *2013 IEEE China summit and international conference on signal and information processing*, IEEE, 2013, pp. 422–426.

[25] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, "CoMoFoD—New database for copy-move forgery detection," in *Proceedings ELMAR-2013*, IEEE, 2013, pp. 49–54.

[26] F. Z. El Biach, I. Iala, H. Laanaya, and K. Minaoui, "Encoder-decoder based convolutional neural networks for image forgery detection," *Multimed. Tools Appl.*, vol. 81, no. 16, pp. 22611–22628, 2022, doi: 10.1007/s11042-020-10158-3.

[27] B. Ahmed, T. A. Gulliver, and S. alZahir, "Image splicing detection using mask-RCNN," *Signal, Image Video Process.*, vol. 14, no. 5, pp. 1035–1042, 2020.

[28] S.-J. Ryu, M.-J. Lee, and H.-K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Information Hiding: 12th International Conference, IH 2010, Calgary, AB, Canada, June 28-30, 2010, Revised Selected Papers 12*, Springer, 2010, pp. 51–65.

[29] Y. Wu, W. AbdAlmageed, and P. Natarajan, "Mantra-net: Manipulation tracing network for detection and localization of image forgeries with anomalous features," in *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, 2019, pp. 9543–9552.

[30] B. Xiao, Y. Wei, X. Bi, W. Li, and J. Ma, "Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering," Inf. Sci. (Ny)., vol. 511, pp. 172–191, 2020.