Mask FORD-NET: Efficient Detection of Digital Image Forgery using Hybrid REG-NET based Mask-RCNN

Original Scientific Paper

Priscilla Whitin*
Department of Electrical and Electronics Engineering,
VelTech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Chennai, Tamil Nadu, India.
priscillawhitin@veltech.edu.in

S. Sivakumar
Department of Electrical and Electronics Engineering,
VelTech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Chennai, Tamil Nadu, India.
ssivakumar@veltech.edu.in

M. Geetha
Department of Electrical and Electronics Engineering,
Sri Eshwar College of Engineering,
Coimbatore, Tamil Nadu, India.
geetha.m@sece.ac.in

M. Devaki
Department of Electrical and Electronics Engineering,
Velammal College of Engineering and Technology,
Madurai, Tamilnadu, India.
devaki852m@outlook.com

A. Bhuvanesh
Department of Electrical and Electronics Engineering,
PSN College of Engineering and Technology,
Tirunelveli, Tamilnadu, India.
bhuvanesh.ananthan@gmail.com

Kiruthiga Balasubramaniyan
Department of Electronics and Communication Engineering,
K. Ramakrishnan College of Technology,
Trichy, Tamilnadu, India.
balasubramaniyankiruthiga44@gmail.com

A. Ahilan
Department of Electronics and Communication Engineering,
PSN College of Engineering and Technology,
Tirunelveli, Tamilnadu, India.
listentoahil@gmail.com

*Corresponding author

Abstract *–Digital image is a binary representation of visual data which provides a rapid method for analyzing large quantities of data. Furthermore, digital images are more vulnerable to fraud when distributed over an open channel via information and communication technology. However, the image data can be modified fraudulently by intruders using vulnerabilities in telecommunications infrastructure. To overcome these issues, this paper proposes a novel Mask-RCNN based Image FORgery Detection (Mask FORD-NET) which is developed for digital image forgery detection. Initially, the input image is passed beyond the recompression module to reduce the insignificance and complexity of the image to preserve or transfer the data efficiently. After image recompression, the recompressed image is transferred to the feature extraction phase which is done by using REG-NET. The extracted features are received to the noise cancellation and ELA converter module to analyze and reduce the ambient noise. After noise cancellation, the data are passed to the MASK-RCNN module, to detect and classify the forged images and finally provide the segmented output. The Mask FORD-NET framework is simulated by using MATLAB. The efficiency of the proposed Mask FORD-NET framework is assessed by using accuracy, precision, recall, and F1-measure. The experimental results show that the accuracy of the Mask FORD-NET framework has increased to up to 98.72% for digital image forgery detection. The accuracy of the proposed Mask FORD-NET framework is 80.72%, 86.32%, and 95.00% better than existing ASCA, VixNet, and MiniNet techniques respectively.*

Keywords: *Digital Image Forgery, Deep Learning, REG-NET, Mask-RCNN*

Received: January 26, 2024; Received in revised form: July 29, 2024; Accepted: August 2, 2024

1. INTRODUCTION

The widespread availability of digital images due to the advancement of imaging technology and the profusion of image manipulation applications that do not require specialized knowledge has led to a significant rise in the number of forged digital images on social media [1-3]. Digital images are used in many industries, including social networking, e-government, military information, and meteorological research [4, 5]. By 2022, 72.6% of the world's population, according to the International Telecommunication Union (ITU), will have access to the Internet. This implies that about 4.1 billion people will have access to these technologies as well as other services [6].

Active and passive methods are the two categories that are utilized for digital image forgery techniques [7, 8]. The passive adaptive detection technique analyses the original image and identifies regions in which the image has been altered using several statistical and semantic criteria linked to the content of the image. The main aim of the detection method for image forgery, that address the increasing issue of image forgery [9, 10]. Digital image forensics experts can employ Deep Learning (DL) and Machine Learning (ML) to appear for forged images. It has been demonstrated that these methods offer high accuracy rates and provide protection against a wide variety of image forgery [11, 12].

Due to their reliance on JPEG compression artifacts, digital images are useful but limited in their ability to reliably detect extremely intricate counterfeits [13, 14]. Furthermore, it is challenging to understand the results and make conclusions due to the transparent nature of the digital image forgery detection process [15]. To resolve these shortcomings, a novel Mask FORD-NET framework is proposed for digital image forgery detection. The main contributions of the proposed Mask FORD-NET framework are presented as follows.

- Initially, the input image is passed beyond to the recompression module to reduce the insignificance and complexity of the image in an efficient manner.
- After image recompression, the recompressed image is transferred to the feature extraction phase which is done by using REG-NET.
- The extracted features are received to the noise cancellation and ELA converter module to analyze and reduce the ambient noise.
- After noise cancellation, the data are passed to the MASK-RCNN module, to detect and classify the forged images and finally provide the segmented output.
- The effectiveness of the proposed Mask FORD-NET framework is evaluated by accuracy, specificity, precision, F_measure, and recall respectively.

The work described in this paper is organized as follows: Section 2 presents a summary of related work. Section 3 presents the deep learning-based Mask FORD-NET framework for image forgery detection. Section 4 provides a thorough explanation of the Framework's Outputs and performance assessment. Conclusions and future work are presented in Section 5.

2. LITERATURE SURVEY

Advanced techniques for identifying changes done on virtual images have emerged as a result of recent trends in image tampering. Earlier studies have been put forth based on various methods such as ML and DL that are mostly predicated on observations made during the entire image history. The following is a brief definition of several related works.

In 2022, Koul et al. [16] proposed a method using convolutional neural networks to detect clone-based image manipulation. The MICC-F2000 dataset is used to assess the suggested method, which detects fake copies with 97.52% accuracy. However, the suggested approach consists of an increased false positive rate. In 2022 Wu et al. [17] suggested a reliable image tampering detection for social media streaming. The suggested method reduces IoU by 2.6%, 2.9%, and 4.5%, on the dataset that OSN transmitted. However, the suggested approach fails to perform robustly in complex degradation scenarios.

In 2022 Kumar et al. [18] suggested using a variation in non-overlapping blocks, the detection, and location of image manipulation. With 98% accuracy for improved detection and classification, the suggested technique is assessed using SSIM parameters. However, the suggested approach consists of high computational complexity. In 2022 Ganguly et al. [19] suggested a Vision Transformer that uses the Xception Network to detect video and image forgeries based on deepfakes. The ViXNet approach was evaluated on the DFDC dataset, generating an F1 score of 79.06% and an AUC score of 86.32% for identifying hypothetical fraudsters. However, the advantages of the deepfake detection techniques still need improvement.

In 2023 Nirmalapriya et al. [20] suggested a Hybrid deep learning network can identify digital image manipulation via Aquila's sin-cosine algorithm. A replicated fraudulent detection dataset is used to assess the suggested approach, which yields TNR and TPR values of 1.003% and 0.991%, respectively. However, the suggested ASCA method is not reversible. In 2023 Sushir et al. [21] suggested enhanced detection of random image manipulation based on accurate deep learning utilizing a combination of DCCAE and ADFC. The accuracy of the suggested hybrid DCCAE approach is 98.07% for the GRIP dataset and 99.23% for the CASIA V1 dataset. However, the noise estimation of the suggested approach is not robust.

In 2023, Tyagi and Yadav [22] suggested an immediate CNN for spotting forged images. For 140,000 real and fake faces, the suggested MiniNet version obtains

an accuracy of above 95%, and for the CASIA dataset, it achieves 93%. However, the suggested MiniNet model consists of low precision. In 2023 Vijayalakshmi et al. [23] suggested utilizing deep learning and error-level analysis, to detect counterfeits through copy-and-paste methods. Using the MICC-F220 dataset, the suggested approach was assessed and yielded an overall 99.2% accuracy, 96.5% specificity, 95.79% recall, and 96.09% F_measure for improved detection. However, the suggested approach is not highly efficient.

The aforementioned findings indicate that the majority of manual feature extraction techniques for counterfeit detection mainly rely on the operator. Mask FORD-NET framework, a deep learning framework that is designed to identify the manipulation of digital images. In this framework, the time complexity is decreased, efficiency is increased, and potential human mistake is eliminated when using the Mask FORD-NET framework.

2.1. RESEARCH GAP

Following a thorough examination of the literature, the following research gaps on the suggested research challenge were identified. Although much progress has been made, there are still several barriers that prevent useful techniques from being used. The deep learning-based development of the Mask-FORD-NET framework for digital image forgery is still occurring continuously. Recent image processing techniques depend on numerous attributes. Most approaches employ DL or ML techniques to identify image modification. Reviewing the literature, however, reveals that there is a significant improvement in deep learning-based image intrusion detection.

3. THE MASK FORD-NET METHODOLOGY

In this section, a novel deep-learning based Mask FORD-NET framework is proposed for the digital image forgery detection. Fig. 1 depicts the block diagram of the Mask FORD-NET architecture.

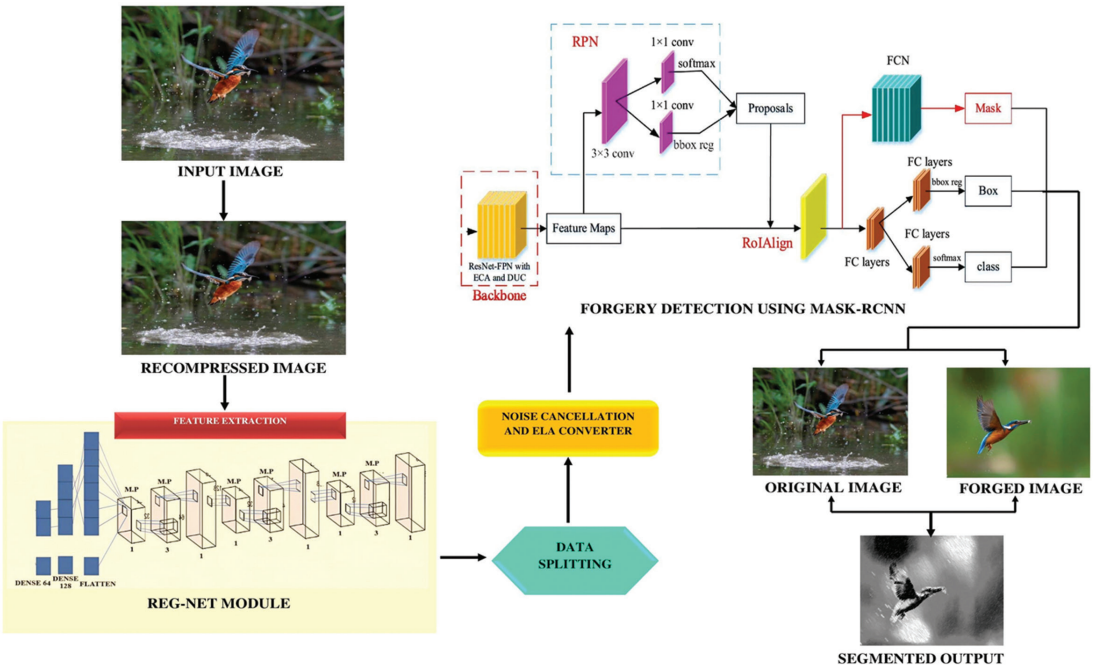

Fig. 1. The block diagram of the Mask FORD-NET framework

3.1. DATA RECOMPRESSION

The proposed method presents a framework for confirming the authenticity of fake images. This technique locates tampered locations and detects image tampering by using data compression features. In step size 2, this was completed in the interval [30, 100]. YCbCr is used in place of the RGB color system. The image's brightness information is stored in the Y channel, while the Cb and Cr channels hold the color information. The difference image is transformed to binary, where black and white regions indicate the original and modified portions of the image, to visualize the altered regions.

3.2. FEATURE EXTRACTION USING REG-NET

To extract features from compressed digital images, two types of ResNet building blocks were proposed such as bottleneck building blocks and non-bottleneck building blocks. Based on this, two different RNN-modified ResNet structural modules were obtained, one using ConvRNN as the regulator and the other using an RNN-modified ResNet structural module.

3.2.1. RegNet Module

ConvLSTM's output from the first module, H^{t1}, is represented by that from the second module, H^{t}. The mod-

ule's feature map is represented by X_i^t. The t-th RegNet (ConvLSTM) module can be expressed as

$$X_2^t = ReLU\big(BN(W_{12}^t * X_1^t + b_{12}^t)\big), \quad (1)$$

$$[H^t, C^t] = ReLU\left(BN\big(ConvLSTM(X_2^t, [H^{t-1}, C^{t-1}])\big)\right), \quad (2)$$

$$X_3^t = ReLU\big(BN(W_{23}^t * Concat[X_2^t, H^t])\big), \quad (3)$$

$$X_4^t = BN(W_{34}^t * X_3^t + b_{34}^t), \quad (4)$$

$$X_1^{t+1} = ReLU(X_1^t + X_4^t) \quad (5)$$

where b_{ji}^t stands for the correlation distance and W_{ij}^t stands for the convolution kernel that translates the features X_i^t to X_j^t. They are 3x3 convolution particles, $W_{12}{}^t$, $W_{34}{}^t$ and $W_{23}{}^t$ consists of 1x1 kernels. The batch normalization procedure is represented by BN (). Concat [] is a shorthand for the concatenation operation. The enter entity $X_2{}^t$ and the previous output of *ConvLSTM* H^t in equation (1) are the input of *ConvLSTM* inside the module. *ConvLSTM* automatically determines whether the data inside the memory cell should be given to the H^t output hidden characteristic map based on the inputs.

3.2.2. Bottleneck RegNet Module

The fundamental component of the RegNet bottleneck module is the ResNet bottleneck building block. For large image processing, the bottleneck construction block was first presented. This makes it possible to represent the RegNet module bottleneck as,

$$X_2^t = ReLU\big(BN(W_{12}^t * X_1^t + b_{12}^t)\big), \quad (6)$$

$$[H^t, C^t] = ReLU\left(BN\big(ConvLSTM(X_2^t, [H^{t-1}, C^{t-1}])\big)\right), \quad (7)$$

$$X_3^t = ReLU\big(BN(W_{23}^t * X_2^t + b_{23}^t)\big), \quad (8)$$

$$X_4^t = ReLU\big(BN(W_{34}^t * Concat[X_3^t, H^t])\big), \quad (9)$$

$$X_5^t = BN(W_{45}^t * X_4^t + b_{45}^t), \quad (10)$$

$$X_1^{t+1} = ReLU(X_1^t + X_5^t), \quad (11)$$

where $W_{12}{}^t$ and $W_{45}{}^t$ are the two 1×1 kernels, and $W_{23}{}^t$ is the 3×3 bottleneck kernel. The $W_{34}{}^t$ is a 1×1 kernel for fusing features in our model.

3.3. NOISE-CANCELLATION AND ELA CONVERSION

Two important techniques were used in image forgery detection which are noise cancellation and ELA (Error Level Analysis). An image can be made noise-free by using a technique called noise removal. Noise elimination can be applied to detect altered images by eliminating artificial noise or artifacts that may have been introduced during the tampering process. The process involves using a DL algorithm to extract a variety of features from an image to identify tampering and filtering techniques are used to detect the noise in the images. Once the noise is identified, it can be removed using various filtering techniques, such as a median filter or a Gaussian filter. By removing the noise, the algorithm can focus on the underlying structure of the image, which may provide clues about the forgery. However, ELA can be used to identify regions of an image that have been altered or compressed. ELA operates by interpreting differences in the degree of inaccuracy in various areas of an image. When an image is recompressed or modified, the error levels in the affected regions will be higher than in other areas of the image. Combining noise cancellation and ELA methods makes it possible to generate algorithms for identifying fake images that are more reliable and accurate.

3.4. DIGITAL IMAGE FORGERY DETECTION USING MASK R-CNN

Mask R-CNN enables the proper labeling of object regions and removals of those object regions from the background of each pixel level. Furthermore, Mask R-CNN may be utilized to detect the forged parts of the digital images by examining the form and edge properties of its mask images.

3.4.1. Feature pyramid network

In DL, feature extraction is a vital phase employed for extracting the relevant features present in the digital images. Especially, for feature extraction ResNet-101 is used as a feature pyramid network (FPN) model over an entire digital image. The ResNet-101 model uses the suggested rectangular zones to extract features, which are convolved into Mask R-CNN. The input data is fed into the convolutional CNN to generate the feature map. Convolutional layers are stacked, pooling layers are added, and ResNet-101 retains the residual connections. Five blocks comprise a convolutional network such as a 7x7 convolutional layer used in the first block, then 1x1, 3x3, and 1x1 convolutional layers are used in consecutive blocks. FPN strengthens the network backbone so that semantic and spatial information can be extracted from different-sized digital images.

3.4.2. Region proposal network

A Region Proposal Network (RPN) was utilized to create regions of interest with fixed points for every feature map. Multiple propositions are generated on rectangular objects with objective scores by superimposing convolutional feature maps across a small network. The digital image's foreground and background values were ascertained in this manner. The server adjusted the size and position of the digital images and chose the best limits using RPN prediction. Finally, using the regions of interest generated by the RPN layer, the FC layer builds bounding boxes and segmentation masks for particular areas of the digital image.

3.4.3. Fully convolutional network

ROI Align is utilized to modify each ROI's size to satisfy the FC input requirements before utilizing the full convolutional input. To extract pertinent attributes

from each RoI on the feature map, RoI Align employed bilinear interpolation as an alternative to the Mask R-CNN approach of RoI pooling equalization. Three prediction branches, a fully convolutional network (FCN), which is used for both classification and prediction segmentation. A regression layer, which modifies bounding box coordinates, and an FC layer, which is used for classification combined to generate the target mask in the multi-branch prediction stage. For both segmentation, bounding box classification, and analysis, the ROI alignment characteristics are fed into the head mask and bounding box head simultaneously. Through the use of all the characteristics in the soft-max layer, the results are fed to the FCN layer for classification.

Table 1. Hyperparameter settings of the proposed REG-NET technique

Parameter	Value
Training Data Ratio	60%
Validation Data Ratio	20%
Testing Data Ratio	20%
Training Time	10 hours
Optimizer	Adam
Cost Function	Binary Cross-Entropy
Batch size	64
Learning Rate	0.0001
Activation Function	Leaky ReLU
Number of Epochs	100

The hyperparameters of the proposed Mask FORD-NET method are covered in Table 1. Experimenting with different combinations of these hyperparameters can help in optimizing the performance of REG-NET for image forgery detection.

4. PERFORMANCE VALIDATION RESULT ANALYSIS

The experimental results of existing detection models and the proposed Mask FORD-NET framework are compared and analyzed in this section. The proposed work's performance is assessed using accuracy. As seen in the attached figures, it offer a thorough evaluation of the model's overall performance at a deep level of comprehension of the input data.

Dataset Description

To assess the efficacy of the proposed Mask FORD-NET framework, experiments are conducted on the widely used image tampering database, CASIA 2.0. The total number of images such as 12,614 images in BMP, JPG, and TIF formats, 5,123 are fictitious images and 7,491 are real shots presented in the dataset. Images from many genres are included in CASIA 2.0, such as those featuring people, animals, plants, architecture, objects, landscapes, textures, and interior shots. The collection contains images in a range of sizes and resolutions, from 800 x 600 pixels to 384 x 256 pixels.

4.1. PERFORMANCE METRICS

The accuracy, precision, recall and $F_{measure}$ is calculated and compared to the proposed strategy with existing approaches. They are computed as follows.

$$Accuracy = \frac{T_P+T_N}{T_{Total\_Images}} \times 100 \quad (12)$$

$$Recall = \frac{T_P}{T_P+F_N} \quad (13)$$

$$Precision = \frac{T_P}{T_P+F_P} \quad (14)$$

$$F_{measure} = \frac{2\times Recall\times Precision}{Recall+Precision} \times 100 \quad (15)$$

4.2. PERFORMANCE ANALYSIS

Fig. 2 and 3 demonstrate the proposed Mask FORD-NET framework with great accuracy throughout both training and testing.

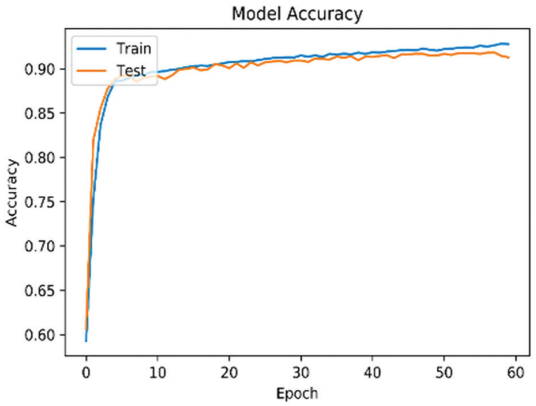

Fig. 2. Accuracy Calculation of existing Algorithm

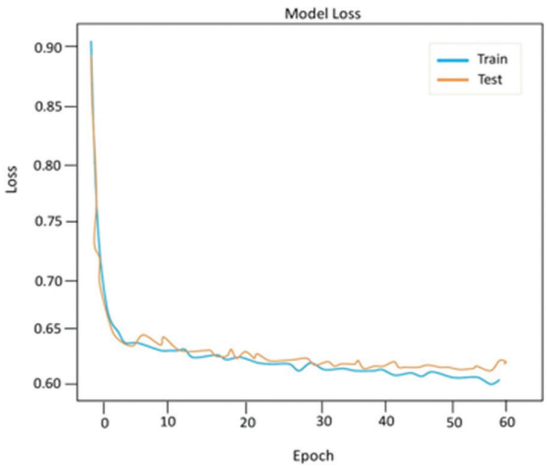

Fig. 3. Loss Calculation of Existing Algorithm

4.3. COMPARATIVE ANALYSIS

In Fig. 4, the image (A) of the table shows the input image and the image (B) of the figure shows the forged image. The image (C) of the figure insists the recompressed image and the extracted features are depicted in image (D). Finally, the segmented output is shown in image (E).

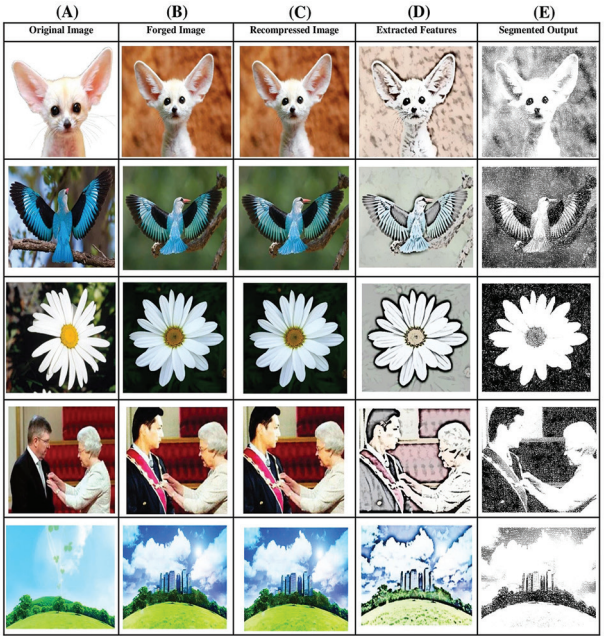

Fig. 4. Result of the proposed methodology

In comparison to alternative ways, Fig. 5 provides a better depiction of the accuracy of the proposed approach. The experimental results show that the Mask FORD-NET framework achieves 98.72% of accuracy, 90.36% of specificity, 92.25% of precision, 93.53% of F1-score, and 94.99% of recall for digital image forgery detection. The accuracy of the proposed Mask FORD-NET framework is 80.72%, 86.32%, and 95.00% better than existing ASCA, VixNet, and MiniNet techniques respectively.

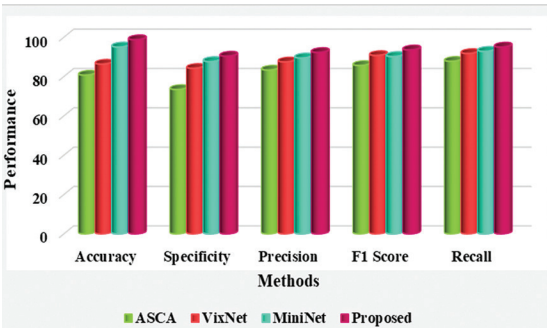

Fig. 5. Performance evaluation of existing approach

From the result analysis, we can infer that the suggested work's accuracy is 95.56 and its processing time is 31 milliseconds, compared to the existing system's accuracy of 92.23 and processing time of 30 milliseconds. For the suggested task to be accomplished more quickly and with greater precision. The existing and proposed DL approaches are graphically compared in Fig. 6. using several criteria, including accuracy, sensitivity, recall, and specificity.

The accuracy of the Bi-LSTM approach is 93.81%, the RCNN approach is 94.74%, and the corresponding accuracy of the REG-NET method is 95.47% both lower than the accuracy of the proposed Mask-RCNN methodology of 97.84% respectively.

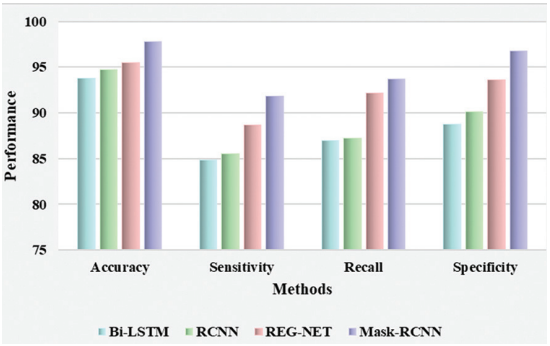

Fig. 6. Successive Rate of Mask-RCNN

5. CONCLUSION

This paper proposed a novel Mask FORD-NET framework which is developed for digital image forgery detection. Initially, the input image is passed through the recompression module to efficiently reduce insignificance and complexity. The recompressed image is then sent to the feature extraction phase using REG-NET. The extracted features are processed by the noise cancellation and ELA converter module to reduce ambient noise. Subsequently, the data are passed to the MASK-RCNN module for detecting and classifying forged images, ultimately providing the segmented output. The proposed Mask FORD-NET framework is validated by using the CASIA 2.0 image forgery dataset. The Mask FORD-NET framework is simulated by using MATLAB. According to the simulation results, a comparison is made between the proposed Mask FORD-NET framework and the existing approaches such as ASCA, VixNet, and MiniNet in terms of accuracy, precision, recall, sensitivity, and $F_{measure}$. The experimental results show that the accuracy of the Mask FORD-NET framework has increased to up to 98.72% for digital image forgery detection. The accuracy of the proposed Mask FORD-NET framework is 80.72%, 86.32%, and 95.00% better than existing ASCA, VixNet, and MiniNet techniques respectively. In the future, integrating multiple modalities such as text and audio, along with image content analysis, to detect sophisticated multimedia forgeries and deepfake content. Additionally, to pave the path for further study on identifying various forms of image forgery, the proposed Mask FORD-NET framework will aid in the field of image forgery detection.

6. REFERENCES:

[1] N. Kaur, N. Jindal, K. Singh, "A deep learning framework for copy-move forgery detection in digital images", Multimedia Tools and Applications, Vol. 82, No. 12, 2023, pp. 17741-17768.

[2] A. K. Jaiswal, R. Srivastava, "Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model", Neural Processing Letters, Vol. 54, No. 1, 2022, pp. 75-100.

[3] S. Walia, K. Kumar, M. Kumar, "Unveiling digital image forgeries using Markov based quaternions in frequency domain and fusion of machine learning algorithms", Multimedia Tools and Applications, Vol. 82, No. 3, 2023, pp. 4517-4532.

[4] M. A. Anwar, S. F. Tahir, L. G. Fahad, K. Kifayat, "Image forgery detection by transforming local descriptors into deep-derived features", Applied Soft Computing, Vol. 147, 2023, p. 110730.

[5] W. Lu, W. Xu, Z. Sheng, "An interpretable image tampering detection approach based on cooperative game", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 33, No. 2, 2022, pp. 952-962.

[6] G. Zhao, C. Qin, H. Yao, Y. Han, "DNN self-embedding watermarking: Towards tampering detection and parameter recovery for deep neural network", Pattern Recognition Letters, Vol. 164, 2022, pp. 16-22.

[7] T. Nazir, M. Nawaz, M. Masood, A. Javed, "Copy move forgery detection and segmentation using improved mask region-based convolution network (RCNN)", Applied Soft Computing, Vol. 131, 2022, p. 109778.

[8] C. You, H. Zheng, Z. Guo, T. Wang, X. Wu, "Tampering detection and localization base on sample guidance and individual camera device convolutional neural network features", Expert Systems, Vol. 40, No. 1, 2023, p. e13102.

[9] G. Mariappan, A. R. Satish, P. B. Reddy, B. Maram, "Adaptive partitioning-based copy-move image forgery detection using optimal enabled deep neuro-fuzzy network", Computational Intelligence, Vol. 38, No. 2, 2022, pp. 586-609.

[10] Y. Rao, J. Ni, W. Zhang, J. Huang, "Towards jpeg-resistant image forgery detection and localization via self-supervised domain adaptation", IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, pp. 1-12. (in press)

[11] D. R. Ramji, C. A. Palagan, A. Nithya, A. Appathurai, E. J. Alex, "Soft computing-based color image demosaicing for medical Image processing", Multimedia Tools Applications, Vol. 79, 2020, pp. 10047-10063.

[12] P. G. Sreelekshmi, M. Bhagavathi Priya, V. Vishu, "Deep forgery detect: enhancing social media security through deep learning-based forgery detection", International Journal of Data Science and Artificial Intelligence. Vol. 1, No. 1, 2023, pp. 9-19.

[13] R. Ganeshan, S. Muppidi, D. R. Thirupurasundari, B. S. Kumar, "Autoregressive-Elephant Herding Optimization based Generative Adversarial Network for copy-move forgery detection with Interval type-2 fuzzy clustering", Signal Processing: Image Communication, Vol. 108, 2022, p. 116756.

[14] S. Kumar, S. K. Gupta, M. Kaur, U. Gupta, "VI-NET: A hybrid deep convolutional neural network using VGG and inception V3 model for copy-move forgery classification", Journal of Visual Communication and Image Representation, Vol. 89, 2022, p. 103644.

[15] C. You, H. Zheng, Z. Guo, T. Wang, X. Wu, "Tampering detection and localization base on sample guidance and individual camera device convolutional neural network features", Expert Systems, Vol. 40, No. 1, 2023, p. e13102.

[16] S. Koul, M. Kumar, S. S. Khurana, F. Mushtaq, K. Kumar, "An efficient approach for copy-move image forgery detection using convolution neural network", Multimedia Tools and Applications, Vol. 81, No. 8, 2022, pp. 11259-11277.

[17] H. Wu, J. Zhou, J. Tian, J. Liu, Y. Qiao, "Robust image forgery detection against transmission over online social networks", IEEE Transactions on Information Forensics and Security, Vol. 17, 2022, pp. 443-456.

[18] S. Kumar, S. K. Gupta, U. Gupta, M. Agarwal, "Non-overlapping block-level difference-based image forgery detection and localization (NB-localization)", The Visual Computer, Vol. 39, No. 12, 2023, pp. 6029-6040.

[19] S. Ganguly, A. Ganguly, S. Mohiuddin, S. Malakar, R. Sarkar, "ViXNet: Vision Transformer with Xception Network for deepfakes based video and image forgery detection", Expert Systems with Applications, Vol. 210, 2022, p. 118423.

[20] G. Nirmalapriya, B. Maram, R. Lakshmanan, M. Navaneethakrishnan, "ASCA-squeeze net: Aquila sine cosine algorithm enabled hybrid deep learning networks for digital image forgery detection", Computers & Security, Vol. 128, 2023, p. 103155.

[21] R. D. Sushir, D. G. Wakde, S. S. Bhutada, "Enhanced blind image forgery detection using an accurate deep learning-based hybrid DCCAE and ADFC", Multimedia Tools and Applications, Vol. 83, 2024, pp. 1725-1752.

[22] S. Tyagi, D. Yadav, "MiniNet: a concise CNN for image forgery detection", Evolving Systems, Vol. 14, No. 3, 2023, pp. 545-556.

[23] K. N. V. S. K. Vijayalakshmi, J. Sasikala, C. Shanmuganathan, "Copy-paste forgery detection using deep learning with error level analysis", Multimedia Tools and Applications, Vol. 83, No. 2, 2024, pp. 3425-3449.