DOI:10.26524/krj.2023.19

Kongunadu Research Journal 10 (2): 81-88, 2023 ISSN 2349-2694, All Rights Reserved,
Publisher: Kongunadu Arts and Science College, Coimbatore. https://krjournal.com/index.php/krj/article/view/632

RESEARCH ARTICLE

FSM and RRU-net module for Image Splicing Forgery Detection

Velmurugan, S.[1],*, Saravana Moorthy, R.[1], Subramanian, K.[2] and Angel, S.[3]
[1]Department of Computer Science, Kongunadu Arts and Science College, Coimbatore -641029,
Tamil Nadu, India
[2]Department of IT and Analytics, Xavier Institute of Management and Entrepreneurship (XIME),
Bangalore, India
[3]Department of Computer Science (SF), Avanishilingam University, Coimbatore,
Tamil Nadu, India

ABSTRACT

Nowadays, it can be difficult to tell whether an image is real or fake. Thanks to technological advancements, an image can be altered or falsified in a matter of seconds. Finding these forgeries has grown to be a major problem in the modern world. Although an image could be crucial evidence, it will be useless if it is faked. Methods for distinguishing between pictures that have been edited and those that have been computer-generated must be developed. In order to identify these forgeries, we plan to create an Image Forgery Detection Model that combines FSM and RRU-Net. Residual propagation and residual feedback are two distinct approaches that are combined in RRU-Net, which stands for Ringed Residual Structure and Network Architecture. To find long-distance dependencies, the Feature Similarity Module, or FSM, will be employed. Our suggested system combines FSM and RRU-Net to improve accuracy. We will extract the differences in the picture attributes between the modified and unmodified parts using image patches of different sizes. Once the forged area has been identified, the final region will be shown in color. The method will prove useful in the future for identifying different types of spliced image frauds that appear on different social media platforms.

Keywords: RU-Net, residual propagation, residual feedback, spliced image

1. INTRODUCTION

Digital photos are seen as critical data in many applications. It can serve as evidence in a number of contexts, such as social networks, computer-aided medical diagnosis systems, tribunals, and the armed forces. Depending on how important the content is, it is imperative to verify an image's validity and prevent tampering. With the assistance of internet computer programs, users and common people can simply modify digital images. As a result, it is challenging for the human eye to recognize these false images. Because there are so many fraud tools available, it is imperative to determine if two types of photographs are real or fake. Stated differently, it is critical to have techniques for identifying photos that aren't real.

As seen in Fig. 1, the primary methods for identifying an image forgery can be generally divided into two categories: active and passive methods [1]. Adding digital signatures and watermarks to images while they are being taken is the core of the active approach. We can hide important image details and change accurate information into erroneous information by using the passive method. Digital picture counterfeiting can be divided into five categories: copy-move forgery, image splicing, retouching, morphing, and enhancement. A single composite image is created by digitally splicing two or more images together in the splicing forgery technique. As an illustration, let's look at two photographs (Figures 2 and 3), which have been composited into one image (Figure 4). It is extremely difficult for the unaided eye to see the boundary between the spliced regions, even under close inspection. Existing picture splicing forgery detection strategies can be categorized into four groups based on the specific image property that has been used: hash techniques-based detection methods [2], compression property-based methods [3], device property-based methods [4], and vital image property-based methods [5]. Because the aforementioned techniques concentrate on a particular aspect of the image, they have the

*Correspondence: Velmurugan, S., Department of Computer Science, Kongunadu Arts and Science College (Autonomous), Coimbatore - 641029, Tamil Nadu, India. E.mail: svelmurugan_cs@kongunaducollege.ac.in following drawbacks when used in practical settings: 1) Since the hash technique-based detection method relies on the hash of the original, unaltered image, it cannot be classified as a type of blind forgery detection. 2) The detection method based on the image compression property can only identify image forgeries in JPEG format. 3) The detection techniques based on the crucial image properties may not work if some obscure methods, like fuzzy operations, are applied after splicing. 4) Lastly, if the device noise intensity is low, detection methods based on the imaging device property become invalid.

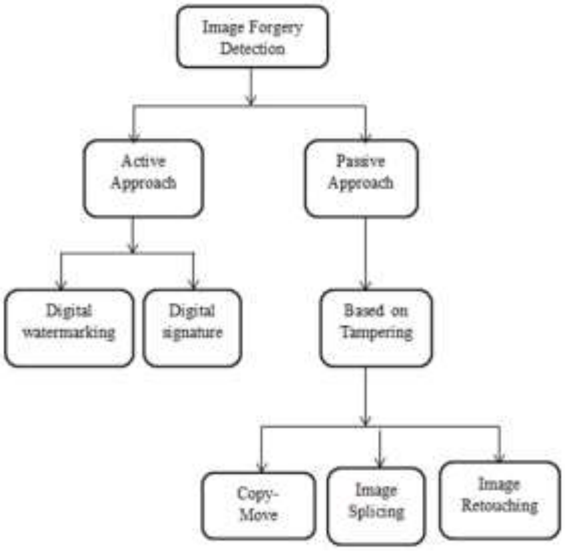


Figure 1. Type of digital image forgery detection.

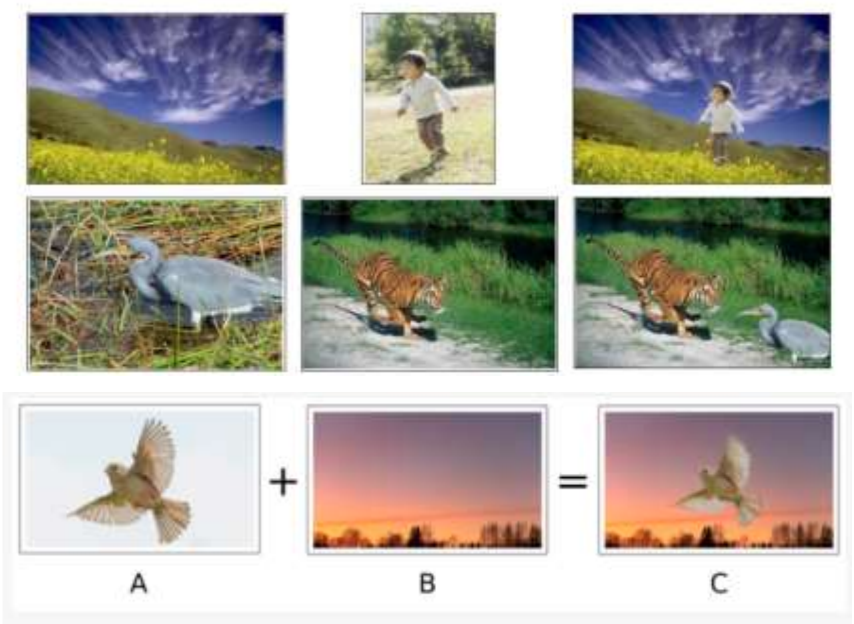


Figure 2. Represents the splicing of original images for obtaining a spliced image forgery, where (A,B) are the original images, and (C) is the spliced image forgery.

2. RELATED WORK

Most splicing forgery detection techniques are passive, meaning they don't rely on any kind of image prior knowledge[6]. Alahmadi et al. [7] and Min and Dong [8] used DCT coefficients, minimum and maximum filter methods, and other techniques to extract characteristics from image blocks and detect splicing forgery. Numerous algorithms employ multiresolution techniques such as DWT [8]. Block matching is not, however, the sole technique used to identify splicing forgeries; SIFT characteristics are also utilized as a backup[9]. The Columbia Color DVMM dataset, the CASIA v2.0 and v1.0 datasets, and most of the splicing forgery detection algorithms are evaluated.

Most splicing forgery detection techniques are passive, meaning they don't rely on any kind of image prior knowledge[6]. Alahmadi et al. [7] and Min and Dong [8] used DCT coefficients, minimum and maximum filter methods, and other techniques to extract characteristics from image blocks and detect splicing forgery. Numerous algorithms employ multiresolution techniques such as DWT [8]. Block matching is not, however, the sole technique used to identify splicing forgeries; SIFT characteristics are also utilized as a backup[9]. The Columbia Color DVMM dataset, the CASIA v2.0 and v1.0 datasets, and most of the splicing forgery detection algorithms are evaluated.

SVM was used to categorize the data. Jalab et al. [14] obtained fractional entropy from DWT [15] coefficients, and SVM was used for classification. Min and Dong developed a novel tampering detection technique in [8] that relies on maximum and minimum filters. The minimum and maximum pixel differences between real and fake images are highlighted when a maximum filter and a minimum filter are combined. The analysis of interpolation and non-interpolation improved the effectiveness of the forgery detection system in composite regions. A novel deep learning technique was recently developed by Jinwei et al. in [16] to detect picture splicing.

3. PROPOSED APPROACH

This paper presents a precise and effective model. In Figure 3, the suggested Feature Similarity Module (FSM) model is displayed. It addresses the entire image. The development of techniques for detecting and localizing spliced image forgeries was spurred by the identified research issues. The limitations of cutting-edge techniques are attempted to be addressed in these methods. The two suggested methods—spliced image detection and spliced region localization—are the main topics of this section. These methods are covered in the corresponding subsections.

The conceptual design of the expected splice forgery detection technique is shown in Fig. 5. Using the suggested method, RRU-Net[17], a specially designed U-Net, offers a hierarchical progression from residual propagation and the residual feedback to identify suspicious forging areas in the host image. The RRU-Net's Feature Similarity Module (FSM) is positioned between the encoder and decoder layers. The FSM receives the encoder output from the encoder layer and uses it to extract long-range spatial contextual information. This aids the model in concentrating more on the forged area while disregarding the remaining, extraneous portions of the picture.

The FSM output is processed by the decoder layer in order to identify the final forged region. The final result highlights the forged region.Subsections C and D, respectively, provide descriptions of the projected RRU-Net with FSM.

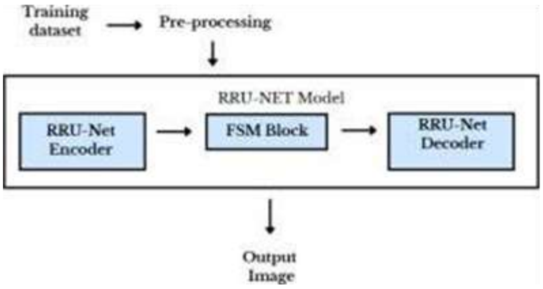


Figure 3. Proposed Architecture of Spliced Image Forgery Detection

A. *Residual Propagation*

The basis for identifying spliced image forgeries is primarily based on differences in the intrinsic nature of image attributes. However, as network architecture becomes more complex, the gradient degradation problem undermines this foundation. The RRU-Net adds the residual propagation layer to each stacked layer to address this gradient degradation problem. One definition of a residual propagation building block is:

$$y_f = F(x, \{W_i\}) + W_s * x \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, (1)$$

where Wi is the weight of layer I, x and yf stand for the building block's input and output, and the function F(x, Wi) denotes the residual mapping that has to be learned. The residual propagation mimics the brain's mechanism for recall. When learning new information, the human brain may forget what it already knows, so it needs a recall mechanism to help jog those hazy memories from the past.

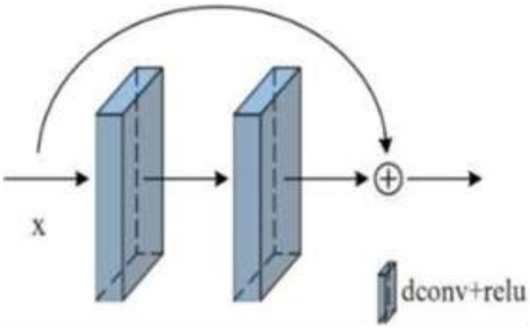


Figure 4. Residual propagation

B. *Residual Feedback*

RRU-Net uses residual feedback to amplify the intrinsic differences in image attributes. It is a system for automatically learning. It doesn't concentrate on one or more particular aspects of the image. When evaluating input data, the residual feedback mechanism gives greater weight to the distinguishing characteristics. To enhance the differences in the intrinsic nature of image attributes between forged and un-forged areas, it applies a sigmoid activation function to the input data. A buildingblock's residual feedback is described as

$yb=(s(G(yf))+1*x$…………………………………………………(2)

where yb is the enhanced input, yf is the residual propagation results as defined in Eq. (1), and x is the input. The linear projection function, G, modifies the dimensions of yf. S stands for the sigmoid activation function. The residual feedback functions as the human brain's consolidation mechanism, as opposed to the recall mechanism that residual propagation mimics. The intrinsic differences in image attributes between the forged and un-forged areas can be accentuated by the residual feedback.

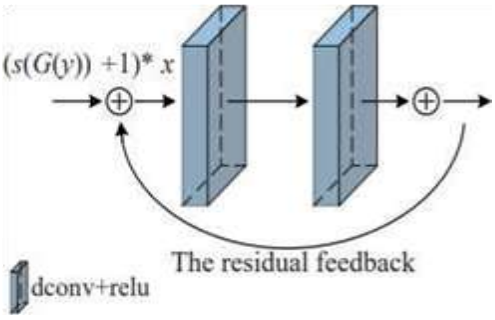


Figure 5. Residual feedback

C. Ringed Residual Structure and Network Architecture

The residual structure with rings that combines the residual feedback and the residual propagation. The residual feedback amplifies the input feature information by consolidating the intrinsic nature of image attributes between the forged and un-forged areas. The residual propagation mimics the human brain's recall mechanism, which retrieves the input feature information to resolve the degradation problem in the deeper network. In summary, the ringed residual structure ensures that the intrinsic characteristics of an image can be distinguished more clearly when features are extracted from the network layers. This leads to a more stable and superior recognition performance compared to both the current CNN-based recognition techniques and traditional feature extraction-based techniques. The RRU-Net network architecture is shown in Fig. 6. It is an end-to-end intrinsic image attribute segmentation network that can detect splicing image forgery without the need for pre- or post-processing.

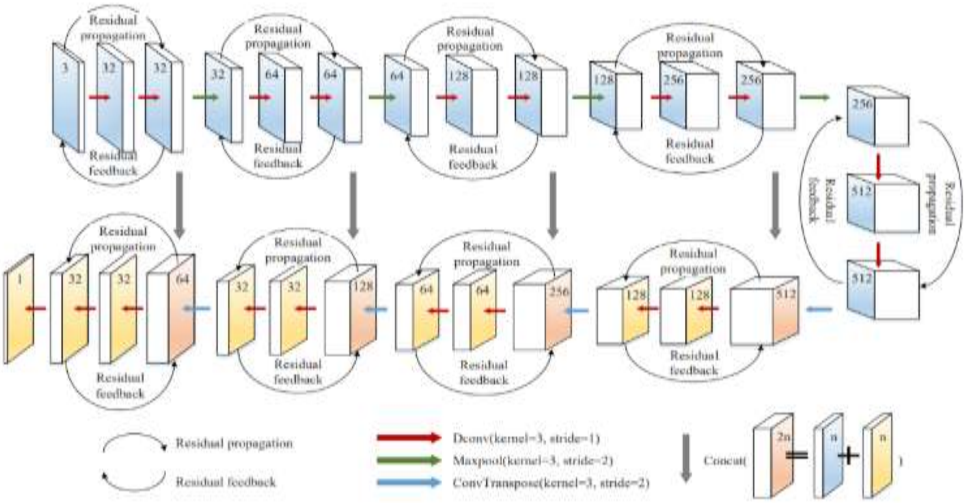

Residual propagation
Residual feedback
3
32
32
64
64
128
128
256
256
512
512
1
Dconv(kernel=3, stride=1)
Maxpool(kernel=3, stride=2)
ConvTranspose(kernel=3, stride=2)
Concat(
2n
n
n
)

Figure 6. Network Architecture of RRU-Net. The number of the box represents the number of features

D. Feature Similarity Module(FSM)

Long-range dependencies can be extracted using the Feature Similarity Module, or FSM. Better segmentation may result from the more efficient extraction of dense contextual information made possible by FSM. Between the encoder and decoder layers of RRU-Net, FSM is used, which can aid in the more effective extraction of spatial information. This module encodes various position-sensitive spatial data and creates feature maps out of it. FSM is easily plugged into other fully convolutional neural networks, leading to a multitude of task-performing applications.In essence, this module purges features from the feature map that are supplied to the convolution layer. Subsequently, the relationship between two distinct feature map values is defined.

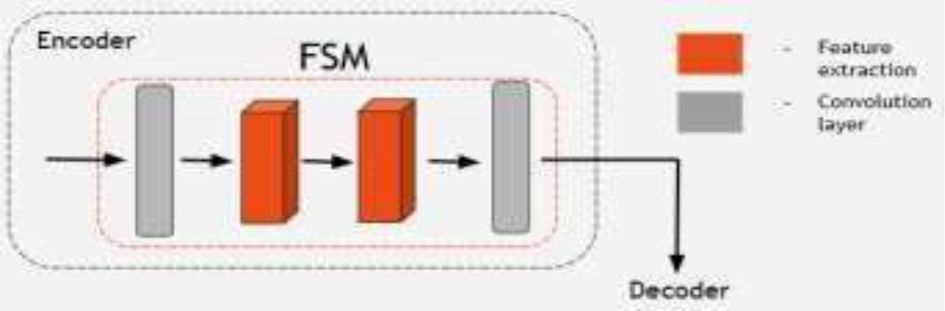


Figure 7. Architecture of Feature Similarity Module

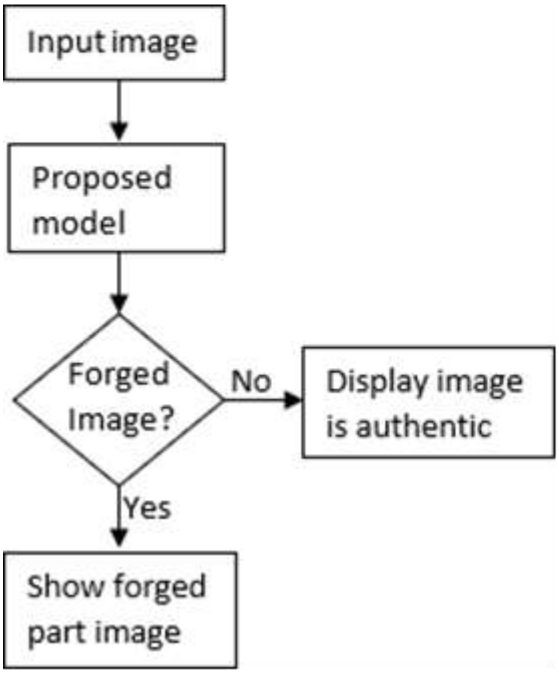


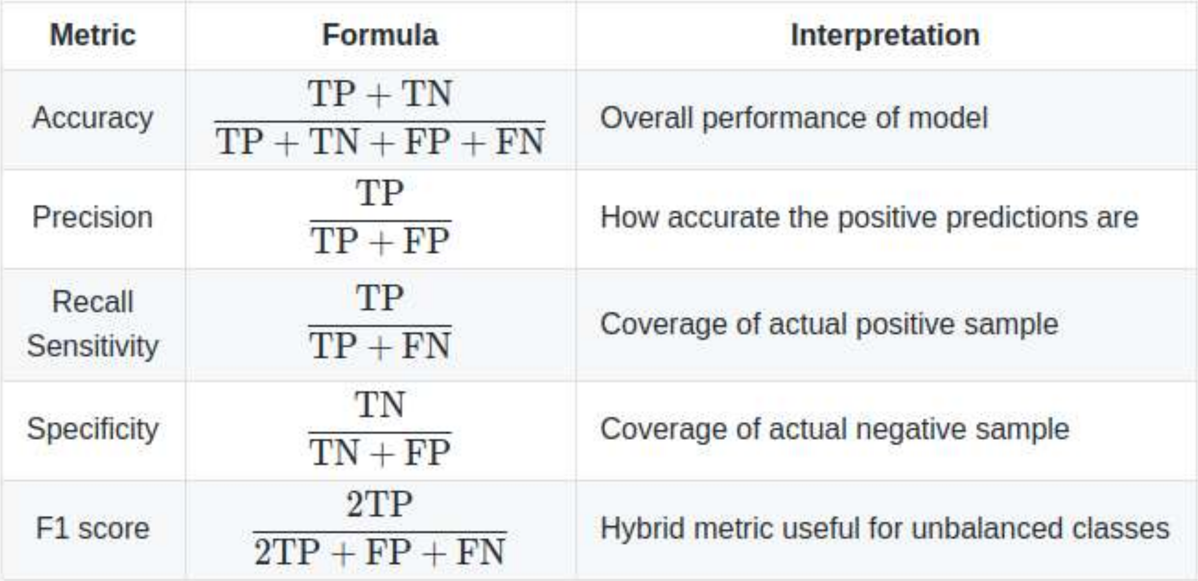
Figure 8. Flow diagram of the proposed method.

4. EXPERIMENTAL RESULTS

We thoroughly described a number of experiments in this section to evaluate the viability of the suggested methodology. The following specifications apply to the Google Collab server machine used for the experiments: 2.5 GB/12 GB of RAM and a TensorFlow backend with Keras are used in Python 3. The CASIA 1.0 dataset has a resolution of 384 × 256 or 256 × 384 and comprises 913 images, 451 original images, and 462 images forgeries. JPG format is used for the images.

Analytical Measures

The suggested model's effectiveness is evaluated using the metrics listed below.



Metric	Formula	Interpretation
Accuracy	$\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP}+\mathrm{TN}+\mathrm{FP}+\mathrm{FN}}$	Overall performance of model
Precision	$\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FP}}$	How accurate the positive predictions are
Recall Sensitivity	$\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}}$	Coverage of actual positive sample
Specificity	$\frac{\mathrm{TN}}{\mathrm{TN}+\mathrm{FP}}$	Coverage of actual negative sample
F1 score	$\frac{2\mathrm{TP}}{2\mathrm{TP}+\mathrm{FP}+\mathrm{FN}}$	Hybrid metric useful for unbalanced classes

Our study has been tested over a CASIA 1.0 and small dataset of 913 photos to train the model. Even with such a small dataset, we are still able to obtain some excellent results that clearly show the forged portions. Results of confusion matrices are specified in Table 1. The sensitivity and specificity of the proposed model over CASIA 1.0datasets are shown in Table 2. The feature map for a spliced forgery image is shown in Figure 9.

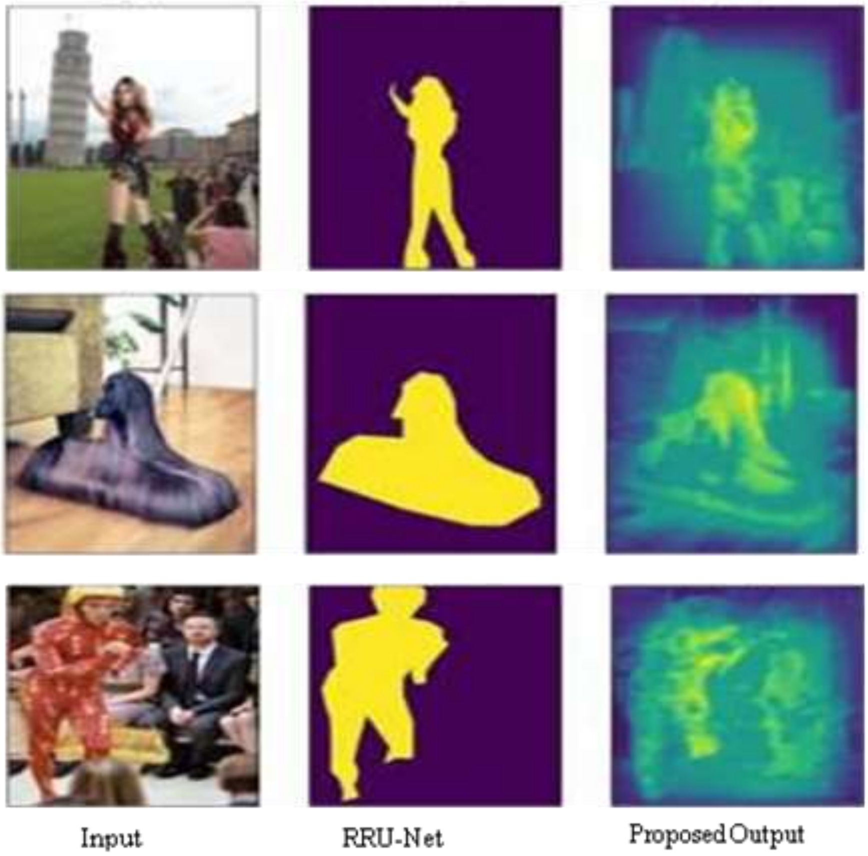
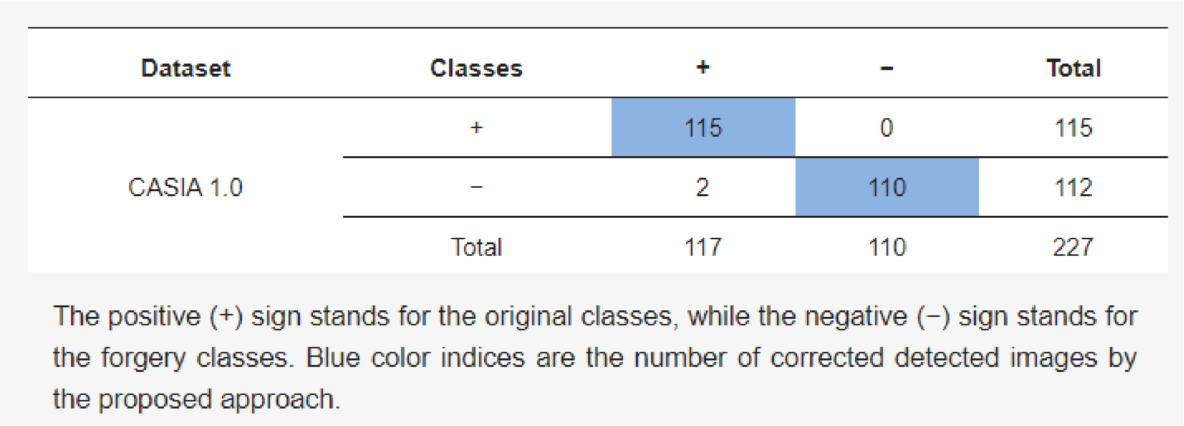


Figure 9. Feature map for a spliced forgery image.

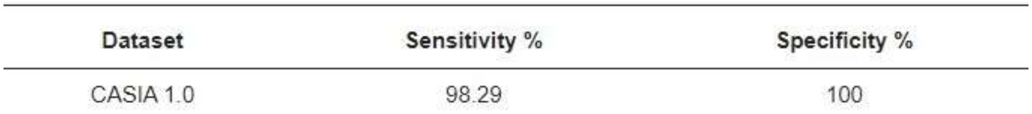
Table 1. Confusion matrices of the proposed model CASIA 1.0 Dataset



Dataset	Classes	+	–	Total
CASIA 1.0	+	115	0	115
	–	2	110	112
	Total	117	110	227

The positive (+) sign stands for the original classes, while the negative (–) sign stands for the forgery classes. Blue color indices are the number of corrected detected images by the proposed approach.

Table 2. Sensitivity and specificity of the proposed model CASIA 1.0 Dataset



Dataset	Sensitivity %	Specificity %
CASIA 1.0	98.29	100

5. CONCLUSION

The suggested technique locates the final image locations that have been altered and yields the expected results using RRU-Net with FSM. The RRU-Net is a ringed residual structure that combines residual feedback and residual propagation. The RRU-Net uses FSM to further improve the output based on the detection results. The effectiveness and applicability of the suggested method will then be evaluated on the publicly available datasets, CASIA, and contrasted with other cutting-edge detection techniques in order to identify image counterfeiting.

FUTURE WORK

The suggested method only proved effective when applied to the image splicing forgery problem; experiments on other problems, such as medical images or other forms of forgery, have not been conducted to demonstrate the approach's generalizability.

ACKNOWLEDGEMENT

The authors wish to acknowledge the Management and Staff of Kongunadu Arts and Science College, Coimbatore, Tamil Nadu, India, for supporting all the facility to complete this study.

REFERENCES

1. Velmurugan, S., Subashini, T.S. and Prashanth, M.S. (2020). Dissecting the Literature for studying various Approaches to Copy Move Forgery Detection. *International Journal of Advanced Science and Technology* 29(04), 6416 - 6438.
2. Pan, X. (2015). Digital Image Forensics with Statistical Analysis. Handbook of Digital Forensics of Multimedia Data and Devices, 481–521.
3. Johnson, M. K. and Farid, H. (2007). Exposing Digital Forgeries in Complex Lighting Environments. *IEEE Transactions on Information Forensics and Security* 2(3), 450–461.
4. Gou, H., Swaminathan, A. and Wu, M. (2007). Noise Features for Image Tampering Detection and Steg analysis. 2007 IEEE International Conference on Image Processing.
5. Han, T.H., Moon, J.G., and Eom, I.K. (2016). Image splicing detection based on inter-scale 2D joint characteristic function moments in wavelet domain. EURASIP Journal on Image and Video Processing, 2016 (1).
6. Muhammad, G., Al-Hammadi, M.H., Hussain, M. et al. (2014). Image forgery detection using steerable pyramid transform and

local binary pattern. *Machine Vision and Applications* 25, 985–995.

7. Alahmadi, A. A., Hussain, M., Aboalsamh, H., Muhammad, G. and Bebis G. (2013). "Splicing image forgery detection based on DCT and Local Binary Pattern," 2013 IEEE Global Conference on Signal and Information Processing, Austin, TX, USA, 253-256.
8. Hwang, M.G. and Har, D.H. (2014). Identification method for digital image forgery and filtering region through interpolation. *Journal of Forensic Sciences* 59(5), 1372-85.
9. Costanzo, A., Amerini, I., Caldelli, R. and Barni, M. Forensic Analysis of SIFT Keypoint Removal and Injection. *IEEE Transactions on Information Forensics and Securit.* 9, 1450-1464.
10. Tian-Tsong Ng, Shih-Fu Chang and Qibin Sun. (2004). Blind detection of photomontage using higher order statistics. IEEE International Symposium on Circuits and Systems (ISCAS), Vancouver, BC, Canada, 2004, pp. V-V.
11. Das, D., Naskar, R. and Chakraborty, R. (2023). Image splicing detection with principal component analysis generated low-dimensional homogeneous feature set based on local binary pattern and support vector machine. *Multimedia Tools and Applications* 82(17), 25847-25864.
12. Meena, K. and Tyagi, V. (2021). Image splicing forgery detection using noise level estimation. *Multimedia Tools and Applications* 82(9), 13181-13198.
13. Alahmadi, A., Hussain, M., Aboalsamh, H. et al. (2017). Passive detection of image forgery using DCT and local binary pattern. *SIViP* 11, 81–88.
14. Pham, N.T., Lee, JW., Kwon, GR. et al. (2019). Efficient image splicing detection algorithm based on markov features. *Multimedia Tools and Applications* 78, 12405–12419.
15. Jalab, H., Subramaniam, T., Ibrahim, R., Kahtan, H. and Noor, N. (2019). New Texture Descriptor Based on Modified Fractional Entropy for Digital Image Splicing Forgery Detection. *Entropy* 21(4), 371.
16. Wang, J., Ni, Q., Liu, G., Luo, X. and Jha, S. K. (2020). Image splicing detection based on convolutional neural network with weight combination strategy. *Journal of Information Security and Applications*.
17. Kumar, N. and Meenpal, T. (2023). ResUNet: An Automated Deep Learning Model for Image Splicing Localization. In: Gupta, D., Bhurchandi, K., Murala, S., Raman, B., Kumar, S. (eds) Computer Vision and Image Processing. CVIP 2022. Communications in Computer and Information Science, vol 1776. Springer, Cham.

About The License