Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

SPLICED IMAGE FORGERY DETECTION USING FSM

Shantanu Tondlekar, Sherin Thomas, Ryan Marian, Tejas Jagdale and Anand Pardeshi,
Department of Information Technology, Fr. C. Rodrigues Institute of Technology, Vashi, Navi Mumbai, India

Abstract: In recent times, determining an image is authenticate or fabricated is big challenge. With advancement in technology an image can be tampered or forged within seconds. Detecting these kinds of forgeries has become significant issue at present. An image can be considered as important evidence but if it is forged it will be of no use. It is necessary to develop methods for differentiating between computer-generated photos and altered ones. With the view of detecting these forgeries we are going to develop Image Forgery Detection Model which will consist of RRU-Net along with FSM. RRU-Net which stands for Ringed Residual Structure and Network Architecture combines two different methodologies namely residual propagation and the residual feedback. FSM stands for Feature Similarity Module will be used to detect long-range dependencies. Combining FSM with RRU-Net to increase accuracy is our proposed system and from image patches of varying sizes, we will extract the differences in the image's attributes between unmodified and modified sections. After detecting the forged area, the final region will be displayed in coloured form. In future, the system will be helpful to detect various spliced image forgeries that surface on the various social media platforms.

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

I. INTRODUCTION

In many applications, digital images are considered as an important data. It can be used as proof in a variety of settings, including courts, the military, computer-assisted medical diagnosis systems, social networks, and more. It is necessary to ensure the authenticity of an image and to keep their contents tamper free based on their importance. Digital photos can be easily manipulated by users and regular people utilising online computer programs. This results in the difficult detection of these fake images by the eye. It is very much required to examine whether two types of images are genuine or fabricated because of many fraud tools being available. To put it differently, it is important to have methods for spotting fraudulent photographs.

The main approaches of discovering an image forgery are broadly classified into two types namely active and passive approach [1], as shown in Fig. 1. The fundamental component of the active technique is adding watermarks and digital signatures to photos as they are being created. The passive method allows us to conceal key image details and transform accurate information into inaccurate information. Five categories can be used to classify digital image forgery: Image splicing, retouching, morphing,and enhancement, as well as copy-move forgery.

In splicing forgery technique, two or more images are digitally spliced into a single composite image. For example, consider two images (Figures 2 and 3), both images are spliced together to form a single composite image (Figure 4). When observed carefully, the border between the spliced areas is very difficult to be noticed by the naked eyes.

Based on the particular image property that has been utilised, existing image splicing forgery detection techniques can be divided into four types: detection methods based on the hash techniques [2], compression property [3], device property [4] and essential image property [5].

The above-mentioned methods are focused on a specific image property, and therefore in real-world applications, have the following limitations: 1) The hash technique based detection method cannot be categorised as a sort of blind forgery detection because this method depends on the hash of the original, un-tampered image. 2) Only JPEG format image forgery can be detected by the

detection method based on the image compression property. 3) If some obscure techniques, such as fuzzy operations, are used after splicing then the detection methods based on the essential image properties may fail. 4) Finally, detection techniques based on the imaging device property becomes invalid if the device noise intensity is low.

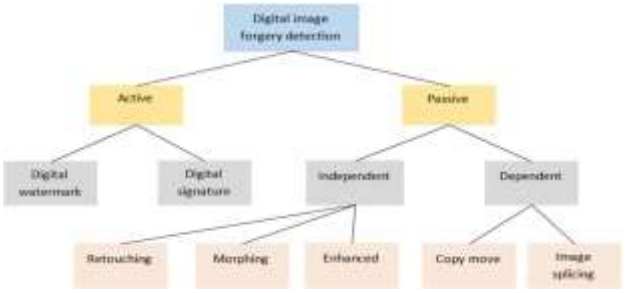

Fig. 1: Type of digital image forgery detection.

Fig. 2: Original Img 1

Fig. 3: Original Img 2

Fig. 4: Spliced Image

II. RELATED WORK

The majority of splicing forgery detection methods are passive. i.e they are not dependent on any kind of prior information of the image[6]. DCT coefficients, minimum and maximum filter methods were utilised by Alahmadi et al. [7] and Min and Dong [8]to extract characteristics from image blocks and identify splicing forgery. Many algorithms use multiresolution methods like DWT [8]. However, Block matching is not the only method used to detect splicing forgeries; SIFT characteristics are also employed as an alternative[9]. On the CASIA v2.0 and CASIA v1.0 datasets, the Columbia Color DVMM dataset, and the majority of the splicing forgery detection algorithms are assessed. The method for detecting image splicing proposed by Ng et al. is based on 3D moments of the image spectrum [10]. For the purpose of detecting picture splicing, Shi et al. [11] utilised DCT coefficients, 1D and 2D moments and Markov chain probabilities. The algorithm's accuracy was assessed using the CASIA v2.0 dataset and is reported to be 84.86%.

With the recent advancements in omnipresent computing and digital media, particularly digital images, the task of detecting image fraud has elevated to become one of the most crucial for the safe and genuine transfer of multimedia information. DCT and LBP characteristics were employed by Alahmadi et al. [12] to detect picture splicing. Pham et al. [13] identified Markov characteristics to spot splicing-related anomalies in pictures. SVM was employed to classify data. Fractional entropy was derived from DWT [15] coefficients by Jalab et al. [14], and SVM was utilised for classification.

A unique tampering detection method based on maximum and minimum filter was created by Min and Dong in [8]. The combination of a maximum filter and a minimum filter draws attention to the minimal and maximum pixel differences between genuine and fake images. The efficacy of the forgery detection system in composite regions was enhanced by the examination of interpolation and non-interpolation. For the purpose of detecting picture splicing, Jinwei et al. recently developed a unique deep learning method in [16].

III. PROPOSED METHODOLOGY

Fig. 5 depicts the conceptual layout of the anticipated splice forgery detection method. To detect suspicious forging areas in the host image using the proposed technique, RRU-Net[17], a specially created U-Net, provides a hierarchical progression from residual propagation and the residual feedback. Feature Similarity Module (FSM) sits between encoder and decoder layer of the RRU-Net. The encoder layer feeds the encoder output to the FSM, which then helps in extracting the long-range spatial contextual information. This helps the model on focusing more on the forged region ignoring rest of the non-essential parts of the image. The decoder layer takes the FSM output and process it to detect the final forged region. The forged region is highlighted in the final output. The projected RRU-N ıd D, respectively.

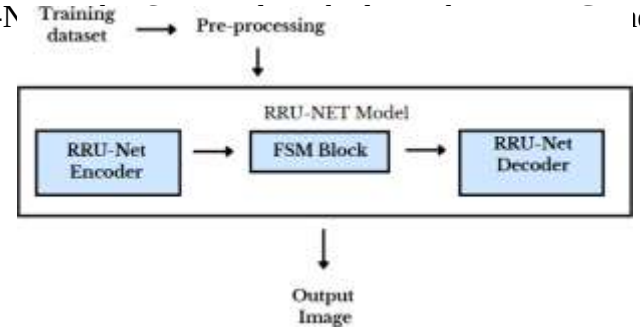

Fig. 5: System Design of Proposed Spliced Image Forgery Detection System.

A. *Residual Propagation*

The differences of the intrinsic nature of image attributes are the notable basis for locating spliced image forgery, nevertheless, the gradient degradation problem destroys the basis as the network architecture goes deeper. In order to solve this gradient degradation issue, the RRU-Net adds the residual propagation layer to each stacked layer. A building block of residual propagation is defined as:

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

where, x and yf represents the input and output of the building block, Wi is the weight of layer i, the function F(x, Wi) means the residual mapping to be learned. The residual propagation imitates the recall mechanism of the human brain. A human brain may forget the preceding knowledge when it learns various additional new knowledge, so it needs the recall mechanism to help arouse those preceding fuzzy memories.

B. *Residual Feedback*

The residual feedback is used in RRU-Net to enhance the differences of intrinsic nature of image attributes. It is an automatic learning mechanism. It does not focus on one or many specific images attributes. The residual feedback mechanism pays more attention to the discriminating features if input information. It uses sigmoid activation function on input information to augment differences of intrinsic nature of image attributes between forged and un-forged areas. The residual feedback in a buildingblock is defined as

$$y_b = (s(G(y_f)) + 1 * x \quad (2)$$

where x represents input, yf is the results of residual propagation defined in Eq.(1), yb is the enhanced input. The function G represents linear projection, which changes the dimensions of yf. The sigmoid activation function is represented by s. In variance to recall mechanism that residual propagation imitates, the residual feedback behaves as the human brain consolidation mechanism. The residual feedback can augment the differences of intrinsic nature of image attributes between the forged and un-forged areas.

[

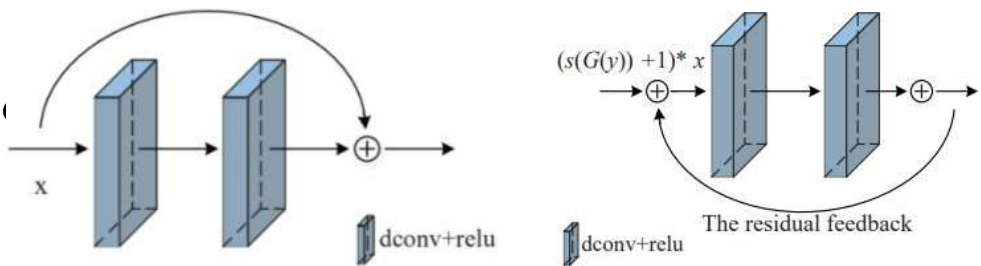

Fig. 6: Residual propagation. Fig. 7: Residual feedback.

C. Ringed Residual Structure and Network Architecture

The ringed residual structure that blends the residual propagation and the residual feedback. The residual propagation imitates the recall mechanism of the human brain, which recollects the input feature information to resolve the degradation problem in the deeper network; the residual feedback amplifies the input feature information by consolidating the intrinsic nature of image attributes between the forged and un-forged areas. To conclude, the ringed residual structure assures the differentiating intrinsic nature of image attributes be clearer when the features are drawn from the layers of network, which results in achieving stable and better recognition performance than traditional feature extraction-based recognition techniques and current CNN-based recognition techniques. Fig. 8 represents the RRU-Net network architecture, it is an end-to-end intrinsic nature of image attribute segmentation network, which is capable of detecting the splicing image forgery without the need of any pre-processingand post-processing.

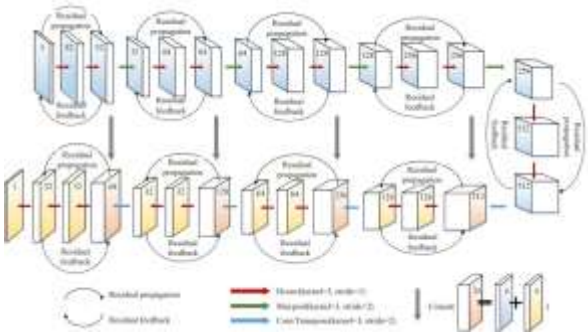

Fig. 8: Architecture of RRU-Net.

D. Feature Similarity Module (FSM)

Feature Similarity Module (also called as FSM) can be used to extract long range dependencies. FSM facilitates us with extraction of dense contextual information in a more effective way, which can improve segmentation. FSM is used between the encoder and decoder layer of RRU-Net which can help in better extraction of spatial information. This module draws a variety of position-sensitive spatial information and encodes it into feature maps. FSM can be easily plugged into other fully convolutional neural networks which can result in various applications that can perform different tasks.

This module basically removes irrelevant features from the feature map that is fed to the convolution layer. Then it defines the relationship between two different values of the feature maps. It defines the impact of one value of feature map on other value.

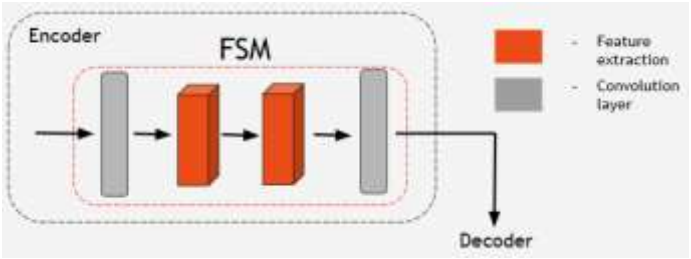

Fig. 9: Architecture of FSM.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 2, No. 1, February : 2023

IV. WORK FLOW

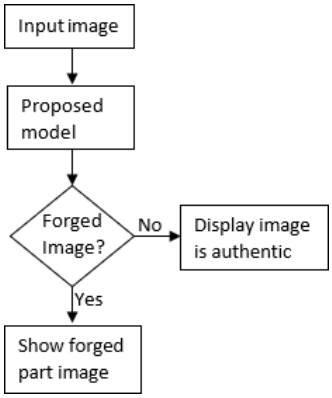

Fig. 10: Flowchart of the proposed system.

V. RESULTS

We have trained the model with a limited dataset of 184 images. With such a limited dataset also we are able to get some fineresults with clear highlighted forged parts.

Fig. 11: Output 1.

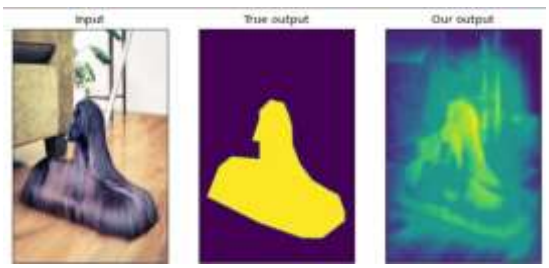

Fig. 12: Output 2.

Fig. 13: Output 3.

Fig. 14: Output 4.

VI. CONCLUSION

The suggested technique makes use of RRU-Net with FSM to acquire the anticipated outcomes and identify the final found tampered locations in the image. The RRU-Net in use is a ringed residual structure that blends the residual propagation and the residual feedback. The RRU-Net uses FSM to further improve the results based on the detection outcomes. The effectiveness and applicability of the suggested method will next be examined on the two publicly available datasets CASIA and FORENSICS and compared with other cutting-edge detection techniques to identify image counterfeiting.

REFERENCES

[1] S. Velmurugan, T. Subashini, and M. Prashanth, “Dissecting the literature for studying various approaches to copy move forgery detection,” Int. J. Adv. Sci. Technol., vol. 29, pp. 6416–6438, Jun. 2020.

[2] P. Xunyu, “Digital image forensics with statistical analysis,” Handbook Of Digital Forensics of Multimedia Data and Devices, John Wiley & Sons, NJ, USA, 2015.

[3] Micah K. Johnson and Hany Farid. Exposing digital forgeries in complex lighting environments. IEEE Transactions on Information Forensics and Security, 2(3):450–461, 2007
[4] Hongmei Gou, Ashwin Swaminathan, and Min Wu. Noise features for image tampering detection and steganalysis. In ICIP (6), pages 97–100. Citeseer, 2007.
[5] Wen Chen, Yun Q Shi, and Wei Su. Image splicing detection using 2- d phase congruency and statistical moments of characteristic function. In Security, Steganography, and Watermarking of Multimedia Contents IX, volume 6505, page 65050R. International Society for Optics and Photonics, 2007.
[6] G. Muhammad, M. H. A. Hammadi, M. Hussain, and G. Bebis, "Image forgery detection using steerable pyramid transform and local binary pattern," Machine Vision and Applications, vol. 25, no. 4, pp. 985–995, 2014.
[7] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," in Proceedings of the IEEE Global Conference on Signal and Information Processing, pp. 253–256, Austin, TX, USA, September 2013.
[8] G. H. Min and H. H. Dong, "Identification method for digital image forgery and filtering region through interpolation," Journal of Forensic Sciences, vol. 59, no. 5, pp. 1372–1385, 2014.
[9] A. Costanzo, I. Amerini, R. Caldelli, and M. Barni, "Forensic analysis of SIFT keypoint removal and injection," IEEE Transactions on Information Forensics and Security, vol. 9, no. 9, pp. 1450–1464, 2014.
[10] T. T. Ng, S. F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics," in Proceedings of the international symposium on circuits and systems, pp. 688–691, Vancouver, Canada.
[11] Y. Q. Shi, C. Chen, and W. Chen, "A natural image model approach to splicing detection," in Proceedings of the 9th ACM Workshop on Multimedia & Security, pp. 51–62, Dallas, Texas.
[12] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour, "Passive detection of image forgery using DCT and local binary pattern," Signal, Image and Video Processing, vol. 11, no. 1, pp. 81–88, 2017.
[13] N. T. Pham, J. Lee, G. Kwon, and C. Park, "Efficient image splicing detection algorithm based on markov features," Multimedia Tools and Applications, vol. 78, no. 9, Article ID 12405, 2019.
[14] H. Jalab, T. Subramaniam, R. Ibrahim, H. Kahtan, and N. Noor, "New texture descriptor based on modified fractional entropy for digital image splicing forgery detection," Entropy, vol. 21, no. 4, pp. 371–385, 2019.
[15] R. C. Gonzalez and R. E. Woods, in Digital image processing, vol. 4, Addison-Wesley, MA, USA, 1992.
[16] W. Jinwei, N. Qiye, L. Guangjie, L. Xiangyang, and K. J. Sunil, "Image splicing detection based on convolutional neural network with weight combination strategy," Journal Information Security and Applications, vol. 54, pp. 1–8, 2020.
[17] Yang Wei, Xiuli Bi, and Bin Xiao. RRU-Net: The Ringed Residual U-Net for Image Splicing Forgery Detection. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshop, 2019.