JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

Enhancing Image Forgery Detection through Lightweight Deep Learning Tool Fusion

D. Mahammad Rafi[1], Kandukuri Venkata Krishna[2], Elguri Shravan Kumar[3]

[1]Professor, Department of CSE, Malla Reddy Engineering College and Management Sciences, Hyderabad, Telangana.

[2,3]Assistant Professor, Department of CSE, Malla Reddy Engineering College and Management Sciences, Hyderabad, Telangana.

Abstract

Image forgery detection is one of the key challenges in various real time applications, social media, and online information platforms. The conventional methods of detection based on the traces of image manipulations are limited to the scope of predefined assumptions like hand-crafted features, size, and contrast. In this paper, we propose a fusion based decision approach for image forgery detection. The fusion of decision is based on the lightweight deep learning models namely Squeeze Net, MobileNetV2 and Shuffle Net. The fusion decision system is implemented in two phases. First, the pretrained weights of the lightweight deep learning models are used to evaluate the forgery of the images. Secondly, the fine-tuned weights are used to compare the results of the forgery of the images with the pre-trained models. The experimental results suggest that the fusion-based decision approach achieves better accuracy as compared to the state-of-the-art approaches.

Keywords: Image forgery detection, Squeeze Net, MobileNetV2, Shuffle Net, deep learning models

1. Introduction

In this digital era, images and videos are being used as influential sources of evidence in a variety of contexts like evidence during trials, insurance fraud, social networking, etc [1]. The easy adaptability of editing tools for digital images, especially without any visual proof of manipulation, give rise to questions about their authenticity. It is the job of image forensics authorities to develop technological innovations that would detect the forgeries of images [2]. There are three primary classes of manipulation or forgery detectors studies until now: those supported features descriptors, those supported inconsistent shadows and eventually those supported double JPEG compression. With sophisticated software, it is easy to tamper the contents of the image to influence the opinions of others [3]. Image forgery techniques are broadly classified into two categories namely copy-move and splicing. For copy-move forgery, elements of the image content area are traced and smudge inside a similar image, whereas for splicing forgery, parts of the image content smudge from alternative pictures [4]. To reconstruct the trust in pictures, various image forgery detection techniques have been proposed over the past few years [5].

Many previous studies have tried to extract totally different properties from the image to spot the copy-paste or splicing of forged areas, such as the lighting, shadows, sensing element noise, and camera reflections [6]. Researchers determined the credibility of the image wherever it is known either as authentic or forged. Currently, there are many techniques to spot forged regions that exploits the artefacts left by multiple JPEG compression and other techniques of image manipulation to sight the forged regions [7]. Camera primarily based ways have additionally analyzed where the detection relies on demos icing regularity or sensing element pattern noise wherever the irregularities of the sensing element pattern area unit extracted and compared for anomalies [8]. Forged or manipulated pictures can mislead people and may threaten individuals' life. This paper aims to find the

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

manipulated pictures by automating the method of feature extraction instead of feature engineering or feature extraction through the manual process [9]. Deep learning to make use of highly correlated pixels in a vicinity, thus considering grouped native connections [10].

Rest of the paper is organized as follows: Section 2 details about literature survey, section 3 details about the proposed methodology, section 4 details about the results with discussion, and section 5 concludes article with references.

2. Literature Survey

Kwon, M. et al. (2021) [11] Detecting and localizing image splicing had become essential to fought against malicious forgery. A major challenged to localize spliced areas was to discriminate between authentic and tampered regions with intrinsic properties such as compression artifacts. They proposed cat-net, an end-to-end fully convolutional neural network including rgb and dct streams, to learned forensic features of compression artifacts on rgb and dct domains jointly. The proposed method outperforms state-of-the-art neural networks for localizing spliced regions in jpeg or non-jpeg images. Wu, Y. et al. (2019) [12] To fight against real-life image forgery, which commonly involves different types and combined manipulations, they propose a unified deep neural architecture called mantra-Net. Unlike many existing solutions, mantra-Net is an end-to-end network that performs both detection and localization without extra pre-processing and postprocessing. Manifold is a fully convolutional network and handles images of arbitrary sizes and many known forgery types such splicing, copy-move, removal, enhancement, and even unknown types. Zheng, L. et al. (2019) [13] Editing a real-world photo through computer software or mobile applications was one of the easiest things one could did today before sharing the doctored image on one's social networking sites. Although most people did it for fun, it was suspectable if one concealed an objected or changed someone's faced within the image. Rony, J. et al. (2019) [14] Used state-of-the-art deep learned models for cancer diagnosis presents several challenges related to the nature and availability of labeled histology images. Cancer grading and localization in these images normally relies on both image- and pixel-level labels, the latter requiring a costly annotation process. In this surveyed, deep weakly-supervised learned (wsl) models were investigated to identified and locate diseases in histology images, without the needed for pixel-level annotations. Given training data with global image-level labels, these models allowed to simultaneously classify histology images and yield pixel-wise localization scores, thereby identifying the corresponding regions of interest (roi). Meena, et al. (2019) [15] this age of digitization, digital images were used as a prominent carrier of visual information. Images were becoming increasingly ubiquitous in everyday life. Unprecedented involvement of digital images could be seen in various paramount fields liked medical science, journalism, sports, criminal investigation, image forensic, etc., where authenticity of image was of vital importance. Various tools were available free of costed or with a negligible amount of costed for manipulating images. Some tools could manipulate images to such an extent that it became impossible to discriminate by human visual system that image was forged or genuine. Hence, image forgery detection was a challenging area of researched.

Abdel-Basset M, et al. (2018) [16] Understanding was considered a key purpose of image forensic science in ordered to found out if a digital image was authenticated or not. It could be a sensitive task in case images were used as necessary proof as an impact judgment. It's known that there were several different manipulating attacks but, this copy moved was considered as one of the most common and immediate one, in which a region was copied twice in ordered to give different information about the same scene, which could be considered as an issue of information integrity. The detection of this kind of manipulating had been recently handled used methods based on sift. Sift characteristics were represented in the detection of image features and determining matched points. Kekre HB, et al. (2013) [17] Image hashing was one of the techniques used to generate hash valued

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

for each image in the database. These hash values generated for images could been used for content-based image retrieval, image database indexing, and image authentication, avoiding, and mitigating the tampering of digital images. In the information era, the increasing availability of multimedia data in digital form had led to a tremendous growth of tools to manipulate digital multimedia. To ensured trustworthiness, multimedia authentication techniques had emerged to verify content integrity and prevent forgery. A novel approached was proposed for forgery detection used image hashing, experimental results showed that even slightest of image tempering could been detection with the proposed technique. Zhou P, et al. (2018) [18] Image manipulation detection was different from traditional semantic objected detection because it pays more attention to tampering artifacts than to image content, which suggests that richer features needed have been learned. They proposed a two-stream faster r-cnn network and train it end-to-end to detect the tampered regions given a manipulated image. One of the two streams was a rgb stream whose purpose was to extract features from the rgb image input to found tampering artifacts liked strong contrast difference, unnatural tampered boundaries, and so on. The other was a noise stream that leverages the noise features extracted from a steganalysis rich model filter layer to discover the noise inconsistency between authentic and tampered regions. They then fuse features from the two streams through a bilinear pooling layer to further incorporate spatial co-occurrence of these two modalities. Experiments on four standard image manipulation datasets demonstrate that our two-stream framework outperforms each individual stream, and achieves state-of-the-art performance compared to alternative methods with robustness to resizing and compression. Kuznetsov A. et al. (2019) [19] Proposed an algorithm for detecting one of the most used types of digital image forgeries-splicing. The algorithm was based on the use of the vgg-16 convolutional neural network. The proposed network architecture took image patches as input and obtains classification results for a patch: original or forgery. On the training stage they select patches from original image regions and on the borders of embedded splicing. Bunk J, et al. (2017) [20] Resampling was an important signature of manipulated images. They proposed two methods to detect and localize image manipulations based on a combination of resampling features and deep learned. In the first method, the radon transform of resampling features were computed on overlapping image patches. Deep learned classifiers and a gaussian conditional random field model were then used to create a heatmap. Tampered regions were located used a random walker segmentation method. In the second method, resampling features computed on overlapping image patches were passed through a long short-term memory (lstm) based network for classification and localization. They compare the performance of detection/localization of both these methods.

3.Proposed Methodology

The architecture of the proposed decision fusion is based on the lightweight deep learning models as shown in Figure 1. The lightweight deep learning models chosen are SqueezeNet, MobileNetV2, and ShuffleNet. The proposed system is implemented in two phases i.e., with pre-trained and fine-tuned deep learning models. In the pre-trained model's implementation, regularization is not applied, and the pre-trained weights are used and for the fine-tuned implementation, regularization is applied to detect image forgery. Each phase consists of three stages namely, data pre-processing, classification, and fusion. In the data pre-processing stage, the image in the query is pre-processed based on the dimensions required by the deep learning models. SVM is used for the classification of the image as forged or non-forged. Initially, we discuss the lightweight deep learning models and then the strategy used for the regularization is discussed in the further sections.

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

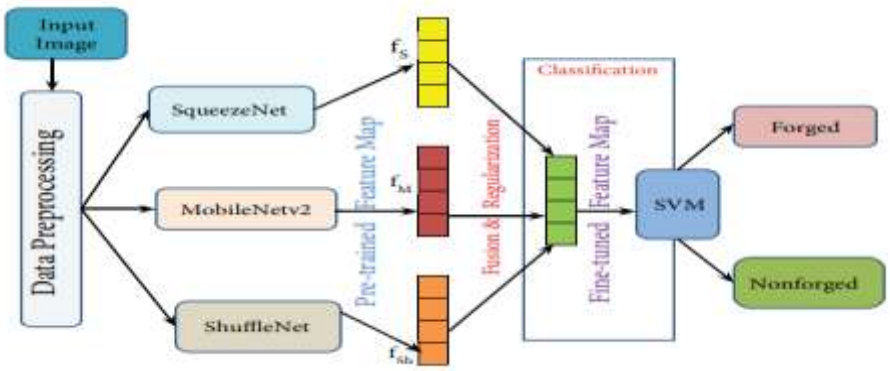

Figure 1: Fusion based decision model for forgery detection.

3.1 Data pre-processing

In this stage, the image in a query that needs to be identified whether it is forged or not is subjected to pre-processing. The height and width of the image required for SqueezeNet is 227×227. The height and width of the image required for MobileNetV2 is 224×224. The height and width of the image required for ShuffleNet is 224×224. The input image is pre-processed first based on the dimensions required for each of the models. Each model then takes the input image to produce feature vector in further stages.

3.2 Lightweight deep learning models

The different lightweight deep learning models that are considered for fusion are SqueezeNet, MobileNetV2, and ShuffleNet. These models are used for the image classification problems numerously. In this section, these models are discussed briefly. The lightweight models1 considered are summarized as shown in the Table 1. It represents the depth, parameters and the image input size required for the lightweight models namely, SqueezeNet, MobileNetV2, and ShuffleNet.

3.2.1 SqueezeNet

It is a CNN trained on the ImageNet dataset with 18 layers deep and can classify the images up to 1000 categories. The network has learned rich representations of the images with 1.24 million parameters. It requires only a few floating-point operations for the image classification.

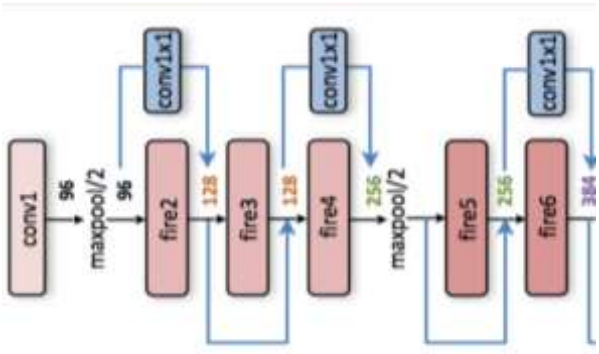

Figure 2: Squeeze Net.

3.2.2 MobileNetV2

It is a CNN trained on the ImageNet dataset with 53 layers deep and can classify the images up to 1000 categories. The performance of the classification is improved based on the learning of the rich representations of the images.

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

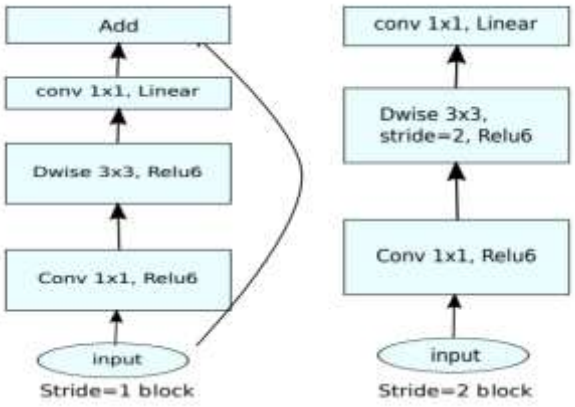

Figure 3: MobileNetV2.

3.2.3 ShuffleNet

It is a CNN that is also trained on the ImageNet dataset with 50 layers deep and can classify the images up to 1000 categories. Table 1. Parameters of lightweight deep learning models. (Depth represents the largest number of sequential convolutional or fully connected layers on a path from the input layer to the output layer, parameter represents the total number of learnable parameters in each layer and image input size represents the required input image size).

Table 1. Models' description.

Models	Depth	Parameter (millions)	Image input size
SqueezeNet	18	1.24	227 × 227
MobileNetV2	53	3.5	224 × 224
ShuffleNet	50	1.4	224 × 224

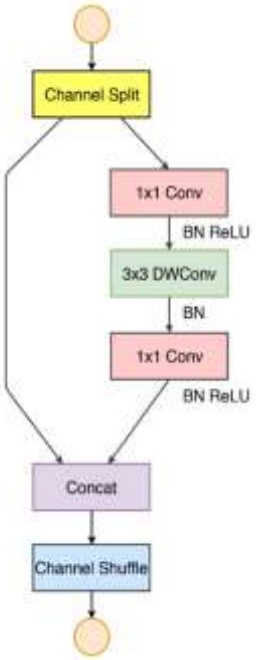

Figure 4.: ShuffleNet.

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

3.3 Fusion model and regularization

The proposed system is first implemented with lightweight deep learning models using pretrained weights for the image forgery detection, afterward, the proposed system is implemented as a fusion of the decision of lightweight models as discussed in the previous section. Initially, the input image is passed to the lightweight models to obtain their feature maps respectively. The feature map from the SqueezeNet is denoted as f_s, the feature map from the MobileNetV2 is denoted as f_m , the feature map from the ShuffleNet is denoted as f_{sh} . For the fusion model, the pretrained lightweight deep learning model's output feature mapping f_p is used. This feature map f_p is a combination of the feature maps obtained from the lightweight models as shown in Equation (1).

$$f_p = f_s + f_m + f_{sh} \quad (1)$$

The fusion model uses feature map f_p as a local descriptor for an input patch to extract the features of the image. The image for the fusion model is represented as a function $Y_{fusion} = f_{(x)}$where x is the patch in the input image. For a test image size $m \times n$, a sliding window of size p×p is used to compute the local descriptor Y_{fusion} is computed as shown in the equation (2) where $Y_1, Y_2, , Y_3$ represents the descriptors of the patches of the image obtained from the deep learning models. It is obtained as a concatenation of all the input patches x_i and the new image representation is given by equation (3) where s is the size of the stride used for transforming the input patch, this new image representation f_{fusion} is used as the feature map for the classification by the SVM as forged or nonforged.

$$Y_{fusion} = [Y_1 + Y_2 + \ldots + Y_T] \quad (2)$$

$$f_{fusion} = \frac{m-w}{s} + 1 * \frac{n-w}{s} + 1 \quad (3)$$

For fine tuning of the parameters of the fusion model, the initialization of the weight kernels is used as shown in Equation (4). In this equation Wf represents the weights of the fusion model, W_s represents the weights of the SqueezeNet model, W_m represents the weights of the MobileNetV2 model and W_{sh} represents the weights of the ShuffleNet model. The weight of the fusion model W_f is initialized as shown in Equation (5). The initialization of the weights acts as a regularization term and facilitates the fusion model to learn the robust features of detecting the forgery rather than the complex image representations.

$$W_f = [W_{sj}\ W_{mj}\ W_{shj}]\ \text{j} = 1, 2, 3 \quad (4)$$

$$W_f = [{W_f}^{4k-2}\ {W_m}^{4k-2}\ {W_{sh}}^{4k}] \text{ where } k = [[j + 1] mod 11] + 1 \quad (5)$$

3.4 Classifier

SVM is used as a classifier. SVM is popular and efficient for binary classification. The performance of the proposed approach is evaluated at the image level by calculating the performance metrics like precision, recall also known as true positive rate (TPR), false positive rate (FPR), F-score and accuracy.

4. Result and Discussion

4.1 Dataset

The dataset used for the experiment is benchmark publicly available MICC-F220 of 110 non forged images and 110 forged images with 3 channels i.e., colour images of size 722 × 480 to 800 × 600 pixels. As shown in Figure 5, Figures 5a–5j are forged images with 10 different combinations of

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

geometrical and transformations attacks and Figure 5k is the non-forged image. From the dataset 154 images are chosen randomly for training purposes and remaining for testing purpose.

Figure 5: Dataset with 10 different combinations of geometrical and transformation attacks; (a–j), forged; (k), no forged images.

4.2 Baseline modules

The baseline models that are used for the comparison of the fusion model are summarized as follows.

1) Upload MICC-F220 Dataset: using this module we will upload dataset to application.
2) Pre-process Dataset: using this module we will read all images and then normalize their pixel values and then resize them to equal size.
3) Generate & Load Fusion Model: using this module we will train 3 algorithms called SqueezeNet, MobileNetV2 and ShuffleNet and then extract features from it to train fusion model. All algorithms prediction accuracy will be calculated on test data.
4) Fine Tuned Features Map with SVM: using this module we will extract features from all 3 algorithms to form a fusion model and then fusion data get trained with SVM and then calculate its prediction accuracy.
5) Run Baseline SIFT Model: using this module we will extract SIFT existing technique features from images and then train with SVM and get its prediction accuracy.
6) Accuracy Comparison Graph: using this module we will plot accuracy graph of all algorithms.
7) Performance Table: using this module we will display all algorithms performance table.

Table 2: Performance comparision.

Method	Accuracy	Precision	Recall	FSCORE
Existing SIFT SVM	68.1	67.9	67.5	67.5
Only SqueezeNet	79.5	81.1	79.5	79.2
Only ShuffleNet	56.8	62.7	56.8	51.1

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

Only MobileNetV2	81.8	82.9	81.8	81.6
Proposed Fusion Model SVM	95.4	95	96.1	95.3

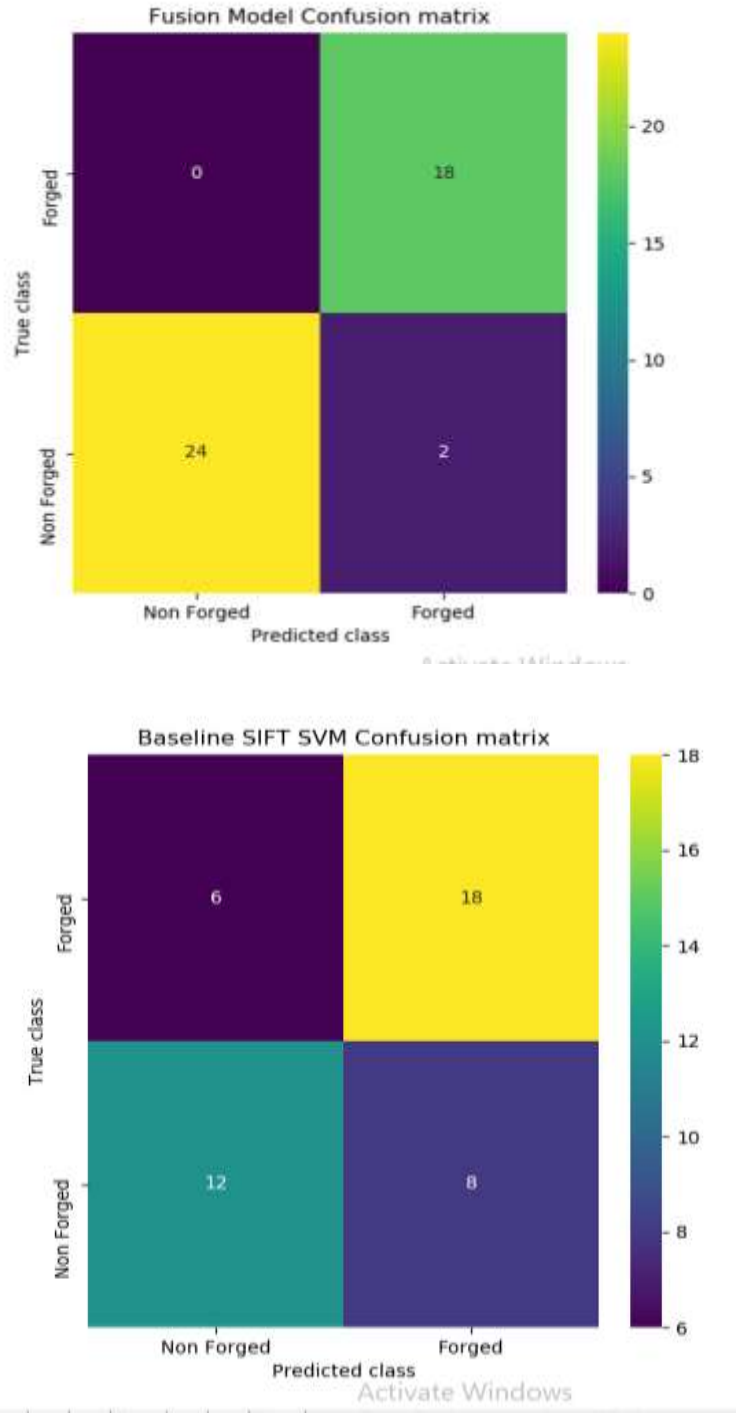

Figure 6: Confusion matrixes of fusion model and baseline SIFT SVM.

5. Conclusion

Image forgery detection helps to differentiate between the original and the manipulated or fake images. In this work, a decision fusion of lightweight deep learning-based models is implemented for

image forgery detection. The idea was to use the lightweight deep learning models namely SqueezeNet, MobileNetV2, and ShuffleNet and then combine all these models to obtain the decision on the forgery of the image. Regularization of the weights of the pretrained models is implemented to arrive at a decision of the forgery. The experiments carried out indicate that the fusion-based approach gives more accuracy than the state-of-the-art approaches. In the future, the fusion decision can be improved with other weight initialization strategies for image forgery detection.

References

[1]. Amerini, T. Uricchio, L. Ballan, and R. Caldelli, "Localization of JPEG Double Compression Through Multi-Domain Convolutional Neural Networks," 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2017, pp. 1865-1871, doi: 10.1109/CVPRW.2017.233.

[2]. B Xiao, Y Wei, X Bi, W Li, J Ma. “Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering”, Information Sciences, Volume 511, Pages 172-191, 2020, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2019.09.038.

[3]. Zhang Y, Goh J, Win LL, Thing VL. Image region forgery detection: a deep learning approach. SG-CRC 2016; 2016: 1-11.

[4]. Goh J, Thing VL. A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection. International Journal of Electronic Security and Digital Forensics 2015; 7 (1): 76-104

[5]. Sutthiwan P, Shi YQ, Zhao H, Ng TT, Su W. Markovian rake transform for digital image tampering detection. In: Shi YQ, Emmanuel S, Kankanhalli MS, Chang S-F, Radhakrishnan R (editors). Transactions on Data Hiding and Multimedia Security VI. Lecture Notes in Computer Science, Vol. 6730. Berlin, Germany: Springer; 2011, pp. 1-17

[6]. He Z, Lu W, Sun W, Huang J. Digital image splicing detection based on Markov features in DCT and DWT domain. Pattern Recognition 2012; 45 (12): 4292-4299.

[7]. Chang IC, Yu JC, Chang CC. A forgery detection algorithm for exemplar-based inpainting images using multi-region relation. Image and Vision Computing 2013; 31 (1): 57-71.

[8]. Rhee KH. Median filtering detection based on variations and residuals in image forensics. Turkish Journal of Electrical Engineering & Computer Science 2017; 25 (5): 3811-3826.

[9]. Lamba AK, Jindal N, Sharma S. Digital image copy-move forgery detection based on discrete fractional wavelet transform. Turkish Journal of Electrical Engineering & Computer Science 2018; 26 (3): 1261-1277.

[10]. Lin Z, He J, Tang X, Tang CK. Fast, automatic, and fine-grained tampered JPEG image detection via DCT coefficient analysis. Pattern Recognition 2009; 42 (11): 2492-2501.

[11]. Kwon, M.J.; Yu, I.J.; Nam, S.H.; Lee, H.K. CAT-Net: Compression Artifact Tracing Network for Detection and Localization of Image Splicing. In Proceedings of the 2021 IEEE Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, 5–9 January 2021; pp. 375–384.

[12]. Wu, Y.; Abd Almageed, W.; Natarajan, P. Mantra-Net: Manipulation Tracing Network for Detection and Localization of Image Forgeries With Anomalous Features. In Proceedings of the 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA, 15–20 June 2019; pp. 9535–9544.

ISSN- 2394-5125 VOL 10, ISSUE 01, 2023

[13]. Zheng, L.; Zhang, Y.; Thing, V.L. A survey on image tampering and its detection in real-world photos. J. Vis. Commun. Image Represent. 2019, 58, 380–399.

[14]. Rony, J.; Belharbi, S.; Dolz, J.; Ayed, I.B.; mccaffrey, L.; Granger, E. Deep weaklysupervised learning methods for classification and localization in histology images: A survey. Arxiv 2019, arxiv:abs/1909.03354.

[15]. Meena, K.B.; Tyagi, V. Image Forgery Detection: Survey and Future Directions. In Data, Engineering and Applications: Volume 2; Shukla, R.K., Agrawal, J., Sharma, S., Singh Tomer, G., Eds.; Springer: Singapore, 2019; pp. 163–194.

[16]. Abdel-Basset M, Manogaran G, Fakhry AE, El-Henawy I. 2-Levels of clustering strategy to detect and locate copy-move forgery in digital images. Multimedia Tools and Applications 2018; 79: 5419-5437. Doi: 10.1007/s11042- 018-6266-0

[17]. Kekre HB, Mishra D, Halarnkar PN, Shende P, Gupta S. Digital image forgery detection using Image hashing. In: IEEE International Conference on Advances in Technology and Engineering (ICATE); Mumbai, India; 2013. Pp.1-6. Doi: 10.1109/icadte.2013.6524736

[18]. Zhou P, Han X, Morariu VI, Davis LS. Learning rich features for image manipulation detection. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR); Salt Lake City, UT, USA; 2018. Pp. 1053-1061

[19]. Kuznetsov A. Digital image forgery detection using deep learning approach. Journal of Physics: Conference Series 2019; 1368 (3): 032028. Doi: 10.1088/1742-6596/1368/3/032028.

[20]. Bunk J, Bappy JH, Mohammed TM, Nataraj L, Flenner A et al. Detection and localization of image forgeries using resampling features and deep learning. In: IEEE Conference on Computer Vision and Pattern Recognition (CVPR) Workshops; Honolulu, HI, USA; 2017. Pp. 1881-1889.