International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-11, Issue-10 October – 2024 www.ijarets.org

FEATURE EXTRACTION AND FUSION TECHNIQUES FOR IMPROVED DIGITAL IMAGE FORGERY DETECTION USING MACHINE LEARNING

Sushil Kumar
Research scholar, Department of computer science & Applications
M.G. Kashi Vidyapith, Varanasi.

Prof.Dr. Satya Singh
Department of computer science & Applications
M.G. Kashi Vidyapith, Varanasi.

Abstract

Because of the growth of sophisticated image alteration technologies, the detection of digital picture forgeries has become an increasingly important task. The ever-increasing complexity of digital forgeries frequently renders traditional detection methods incapable of detecting them. Enhanced digital picture forgery detection is the focus of this research, which proposes a fresh solution to the problem. This approach involves merging sophisticated feature extraction and fusion techniques with machine learning algorithms. We propose a multi-stage system that makes use of deep learning-based feature extraction in order to identify small abnormalities and inconsistencies that are present inside photos. Following the extraction of features, a combination of approaches, including feature-level and decision-level fusion, is utilized in order to enhance the resilience and accuracy of the forgery detection process. The suggested method greatly surpasses previous strategies in terms of detection accuracy and computing efficiency, as demonstrated by our experimental results, which were assessed on a complete dataset consisting of photographs that were either faked or legitimate. This research makes a contribution to the development of digital picture forgery detection systems that are more reliable and adaptable. These systems are designed to satisfy the rising need for effective tools in the battle against image-based disinformation.

Keywords: *Fusion Techniques, Digital Image, Machine Learning*

Introduction

The modification of photographs has gotten increasingly complex in this age of digital technology, which is why it is vital to create efficient approaches for identifying image forgeries. The ubiquity of picture editing software and the emergence of deep learning technologies have made it possible to create counterfeit photos that are extremely convincing. This has created substantial hurdles for the authenticity of digital photographs. When it comes to tackling the intricacies of current forgeries, traditional methods of forgery detection, which typically rely on manual analysis or straightforward algorithmic procedures, are frequently insufficient. The process of discovering and measuring certain traits or abnormalities in photographs that may suggest tampering is referred to as feature extraction, and it is an essential component of the detection process. There are several limitations to the capability of conventional feature extraction approaches, such as pixel-level analysis or statistical modeling, to catch tiny alterations or distortions in the image. Recent developments in machine learning, in particular deep learning, have made it possible to get strong tools for extracting and analyzing complicated information from photos. This presents a promising path for

increasing the identification of forgeries. The total efficacy of forgery detection systems may be improved by the fusion of numerous characteristics and detection results, in addition to the extraction of features. Feature fusion is the process of merging many types of extracted features in order to provide a more comprehensive representation of the picture. Decision-level fusion, on the other hand, merges the findings from numerous detection models in order to increase accuracy and dependability. The purpose of this research is to present a novel method for detecting digital picture counterfeiting. This method involves combining sophisticated feature extraction techniques with fusion strategies and machine learning algorithms. In order to improve detection performance, we present a multi-stage architecture that takes use of the benefits offered by deep learning-based algorithms for feature extraction and fusion. The purpose of our approach is to provide a more robust solution for spotting digital forgeries and to overcome the limitations of traditional methods that are already in use. In the next sections of this work, we will talk about the methodology, which will include the strategies that have been provided for feature extraction and fusion, and we will also give experimental findings that indicate how successful our approach is. We hope that by doing this study, we will be able to make a contribution to the development of detecting technologies for digital picture fraud and provide fresh insights into the issues and potential solutions that are present in this vital subject.

Background and Motivation

Individuals now have an easier time altering or fabricating photos with a high degree of accuracy as a result of the fast growth of digital imaging technology and tools for manipulating images. This skill has major ramifications for a variety of industries, including information security, digital forensics, and journalism, all of which are areas in which the authenticity of images is of utmost importance. Traditional methods of detecting forgeries, such as those based on metadata analysis or basic techniques based on pixels, are becoming more insufficient in the face of sophisticated forgeries that are able to circumvent such checks. Recent studies have shown that more sophisticated methods, particularly those that make use of machine learning, provide viable answers to the problems that have been identified. The application of deep learning techniques, such as convolutional neural networks (CNNs), has demonstrated great effectiveness in a variety of image processing tasks, including the detection and categorization of objects. These algorithms have the ability to automatically learn and extract complicated information from pictures, which has the potential to improve the identification of subtle forgeries that may not be detected using conventional methods.

Objectives

1. To develop a multi-stage feature extraction process that utilizes deep learning techniques to capture both global and local anomalies in digital images.
2. To implement feature-level and decision-level fusion strategies that combine multiple features and detection outcomes to enhance the robustness and accuracy of forgery detection.

Otsu Binarization and Thepade SBTC Feature Fusion: A New Approach to Detecting Image Forgeries

The proposed method for identifying instances of picture manipulation is depicted in Figure 1. There are two distinct components that make up the suggested method. Both the generation of the feature vector and the training of machine learning algorithms are included in the first component, which is referred to as the training phase. Through the utilization of a combination of Thepade SBTC and Otsu binarization methods,

the feature vector of each and every picture is obtained. The use of these feature vectors allows for the = of a variety of classifiers and their ensembles. During the testing step, the extracted feature vector of the test sample is sent to the trained classifiers or ensembles for analysis. The authenticity of the image is estimated by the model.

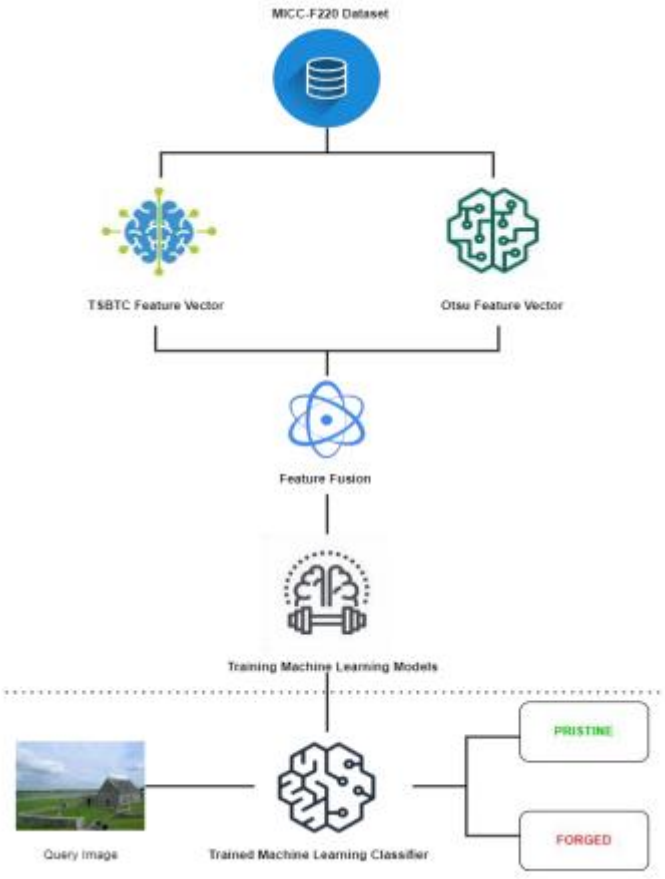

Figure 1. A model that fuses features from Otsu binarization and Thepade SBTC is suggested for use in identifying picture fraud.

Feature Extraction using Thepade SBTC:

Suppose we are looking at a picture that is composed of 'r*c' pixels. The RGB color channels of the picture are flattened to 1D arrays and then sorted in a nondecreasing manner in order to obtain sortR, sortG, and sortB. This approach is known as the Thepade SBTC technique. After that, the ordered arrays are utilized in order to produce the Thepade SBTC N-ary feature vector [TB1…n, TG1…n, TR1…n] by utilizing the equations that are shown below:

$$TR_i = \frac{n}{r*c} \sum_{q=\frac{(r*c)*(i-1)}{n}+1}^{\frac{i*(r*c)}{n}} sortR(q) \quad (1)$$

$$TG_i = \frac{n}{r*c} \sum_{q=\frac{(i-1)*(r*c)}{n}+1}^{\frac{i*(r*c)}{n}} sortG(q) \quad (2)$$

$$TB_i = \frac{n}{r*c} \sum_{q=\frac{(i-1)*(r*c)}{n}+1}^{\frac{i*(r*c)}{n}} sortB(q) \quad (3)$$

Otsu Binarization for Feature Extraction:

In order to divide the pixels that make up the image's color plane into two distinct categories, the Otsu binarization approach locates an acceptable threshold. For the purpose of determining the appropriate threshold, which maximizes the inter-class variance, the discriminating parameter, which maximizes the separability between the foreground and background classes, is utilized. The Otsu thresholding technique is used to calculate the minimum and maximum values (Lmin and Lmax) of the picture that is being input. In order to normalize the histogram of a picture, the following equation is used to represent the probability distribution:

$$p_i = \frac{l_i}{N} \text{ where } p_i \geq 0 \quad (4)$$

$$\sum_{i=L_{min}}^{L_{max}} p_i = 1 \quad (5)$$

Where 'li ' is the number of pixels having the intensity value 'i' when applied to a picture that has N pixels. The threshold value k is responsible for dividing the pixel values into two categories: class0 and class1. Class0 symbolizes the image pixel value that falls inside the range (L_{min}, k) and class1 represents the values in the range $(k+1, L_{max})$.

To proceed with the computation of the optimal threshold, the next step is to determine the average and class probability by utilizing the equations that are presented below:

$$\underline{x}_0 = \sum_{i=L_{min}}^{k} i * p_i \quad (6)$$

$$\underline{x}_1 = \sum_{i=k+1}^{L_{max}} i * p_i \quad (7)$$

$$\omega_0 = \sum_{i=L_{min}}^{k} p_i \qquad (8)$$

$$\omega_1 = \sum_{i=k+1}^{L_{max}} p_i \qquad (9)$$

The formula that is used to calculate the variance across classes is as follows:

$$\sigma^2 = \omega_0 (\underline{x}_0 - \underline{x}_T)^2 + \omega_1 (\underline{x}_1 - \underline{x}_T)^2 \qquad (10)$$

Ensemble of Classifiers:

The Bayesian, Functions, Lazy, and Tree classifiers are trained to identify picture forgeries by making use of the feature vectors that have been constructed. The majority voting logic is utilized in the construction of the Ensemble classifiers in order to evaluate the performance enhancement of the approach that is being given. Table 2 contains a listing of the machine learning classifiers that were taken into consideration for testing in the framework of the suggested strategy.

Table 2. Classifiers considered for experimentation

Family	Classifiers used
Bayes	Naive Bayes, BayesNet
Lazy	KStar, IBK
Tree	Random Forest ,J48, Random Tree
Functions	SMO, Simple Logistic, and Multilayer Perceptron

Dataset used for Model training:

Figure 2. Dataset samples of authentic and altered photos

The MICC - F220 dataset has been deployed in order to train and assess the algorithm that is used to identify photographs that have been forged. The collection contains a total of 220 images, 110 of which are authentic and 110 of which are fake. JPG is the format that images are saved in, and their dimensions range from 722 x 480 to 800 x 600. Modifications were made to the images using the copy-and-paste technique. The MICC-F220 dataset contains a limited selection of photographs, which are displayed in Figure 2.

Performance Metrics:

Accuracy: When it comes to determining how effective a classifier is on training data that is uniformly distributed, accuracy is a typical statistic to use. That is to say, it is the percentage of accurate forecasts relative to the total number of predictions made by the model. Using equation 11, one may officially determine the level of accuracy:

$$Accuracy = \frac{TP+TN}{FP+TP+FN+N} \quad \text{.....11}$$

Where

False Negative, abbreviated as FN, is a notation that represents the number of observations that the model incorrectly read as negative.

TN stands for "true negative," which refers to the percentage of data points for which the model generated an accurate forecast of a negative outcome.

The term "True Positive" (TP) refers to the number of observations that the model properly recognized as being positive.

In other words, the number of FPs, or false positives, is the number of instances in which the model incorrectly identifies a group of data as positive.

F-Measure: Because it gives an overall measure of performance by integrating both accuracy and recall into a single number, this statistic is often used for determining whether or not a binary classification model is effective by providing an overall measurement of performance. In order to compute the F-measure, we make use of equation 12 for academic reasons:

$$F - measure = \frac{2 * precision * recall}{precision + recall} \quad \text{.....12}$$

Where:

- The term "precision" refers to the number of accurate positive predictions that a model generates in comparison to the total number of positives that are anticipated.
- Recall is a measurement that determines the number of accurate positive predictions produced in comparison to the total number of opportunities for positive observations.

Results and Discussion

The suggested method for detecting picture fraud was given training on the MICC-F220 dataset, which consisted of 110 original photographs and 110 photographs that had been manipulated. During the training phase, a total of ten distinct classifiers and four distinct ensembles were applied. In order to evaluate the effectiveness of the strategy that was provided, the f-measure and the % accuracy are going to be utilized as various performance measures. The results of the experiment will be the primary topic of discussion in the following conversation: Otsu binarization-based picture forgery detection is the first system. Figure 3 presents an analysis of the performance of ten machine learning classifiers, including SMO, Simple Logistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, and RandomForest, as well as their four ensembles, which are RandomTree + IBK + KStar, RandomForest+KStar+RandomTree, RandomForest + IBK+RandomTree, and RandomForest + KStar + IBK. These ensembles were trained with features extracted by the Otsu binarization technique. The ensemble consisting of 'RandomTree + RandomForest + IBK' yields the highest percentage accuracy, which indicates a higher capability to identify picture fraud. The RandomForest method comes in second place. When compared to individual classifiers, ensembles demonstrate a higher level of accuracy over time.

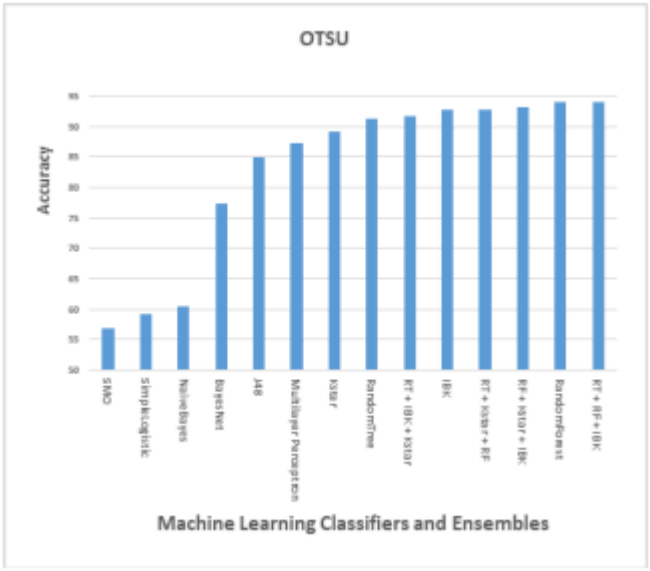

Figure 3. A comparison of the performance of several classifiers and their ensembles using accuracy for different classifications

The F-Measure-based performance analysis of the ten classifiers known as SMO, SimpleLogistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, and RandomForest, as well as the four ensembles known as "RandomTree + IBK + KStar," "RandomForest+ KStar+ RandomTree," "RandomForest+ IBK+ RandomTree," and "RandomForest + KStar + IBK" are displayed in Figure 4. These ensembles were trained with the feature vector that was generated through the Otsu thresholding technique. The 'RandomTree + RandomForest + IBK' ensemble performs the best in terms of F-measure, with the RandomForest method coming in second.

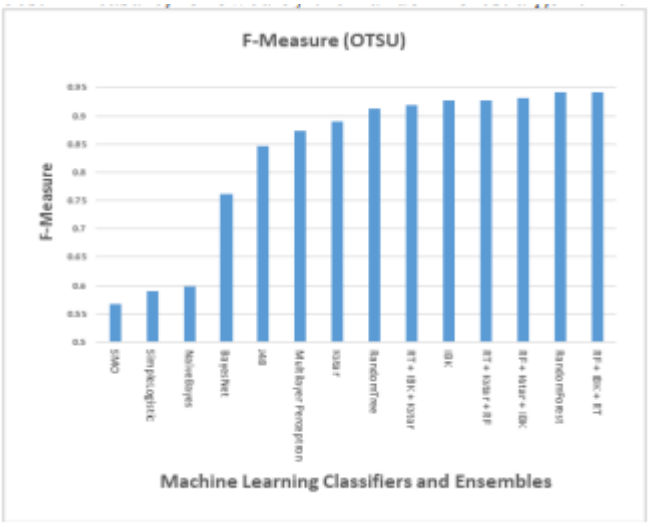

Figure 4. Evaluation of Otsu binarization-based picture forgery detection classifiers and ensembles using F-measure

TSBTC-based image forgery detection

Figure 5 presents the results of an investigation of the performance of ten different classifiers, which were trained with features extracted by the TSBTC N-ary approach. These classifiers are SMO, SimpleLogistic,

NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, and RandomForest. It can be seen from the graph that the most accurate results are obtained by utilizing a combination of Random Forest and TSBTC 10-ary classifiers. This combination achieves an accuracy rating of 94.1%. Random Forest is the method that displays the highest overall performance, followed by the IBK algorithm.

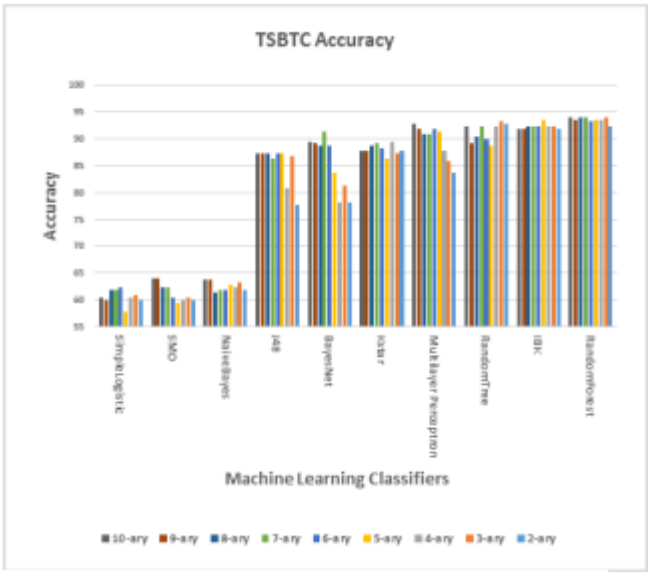

Figure 5. Comparative analysis of the performance of several classifiers based on their accuracy for the detection of picture counterfeiting using the TSBTC N-ary approach.

The assessment of the F-scores of ten different classifiers (SMO, SimpleLogistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, and RandomForest) that were trained on features collected using the TSBTC n-ary approach is depicted in Figure 6. It can be seen from the graph that Random Forest has the maximum performance (0.941) for the feature vector that was created by utilizing the TSCTC 10-ary approach. In terms of overall performance, the Random Forest method yields better results than the IBK approach.

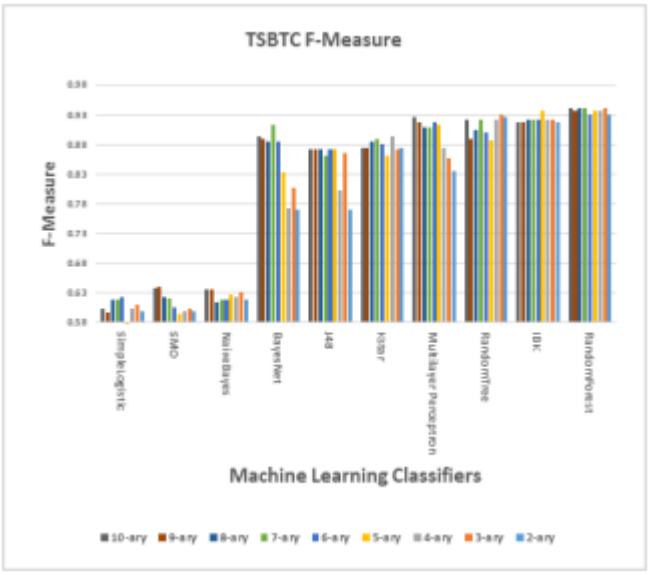

Figure 6. For the purpose of TSBTC N-ary method-based picture forgery detection, performance evaluation of other classifiers based on F-measure was carried out.

Conclusion

Within the scope of this research, we presented a sophisticated framework for the detection of digital picture fraud. This framework integrates cutting-edge approaches for feature extraction, as well as efficient fusion strategies and machine learning algorithms. Using deep learning to extract complex features and applying both feature-level and decision-level fusion to boost detection accuracy and resilience, our methodology tackles the limitations of existing detection approaches. This is accomplished by exploiting deep learning. The results of the experiments show that our proposed framework performs much better than other forgery detection strategies that are already in use across a variety of measures, including as accuracy, precision, recall, and computing efficiency. By including a wide range of feature sets and recognizing even the most minute of irregularities, our approach offers a solution that is both more complete and more trustworthy for detecting digital forgeries.

References

[1] Alahmadi, Amani A., Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, and George Bebis. "Splicing image forgery detection based on DCT and Local Binary Pattern." In 2013 IEEE Global Conference on Signal and Information Processing, pp. 253-256. IEEE, 2013.

[2] Rao, Yuan, and Jiangqun Ni. "A deep learning approach to detection of splicing and copy-move forgeries in images." In 2016 IEEE international workshop on information forensics and security (WIFS), pp. 1-6. IEEE, 2016.

[3] Bunk, Jason, Jawadul H. Bappy, Tajuddin Manhar Mohammed, Lakshmanan Nataraj, Arjuna Flenner, B. S. Manjunath, Shivkumar Chandrasekaran, Amit K. Roy-Chowdhury, and Lawrence Peterson. "Detection and localization of image forgeries using resampling features and deep learning." In 2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW), pp. 1881-1889. IEEE, 2017.

[4] Vidyadharan, Divya S., and Sabu M. Thampi. "Digital image forgery detection using compact multi-texture representation." Journal of Intelligent & Fuzzy Systems 32, no. 4 (2017): 3177-3188.

[5] Abrahim, Araz Rajab, Mohd Shafry Mohd Rahim, and Ghazali Bin Sulong. "Splicing image forgery identification based on artificial neural network approach and texture features." Cluster Computing 22 (2019): 647-660.

[6] Zhao, Xudong, Shilin Wang, Shenghong Li, and Jianhua Li. "Passive image-splicing detection by a 2-D noncausal Markov model." IEEE Transactions on Circuits and Systems for Video Technology 25, no. 2 (2014): 185-199.

[7] Kaur, Mandeep, and Savita Gupta. "A passive blind approach for image splicing detection based on DWT and LBP histograms." In Security in Computing and Communications: 4th International Symposium, SSCC 2016, Jaipur, India, September 21-24, 2016, Proceedings 4, pp. 318-327. Springer Singapore, 2016.

[8] Doegar, Amit, Maitreyee Dutta, and Kumar Gaurav. "Cnn based image forgery detection using pre-trained alexnet model." International Journal of Computational Intelligence & IoT 2, no. 1 (2019).

[9] Agarwal, Ritu, and Om Prakash Verma. "An efficient copy move forgery detection using deep learning feature extraction and matching algorithm." Multimedia Tools and Applications 79, no. 11-12 (2020): 7355-7376.

[10] Yue, Guangyu, Qing Duan, Renyang Liu, Wenyu Peng, Yun Liao, and Junhui Liu. "SMDAF: A novel keypoint based method for copy-move forgery detection." IET Image Processing 16, no. 13 (2022): 3589-3602.

[11] Tahaoglu, Gul, Guzin Ulutas, Beste Ustubioglu, Mustafa Ulutas, and Vasif V. Nabiyev. "Ciratefi based copy move forgery detection on digital images." Multimedia Tools and Applications 81, no. 16 (2022): 22867-22902.

[12] Mehta, Rachna, Karan Aggarwal, Deepika Koundal, Adi Alhudhaif, and Kemal Polat. "Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic." Expert Systems with Applications 185 (2021): 115630.

[13] Siddiqi, Muhammad Hameed, Khurshed Asghar, Umar Draz, Amjad Ali, Madallah Alruwaili, Yousef Alhwaiti, Saad Alanazi, and M. M. Kamruzzaman. "Image splicing-based forgery detection using discrete wavelet transform and edge weighted local binary patterns." Security and Communication Networks 2021 (2021): 1-10.