IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 4, April 2024

DOI: 10.17148/IJARCCE.2024.13440

Digital Image Forgery Detection Using CNN & ELA

Swetha Bana[1], Bhavana P[2], Abhinaya N[3], Siva Pullaiah M[4], Sukeerthi B[5]

Assistant Professor, Department of Computer Science and Engineering, Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, 518501[1]

Department of Computer Science and Engineering, Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal, 518501[2-5]

Abstract: With the expanding utilize of advanced pictures in different applications, the issue of picture fraud has ended up more predominant than ever One of the greatest issues these days is picture frauds or control using different procedures In this paper, we propose a novel advanced picture fraud location framework based on Convolutional Neural Systems (CNNs) that can identify different sorts of picture controls, counting copy-move, grafting, and correcting. Our proposed framework coordinating Mistake Level Investigation (ELA) with profound learning strategies to supply a more exact and dependable arrangement to the issue of computerized picture imitation location. We assessed the proposed framework on a dataset of real-world pictures and accomplished a tall location precision of 93% Our framework outflanked existing strategies for picture imitation location and illustrated its potential for different applications, counting forensics, security, and computerized picture investigation. A convolutional neural organize that has been appeared successful for picture preparing is utilized at first. Generally, the proposed CNN-based picture imitation location framework offers a vigorous and successful arrangement to the developing issue of picture control and fraud in today's visual media scene. The execution of the proposed strategy is tried quantitatively, and picture alteration is distinguished

Keywords: Digital image analysis, Convolutional neural network (CNN), Error Level Analysis (ELA), Image processing.

I. INTRODUCTION

Digital image forgery detection is a critical task in today's digital landscape, where images are widely shared and manipulated for various purposes, including spreading misinformation and perpetrating fraud. This introduction delves into the application of Convolutional Neural Networks (CNNs) and Error Level Analysis (ELA) in detecting digital image forgeries, highlighting their significance and potential in combating the proliferation of fake images. With the advent of social media and advanced editing tools, the dissemination of manipulated images has become pervasive. This poses significant challenges in discerning authentic content from manipulated ones, especially given the sheer volume of visual content shared daily on digital platforms.

ELA, a forensic technique, plays a pivotal role in identifying digital image forgeries. It works by analyzing the error introduced during the compression process, thereby differentiating between authentic and manipulated portions of an image. When an image is forged, such as through splicing or copy-move manipulation, ELA detects discrepancies in compression artifacts, revealing regions of potential manipulation.

Complementing ELA, CNNs offer a powerful tool for detecting image forgeries by leveraging deep learning techniques. CNNs are adept at learning hierarchical representations of features within images, making them well-suited for tasks such as image classification and manipulation detection. By training CNNs on datasets of authentic and manipulated images, the network learns to distinguish between genuine and forged content based on learned features.

In the proposed approach, ELA is used to preprocess images, highlighting potential areas of manipulation based on compression artifacts. These ELA-enhanced images are then fed into a specialized CNN architecture designed for forgery detection. The CNN analyzes the images to identify patterns and features indicative of manipulation, enabling accurate detection of digital image forgeries.

One of the key advantages of using CNNs and ELA together is their ability to address different types of image forgery. While ELA excels at detecting passive forgery techniques like splicing and copy-move manipulation, CNNs can further refine the detection process by learning intricate features indicative of manipulation.

DOI: 10.17148/IJARCCE.2024.13440

Furthermore, the integration of CNNs and ELA offers a holistic approach to digital image forgery detection, combining the strengths of both techniques to achieve higher accuracy and robustness. By leveraging the power of deep learning and forensic analysis, this approach holds promise in mitigating the spread of fake images and preserving the integrity of digital media content.

Our contributions in this paper are summarized as follows:

- Introduction of a novel architecture exhibiting superior accuracy compared to other methods.
- Comparative analysis of our proposed technique against statistical and deep learning methods.
- Evaluation of the models on diverse datasets to assess functionality across varied sample sets.

In summary, the combination of CNNs and ELA represents a cutting-edge approach to digital image forgery detection, offering a potent solution to the challenges posed by the proliferation of manipulated images in the digital age.

II. RELATED WORK

A technique was presented by Hakimi et al. [1] in which the chromatic components of an image were utilized to improve the procedure for identifying fake images. After testing on the CASIA v2.0 dataset, they discovered that the Cb showed the coherence of their suggested strategy, as the component was nearly identical to the Cr component.. [2] introduced a method to enhance forgery detection by reducing processed information and employing Discrete Wavelet Transform (DWT) with Singular Value Decomposition (SVD) for robust block representation. Mahale, V. H et al. [3] developed a technique using Local Binary Patterns (LBP) on the COMOFOD dataset to identify image inconsistencies. Wu-Chi et al. [4] summarized forgery methods, including watermarking and alpha manipulation detection, while [5] proposed a CNN-based approach for copy-move manipulation detection, pioneering research in this area, though lacking robustness for real-world application.

III. DATASETS

For the purposes of this study, we have employed three datasets: MICC-F220, CASIA V2.0 [6], and MICC-F2000 [7]. The hand-selected datasets guarantee that the suggested approach is extensively tested using a range of use scenarios. These datasets contain manipulated images that are harder to spot with the unaided eye and appear more realistic to the human eye. The dataset was chosen because the algorithms are tested on a wide range of photos, and the results are comprehensive, accounting for the majority of use cases that are present and demonstrating their use across all of them. Table 1 provides a summary of the datasets information.

IV. PROPOSED METHODOLOGY

A. Preprocessing:

During preprocessing, the following methods are applied:

- Image resizing: Set input images' dimensions to a constant of (224,224,3)
- Image normalization: Increasing convergence in training and accuracy in testing by scaling pixel values to a predetermined range.
- Color space conversion: Relevant properties for counterfeit detection are improved by converting RGB to a new color space.
- Error Level Analysis (ELA): This technique finds possible forging locations by identifying areas with varying compressions.
- Image augmentation: By transforming input images randomly, more training data is produced and overfitting is decreased.

B. **Error Level Analysis**

ELA is one of the most significant methods for spotting image manipulation [8]. Compressing an image is claimed to be a lossy process, and ELA records the distortion caused by compression throughout that time. JPEG is one such format where it works well. An image captured with a digital camera undergoes compression only once during the saving process. But the picture undergoes additional compression when someone tries to alter or tamper with it using programs like Adobe Photoshop, GIMP, etc. After storing them at a specific quality, ELA computes the ratio to detect the difference between the compression levels and finds the tampering. The areas that have been altered are depicted by the genuine components are represented by the local minima, not the local maxima.

DOI: 10.17148/IJARCCE.2024.13440

When JPEG files are saved, they are compressed individually and stored in 8 x 8 blocks. The compression difference of each 8 x 8 block in a clean image is consistent throughout, however it is erratic with altered images, as previously stated. When the amount of image editing grows, the ELA further declines.

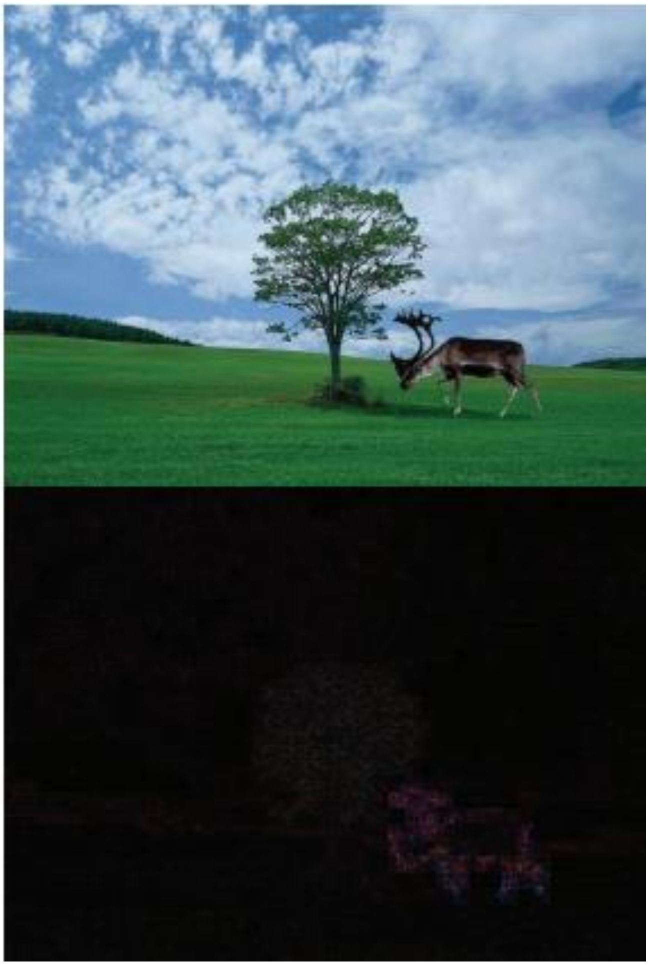

Fig. 1: Forged image and it's ELA image

As we can see in Fig. 1 the regions that appear to be brighter in ELA are considered to be forged.

C. CNN (Convolutional Neural Network)

A feedforward neural network architecture for deep learning that learns from the data itself is the convolutional neural network (CNN) [9]. The mathematical phenomena of repeatedly feeding the output of one function into another is referred to as convolution. Although its primary purpose was handwriting detection, it has been shown to be useful in classification, identification, segmentation, and detection of images. It makes an attempt to mimic the visual nerve system of humans. CNN is a great tool for handling data having a lot of dimensions. CNN successfully decreases the number of dimensions while preserving the image's pertinent and significant elements.

The architecture of CNN is made up of three layers: the pooling layer, the fully linked layer, and the convolution layer. The pooling layer reduces dimensionality and guards against overfitting. Features are taken out of the convolution. The fully connected layer is used to obtain the desired output, just like in traditional neural networks. In order to obtain different feature maps and make it easier to categorize the filtered output, we can calibrate numerous filters in the CNN convolution layer with both variable and trainable values. The goal was to create a simplified CNN model that could effectively recognize images, however the original CNN design used complex models with multiple layers. manipulation with relation to current theories

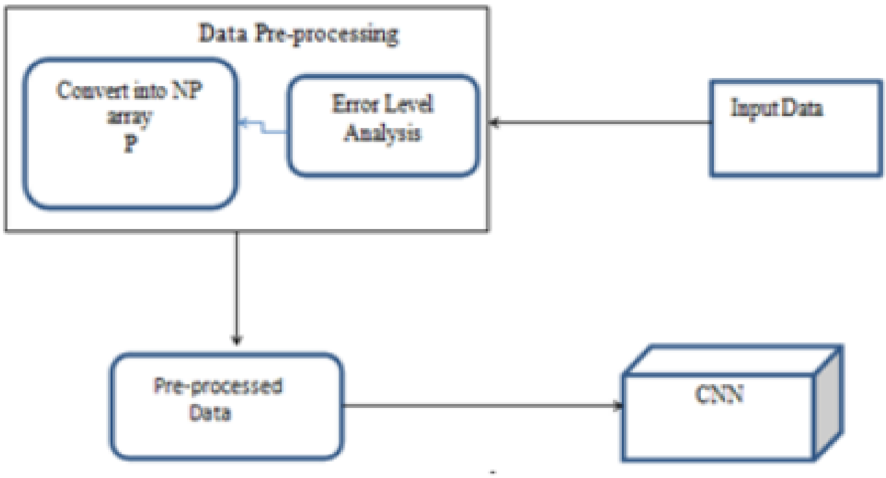

Fig .2: shows the overall structure of the proposed model.

D. Feature Extraction
The max pool layer of size 2x2 is inserted after each convolutional layer in the suggested model, which consists of five convolutional layers in total. The max pool layer enforces the dimensionality reduction of the feature map and the selection of the maximum element from a certain location. With the initial image input size set to (224x224x3), the CNNs use filters to identify characteristics throughout the whole input image, including edges.

The convolution layer in all five layers of the suggested model has a filter size of (3, 3), and it is backed by a RELU activation function (equation 1) [10]. This is followed by a max pooling layer with a size of (2, 2).

The input size for the first layer is (224, 224, 3). The number of feature maps that are present in each layer, which increases gradually, is what sets each layer apart from the others. The first layer has 16 feature maps, the second has 32, the third has 64, and the fourth and fifth layers have 128 and 256 feature maps, respectively.

$$\mathrm{Relu}(x) = \max(0, x) \quad (1)$$

Fig 3: shows the detailed architecture of cnn used in the proposed method

E. Classification
The categorization of the supplied image is the last phase in the suggested model. The final layer of the convolutional process yields an output, which is fed into the global average pooling layer that makes up the classification part.

After that, there is a fully connected layer that uses the activation function (equation 2) of SoftMax [11] to build final feature maps, from which it acquires vectors during the pooling phase. Equation 3, which uses the binary cross entropy function [12] as the loss function, was optimized by Adam [13] for faster computing. At some point, it will be possible to tell if the input image is legitimate or a fake by identifying its type

$$\sigma(y_i) = \left(\frac{e^{y_i}}{\sum_j e^{y_j}}\right) j = 1, \dots, n \qquad (2)$$

$$BCE = \left(-(y\log(p) + (1 - y)\log(1-p))\right)\ j = {}_{1,\,\dots,\,n}$$

where, y is the binary indicator (0 or 1) if class label c is the correct classification for observation o and p is the predicted probability observation o is of class c

DOI: 10.17148/IJARCCE.2024.13440

TABLE 1: DATASET

Dataset Name	Configurations	Size of Images(In Pixels)	Characteristics
CASIA v2.0	7,200 unspoiled images and 5,123 tampered images	Between 320 x 240 to 800x600	It contains blurring of the tampered image set besides the splicing
MICC-F220	110 pristine and 110 tampered images	Between 722 x 240 and 800 x 600	The tampered region represents 1.2% of the entire image
MICC-F2000	1300 authentic and 700 tampered images	2048x1536	The tampered region comprises of 1.12% of the entire image

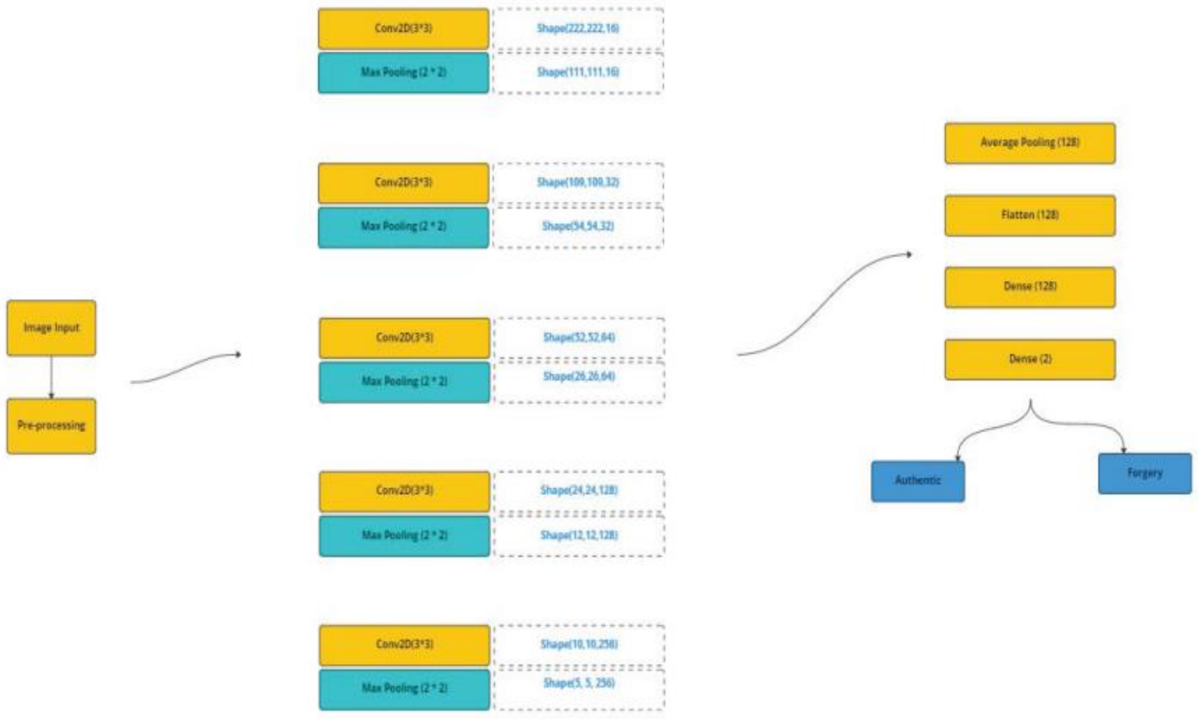

Fig3: CNN Architecture

V. EXPERIMENTATION AND RESULT

We used a device with an Intel CPU, 8GB RAM, and no GPU for our study. We have assessed the performance of our suggested model utilizing the existing 100 epoch training configuration with a learning rate of 0.0001 and a batch size of 32. ResNet50, VGG16, and VGG19 architectures were examined with a training configuration consisting of 10 epochs, 32 batch sizes, and a 0.0001 learning rate. Additionally, we changed the batch size, number of epochs, and learning rate to see how these factors affected the accuracy of the model. Predicated on block DCT coefficients' statistical characteristics:

A. Comparative Analysis

Predicated on block DCT coefficients' statistical characteristics:
First, the test image supplied for this investigation is converted to the Y Cb Cr color system. The majority of tampering indicators are hidden in the chroma components, and human eyes are better at discerning the difference between luminance and chroma components.

DOI: 10.17148/IJARCCE.2024.13440

The Y, Cr, and Cb chroma components generate features, which when added together result in a terminal feature vector. For every 8x8 pixel block that does not overlap with another, a 2D-DCT operation was performed. To generate a sub-image, use this. We employ the three feature vectors (Y, Cr, and Ch) produced from these three sub images to create the final feature vector. The difference between spliced and genuine be applied to categorize photos. SVM is used for image classification [14].

2) SVM Classifier and LBP-DCT-Based: The input Images are transformed into a Gray, Y, Cb, and Cr color space. After being split into blocks, the first phase's output is passed into the block DCT for additional processing. The DCT coefficient's magnitude component is taken out and entered into the LBP operator. Following this, the LBP picture is divided into blocks, and the mean features are taken out and fed into the SVM classification model. By only taking into account neighboring pixels with values strictly greater than the candidate pixel value, LBP suppresses other pixels. LBP is applied following and not before to due to decreased precision because The results of the comparison between the suggested approach and the three trained CNN architectures, VGG16, VGG19 [16], and RESNET50 [17], are detailed

B. Evaluation Metrics

Evaluation metrics are used to measure the performance of machine learning models and algorithms. They provide a quantitative measure of how well a model is performing on a particular task or dataset. Different evaluation metrics are used depending on the nature of the problem being solved and the goals of the analysis. Here are some common evaluation metrics: Accuracy, Precision and Recall.

Accuracy:

Accuracy is a measure of how often a classifier correctly predicts the correct label out of all the instances. It's a simple and intuitive metric commonly used to evaluate classification models. A higher accuracy indicates better performance, but it may not be the best metric for imbalanced datasets where one class dominates the others. Accuracy doesn't provide insights into the types of errors a model makes, such as false positives or false negatives.

$$\text{Accuracy} = \frac{(TP+TN)}{(TP+FP+FN+TN)}$$

Precision:

Precision is a measure of the proportion of true positive instances among all instances that the model classified as positive. It indicates the accuracy of positive predictions made by the model. A higher precision value suggests that the model is making fewer false positive predictions. Precision is particularly important when the cost of false positives is high, as it focuses on the accuracy of positive predictions.

$$\text{Precision} = \frac{TP}{TP+FP}$$

Recall:

Recall, also known as sensitivity, measures the proportion of true positive instances that were correctly identified by the model. It assesses the model's ability to capture all positive instances in the dataset. A higher recall value indicates that the model is effectively identifying most of the positive instances. Recall is crucial when the cost of missing positive instances (false negatives) is high, as it focuses on the model's ability to minimize such errors.

$$\text{Recall} = \frac{TP}{TP+FN}$$

TABLE II: Results

Algorithm/Dataset	**CASIA V2.0**			**MICC-F220**			**MICC-F2000**		
	Accuracy	Precision	Recall	Accuracy	Precision	Recall	Accuracy	Precision	Recall
DCT+SVM	0.97	0.95	0.92	0.86	0.83	0.78	0.93	0.88	0.90
DCT+LBP+SVM	0.96	0.94	0.92	0.92	0.86	0.91	0.94	0.92	0.89
ELA+VGG16	0.72	0.66	0.67	0.87	0.82	0.88	0.89	0.88	0.90
ELA+VGG19	0.74	0.69	0.72	0.88	0.89	0.85	0.90	0.89	0.88
ELA+RESNET50	0.60	0.59	0.55	0.70	0.60	0.85	0.76	0.65	0.80
ELA+CNN (Proposed)	0.98	0.95	0.92	0.97	0.93	0.91	0.98	0.96	0.94

DOI: 10.17148/IJARCCE.2024.13440

C. Results
Our suggested approach was tested with several statistical and deep learning techniques on three distinct datasets: CASIA V2.0, MICC-F220, and MICC-F2000.The best technique that performs well across all image datasets can be inferred from the results. The metrics gathered after testing are displayed in Table 2. The CNN model with ELA demonstrated high validation accuracy for forgery detection on several datasets, including 98.25% for CasiaV2, 97.32% for MICC F-220, and 98.67% for MICC F-2000, according to the research paper's findings.

Furthermore, the suggested approach outperformed popular pretrained models like VGG16, VGG19, and ResNet50 as well as widely used statistical techniques like DCT and LBP+DCT. The statistical methods were able to outperform the other deep learning methods on the CASIA V2.0 dataset, which is significant. The CNN architecture introduced in this paper was able to work better with ELA than other well-established architectures.

The proposed method obtained lowest accuracy on the MICCF220 dataset, even though this dataset is the smallest of the three. This can be attributed to the fact that this dataset contains images of variable sizes. On the other hand, the lowest average accuracy was obtained on the CASIA V2.0 dataset, which may be due to its larger size and varying image resolutions. Notably, for the majority of models, the testing accuracy matched the validation accuracy. These findings imply that the suggested CNN model with ELA pre-processing may be a useful method for detecting forgeries in a variety of situations.

VI. CONCLUSION AND FUTURE WORK

Today's culture finds it annoying when people tamper with images and videos. Given the volume of data that is becoming more readily available online and the rapid improvements in technology, this issueis just going to get bigger. Forgery detection is a problem that has to be given the attention it deserves and updated with the always changing tools and technologies. In this study, we suggested a methodology that uses CNN and ELA in tandem to tackle this problem. With little processing resources needed, the approach's results were able to attain excellent accuracy across a variety of databases. When tested against a few cutting-edge techniques, our strategy outperforms others on particular datasets.

The study goes into great detail on how to use ELA for feature extraction and how it simplifies the counterfeit detection process by offering a ballpark area where the image has the maximum potential for manipulation. The CNN algorithm has demonstrated its effectiveness in handling pixel data, and the study supports the method's ability to process and categorize images. in the future, this technology can be expanded to be used in the areas of segmenting images and videos, detecting numerous kinds of tampering techniques. There is always a need to improve approaches' resilience and speed in an environment where the volume of data being transmitted is growing exponentially. More work may be put into creating improved image datasets with a variety of samples to fully test detection algorithms. people must do research and address the various applications of fabricated photos as the accuracy of tools and software in this regard is growing.

REFERENCES

[1]. Hariri, Mahdi & Hakimi, Fahime. (2015). Image-Splicing Forgery Detection Based On Improved LBP and K-Nearest Neighbors Algorithm.Electronics Information and Planning. 3.

[2]. G. Li, Q. Wu, D. Tu & S. Sun, ”A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries Based on DWT and SVD,” 2007 IEEE International Conference on Multimedia and Expo,Beijing, China, 2007, pp. 1750-1753

[3]. Vivek H. Mahale, Mouad M.H. Ali, Pravin L. Yannawar & Ashok T.Gaikwad, ”Image Inconsistency Detection Using Local Binary Pattern (LBP)”, Procedia Computer Science, Volume 115, 2017, Pages 501-508.

[4]. Hu, W. C., Chen, W. H., Huang, D. Y., & Yang, C. Y. (2016). ”Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes.” Multimedia Tools and Applications, 75, 3495–3516, (2016)

[5]. J. Ouyang, Y. Liu & M. Liao, ”Copy-move forgery detection based on deep learning,” 2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISPBMEI), Shanghai, 2017, pp. 1-5.

[6]. J. Dong, W. Wang & T. Tan, ”CASIA Image Tampering DetectionEvaluation Database,” 2013 IEEE China Summit and InternationalConference on Signal and Information Processing, Beijing, China, 2013,pp. 422-426.

[7]. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo & G. Serra. “A SIFT-based forensic method for copy-move attack detection and transformation recovery”, IEEE Transactions on Information Forensics and Security, vol. 6, issue 3, pp. 1099-1110, 2011.

[8]. N. Krawetz, ”A picture’s worth...digital image analysis and forensics”, Texas, United States, Hacker Factory

DOI: 10.17148/IJARCCE.2024.13440

Solutions, pp. 11-16; 52-64, 2007

[9]. Y. LeCun, L. Bottou, Y. Bengio, & P. Haffner, ”Gradient-Based Learning Applied to Document Recognition,” Proceedings of the IEEE, vol. 86, no. 11, pp. 2278-2324, Nov. 1998.

[10]. V. Nair & G. E. Hinton, ”Rectified Linear Units Improve Restricted Boltzmann Machines,” in Proceedings of the 27th International Conference on Machine Learning (ICML), Haifa, Israel, 2010, pp. 807-814.

[11]. John S. Bridle, 1989,”Training stochastic model recognition algorithms as networks can lead to maximum mutual information estimation ofparameters.” In Proceedings of the 2nd International Conference on Neural Information Processing Systems (NIPS’89). MIT Press, Cambridge,MA, USA, 211–217.

[12]. C. Cortes and V. Vapnik,”A Theory of Multiclass Support Vector Machines,” Journal of Machine Learning Research, vol. 2, pp. 1-32, 1995.

[13]. S. Ruder, “An overview of gradient descent optimization algorithms,”arXiv preprint arXiv:1609.04747, 2016.

[14]. Shilpa Dua, Jyotsna Singh & Harish Parthasarathy, Image forgery detection based on statistical features of block DCT coefficients, Procedia Computer Science,Volume 171, 2020, Pages 369-378, ISSN 1877-0509.

[15]. Islam, M.M.; Karmakar, G.; Kamruzzaman, J.; Murshed, M. ”A RobustForgery Detection Method for Copy–Move and Splicing Attacks in Images.” Electronics 2020, 9, 1500.

[16]. Simonyan, Karen & Zisserman, Andrew, ”Very Deep ConvolutionalNetworks for Large-Scale Image Recognition.”, 2014, arXiv 1409.1556.

[17]. K. He, X. Zhang, S. Ren & J. Sun, ”Deep Residual Learning for ImageRecognition,” in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 2016, pp. 770-778.