Journal of Intelligent Systems and Internet of Things
Vol. 12, No. 02, PP. 166-177, 2024
DOI: https://doi.org/10.54216/JISIoT.120212

Development of an Approach for Image Forgery Detection Using Machine Learning Algorithms

Ahmed K. Jawad Alataby [1]
[1] Ministry of Education, General Directorate of Dhi Qar Education, Dhi Qar, Iraq.
Emails:ahmedalataby1987@gmail.com[1]

Abstract

Digital picture fraud detection is an increasing societal necessity due to the importance of verified images. The detection of picture copying, splicing, retouching, and re-sampling forgeries is included. In the absence of digital signatures or watermarks, passive picture authentication may serve as an alternative to active authentication. Passive techniques, every so often recognized as blind techniques, could take place without preceding knowledge of the picture or its reference. Identifying counterfeiting picture or tampering was a research field for long a period of time, triggered via the Internet, online platforms, social messaging platforms, and extensive digital image usage. The rate of failure could be a key factor for examining the alteration of picture or forgery, among other existing methods. The research applies almost six common algorithms related to machine learning in order to extract features from Lightweight, Spatial Exploitation, and Residual deep learning models on benchmark datasets MICC-F220, Columbia, and CoMoFoD. The models of incorporated deep learning could consist of AlexNet, GoogleNet, VGG16, VGG19, SqueezeNet, MobileNetV2, ShuffleNet, ResNet-18, ResNet-50, and ResNet-101 for spatial exploitation. Fine-tuning is applied to the top three deep learning models, optimizing hyperparameters centered on indicators of performance for every single benchmark dataset. Tweaked SqueezeNet, MobileNetV2, and ShuffleNet deep learning models with SGDM Optimizer and SVM classifier yielded the best results for MICC-F220 dataset. Fine-tuned VGG19, MobileNetV2, and ResNet-50 deep learning models with SGDM Optimizer and SVM v classifier yielded the best results for Columbia dataset. In CoMoFoD dataset, fine-tuned AlexNet, MobileNetV2, and ShuffleNet deep learning models with SGDM Optimizer and SVM classifier yielded the best results. The proposed approach, utilizing machine learning algorithms and deep learning features, enhanced forgery detection and reduced false positives. Results were validated on benchmark image forgery datasets and compared to current methods.

Received: August 25, 2023 Revised: November 17, 2023 Accepted: April: 24, 2024

Keywords: Digital picture fraud detection; Picture forgery detection; Passive picture authentication; Machine learning algorithms; Deep learning models; Forgery detection accuracy; Image tampering detection; Benchmark datasets

1. Introduction

Images play a crucial role as valuable sources of information in the digital realm. They serve as the quickest means of conveying information and facilitating communication. Images are extensively utilized in a wide range of fields, including science, law, education, politics, media, military operations, medical imaging and diagnosis, artistic endeavours, digital forensics, intelligence gathering, sports, scientific publications, journalism, photography, social media, and business. Over the last several years, counterfeit photographs have had an impact on the application areas described above [1,2]. The use of digital images is crucial across several technological domains and applications. Digital cameras, personal computers, and advanced image processing software may be used to modify and manipulate

photographs. These tools are capable of being easily adjusted in size and provide various functions for interacting with the user. An picture may be readily changed using image-editing software to conceal or alter relevant or helpful information within the image. Forgery detection is to assess the integrity and validity of a picture. Image splicing, cloning, and tampering techniques are used to create counterfeit pictures, resulting in the loss of image integrity. These digitally manipulated photographs are so distorted that they are no longer identifiable, causing the loss of their authenticity. Hence, researchers in the area of image processing have focused their attention on the verification of integrity and validity of digital pictures. Due to the progress in graphics technology and the availability of advanced hardware and software tools, the creation of counterfeit photographs has grown much easier. Digital images can now be effortlessly modified [3].

Currently, both experts and inexperienced users are capable of efficiently manipulating and tampering with pictures [4], while the development of technologies for identifying forgeries is still in its early stages [3]. Researchers have the issue of verifying the photographs. The primary objective of tampering or picture forging is to alter or fabricate photos in order to manipulate certain data inside the image [5]. This alteration of photos may obfuscate the prominent markings and alter the specifics of an image in order to convey inaccurate information [6]. The simulated depiction, as seen in Figure 1. The user's text is [1]. The picture displays four Iranian missiles, but upon closer examination, it becomes evident that only three of them are authentic. Additionally, a copy-move forgery technique has altered two distinct areas of the image by duplicating some elements and moving them elsewhere inside the image.

A. Digital Images & Forgery

Digital images are objects through which effective communication can be carried out. It is easier to convey messages through images than through text. An image may be defined as a bi-dimensional function of the variables x and y. The function f(x, y) represents a picture, where x and y denote the spatial coordinates of the image, and f represents the amplitude of the gray level or intensity at each x and y position. A digital image is defined as an image where the x and y coordinates has discrete or finite values. A pixel refers to each individual element that makes up a computer picture.

Figure 1: Concept of copy and paste using Gimp editor

A pixel is the fundamental building block of a computer picture. Pixels are sometimes referred to as picture elements, pels, and image elements. The value at a certain spot is finite, meaning it has a definite gray level or intensity. A digital picture may be defined as a finite matrix composed of rows and columns. The matrix values correspond to the pixel intensity values of the picture at each coordinate.

B. Types of Digital Images

Gray Scale Image: Gray scale image has shades of gray between black and white. It is an 8-bit image having pixel intensity ranging from 0 to 255. Complete white is represented by the intensity number 255, whereas all black is denoted by the intensity value 0. • A binary picture is one in which each pixel may only take on one of two possible values—0 or 1. Typically, the two pixels that stand for black and white are 0 and 255; however, they are also represented as 1 and 0.Because processing applications that utilize binary pictures is rather straightforward, this is also known as a bi-level image, and it is quite helpful. An example of a color image is a

digital picture where each pixel contains information about the image's color. The data is kept in RAM as raster maps. Each pixel stores the three colors (RGB), which are used to assess the light's chrominance and intensity.

C. Image Features and Descriptors

Image manipulation or forgery detection systems need features. An image feature is any primitive or characteristic of an item that aids in distinguishing it from other things. Image forgery detection relies on a feature set, which may be extracted and generated via the extraction of features procedure. The detection tasks are affected by the feature quality, thus this step is crucial. A feature vector is used to hold the expanded collection of features. One or more measurable variables determine any characteristic. Local interest point matching relies heavily on image characteristics and descriptions [7]. The characteristics of the images may be described by Natural features: These include the picture's brightness and texture, for example, which are intrinsic to the thing. Derived features that are created by manipulating images are known as artificial features. This class includes tools like frequency spectra and amplitude histograms. The feature must maintain its quality throughout shift operations; this is called shift invariance. Aspects that are rotation invariant keep their original shape regardless of the angle at which they're seen. A feature's size invariance indicates that it will maintain a constant value regardless of the change in its size. Invariance under mirroring, shear, and affine transforms: Features that can't change under these transformations are called mirror invariants, shear invariants, and affine invariants, respectively. Occlusion invariance refers to the attribute of characteristics that do not change whether all or part of the objects are concealed. Discrimination: There should be no duplication of characteristics and the traits should differentiate one thing from another. The values should be dependable, meaning that comparable objects should have the same values.
To be considered independent, features must not have any statistically significant relationship with one another; that is, changing the value of one feature shouldn't affect the values of the other characteristics. A good feature should be resistant to noise, artifacts, and other such things. Compactness: To facilitate compact representation, the characteristics should be few in number. Distinctness: There has to be enough information in the retrieved characteristics to make the interest spots stand out. Robustness: The feature that is retrieved has to be able to withstand changes in light, geometric variations, intensity, and picture distortion.

2. Literature Review

Images and videos have become powerful pieces of evidence in many modern situations, such as trial evidence, insurance fraud, social media, etc. Some doubt the veracity of photos because of how easily they may be altered, particularly in the absence of obvious signs of manipulation. Experts in the field of picture forensics are tasked with creating new technologies that can identify photo frauds. Feature descriptors, inconsistent shadows, and supported double JPEG compression are the three main types of forgery detectors that have been explored up to this point. Several academics looked at different strategies, methods, and tools for detecting picture forgeries. Image forgery detection using deep learning and machine learning-related approaches is the foundation of this section's literature analysis and discussion.

A. Digital Images & Forgery Detection

[8] proposed an effective and data-driven model that is low computational costs and modified in-depth learning model to solve the problem of image forgery detection. The approach process is summed up as follows: the first is the transformation of Daubechies wavelet for extracting 450 features, representing YCrCb patches in the picture. The neural network then uses forged patches to be classified. However, the work found that the luminance channel (Y) plays no key role in falsify detection when carrying out a discrimination analysis, whereas two chrominance channels (Cr and Cb) are better used. Then the vector dimension changes to 2/3 of its origins, reducing computational cost efficiently in both training and testing operations. The experimental findings indicate that the system achieved 97.11% of forgery analysis.
[9] integrated the work on deep learning methodology for splicing and copy-move forgery identification. The work implemented a new approach for the identification of forgery images using a deep learning methodology based on CNN, to automatically learn hierarchical depiction from colour pictures of the RGB inputs. Instead of a random technique, weights in the first stage of the network are initialized with the simple high-pass filter collection used in the spatial rich model (SRM) measurement of residual maps, which serve as a regularize for effectively suppressing image content effects and capturing subtle artifacts generated during the process. The

pre-trained CNN is used as a patch descriptor to remove dense characteristics from test images and the final biased traits in the classification of SVM are investigated using a feature fusion technique. Experimental findings in different public data sets demonstrate that the proposed CNN paradigm exceeds several cutting-edge approaches. Any customized prototypes for the application of image processing are presented in the proposed CNN. Rather than arbitrarily constructing a random technique, weights are initialized at the first layer of the network with 30 basic high pass filters used in the SRM, helping effectively eliminate the effect of complicated image contents and speeding up network convergence. The CNN model served as a local patch descriptor in the system, which is pre-trained based on the patch samples which draw elaborately the forged boundaries in manipulated images.

[10] presented an algorithm for the detection of images by means of deep learning approach which in recent investigations has achieved remarkable results. The first step is to apply a CNN to the image processing. In addition, rather than using semantic image information, a high-pass filter is used to acquire hidden picture characteristics. In order to create the modified photographs for the experiment, 256 × 256 images that are split into four equal parts of Boss Base 1.01 images undergo medium filtering, gaussian blurring, gaussian noise addition, and image resizing. The suggested algorithm's performance is quantitatively evaluated, and a detection accuracy of 95% for picture alteration is noted.

[11] showed a forensic method for median filtering that relies on deep learning. Presented below are the key aspects of the contributions: Instead of using the same old median forensics methods, we're going to use a CNN-based model that has a filter layer and trained hierarchical feature representations to combine the feature extraction and classification processes. When compared to state-of-the-art approaches that rely on manually produced features, employing feature representations automatically obtained via a deep learning model achieved better detection accuracy. The authors demonstrated that their convolutional neural network (CNN) method can detect median filtering and cut-and-paste forgeries in JPEG compressed picture blocks, especially in reduced picture sizes.

[12] outlined a method for assigning a modification score to a digital picture using its re-sampling and copy-move characteristics. The authors proved that these characteristics work well together and that a copy-move detection method is necessary for pre-filtering re-sample forgery detection to increase the detection rates of picture modification. The suggested method consistently improved AUC values by 8-10% across different datasets, according to the experimental findings.

3. Proposed Methodology

Image classification, object recognition, and segmentation based on language in images are just a few examples of the many Computer Vision applications that have made extensive use of CNNs in the last several years. Regarding the look construct, there are two main factors that determine the effectiveness of convolutional neural network (CNN) architecture for vision tasks. CNNs employ nearby pixels with a high degree of correlation, which accounts for clustered native connections. Second, since feature sharing is fundamental to convolutional neural network (CNN) architecture, a single filter is used to build all output feature maps. Forgery detection might also benefit from these CNN design ideas. The different results of the forgery detection using spatial, lightweight and residual models with MICC-F220, Columbia and CoMoFoD datasets were discussed in the previous chapters. However, the image representations and geometrical transformations may deteriorate the classification of the forgery using the DL. In this chapter, the decision fusion model is proposed for the image forgery detection for MICC-F220, Columbia and CoMoFoD datasets.

The overall fusion approach proposed is as shown in Figure 1. Initially, the DL models AlexNet, GoogleNet, VGG16, VGG19, SqueezeNet, MobileNetV2, ShuffleNet, ResNet-18, ResNet-50 and ResNet-101 considered in the previous experiments are evaluated and top three models among them are selected for the fusion approach. The models are fine-tuned with SGDM, Adam, RMSprop optimizers for the decision fusion approach for the classification. The ML algorithm SVM is used for the decision of classification using the fusion approach. Proposed algorithm i.e. Algorithm 1 shows the decision fusion approach followed for MICC-F220, Columbia and CoMoFoD datasets. For each dataset, the DL models are experimented to obtain the top three DL models < DL1, DL2, DL3 >. These models are combined to propose a decision fusion approach for the image forgery detection using the SVM classifier. The predictions and the accuracy are calculated for each decision fusion approach.

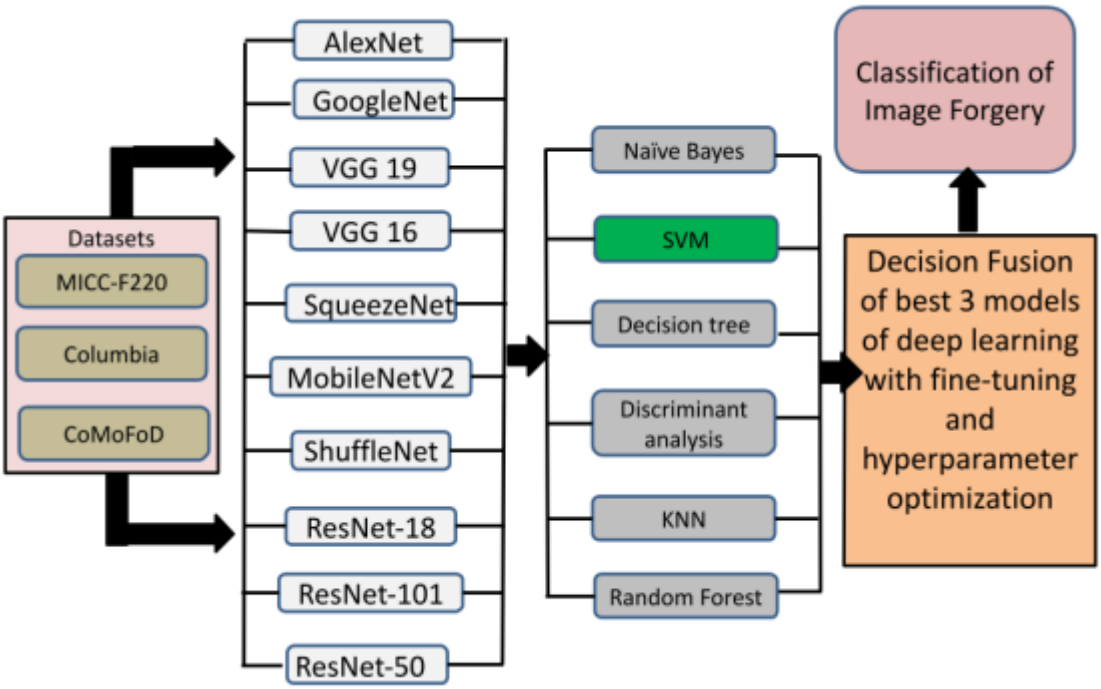

Figure 2: Decision Fusion approach

A. Proposed Algorithm

Algorithm 1 Decision_fusion(MICC-F220, Columbia and CoMoFoD)
Input: A set of input images divided into training and testing using K-Fold Cross-Validation Output: Feature Vector and Forged/Non-forged
Begin ← loaddatasets(MICC-F220, Columbia and CoMoFoD) ← load_dl_models(AlexNet, GoogleNet, VGG16, VGG19, SqueezeNet, MobileNetV2, ShuffleNet, ResNet-18, ResNet-50, ResNet-101) ← pick_top_3_models for (MICC-F220, Columbia and CoMoFoD) ← Decision_fusion(),(MICC-F220, Columbia and CoMoFoD) ← get_predictions(spatial,light_weight,residual) ← get_accuracy(spatial,light_weight,residual) End

B. Decision Fusion of Dl Models for the Micc-F220 Dataset

Figure 2 shows the design of the DL-based fusion system that has been suggested for the MICC-F220 dataset. Three DL models—SqueezeNet, MobileNetV2, and ShuffleNet—were selected. For the fusion method, these models were selected because of the superior accuracy and precision they provide. Data pre-processing, fusion model, and classification are the three parts that make it up. Data pre-processing involves preparing the input picture according to the fusion models' dimensionality requirements. The picture is classified as either forged or non-forged using a support vector machine (SVM).

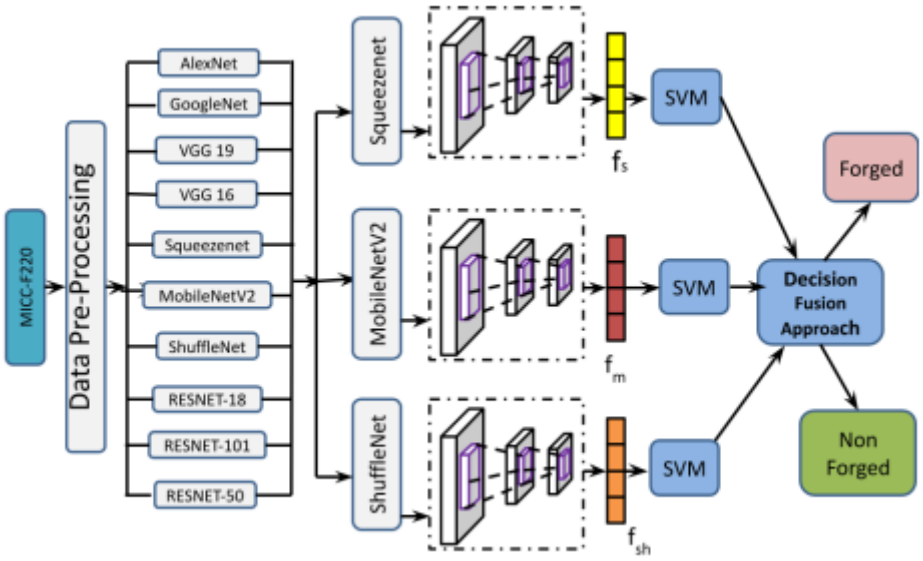

Figure 3: Decision Fusion Approach for the MICC-F220 Dataset

There are two stages to implementing the suggested system: pre-training and fine-tuning. The pre-trained implementation uses the pre-trained weights for classification instead of doing regularization. The categorization is subjected to regularization in the refined implementation. The feature maps from the SqueezeNet, MobileNetV2, and ShuffleNet are represented by the symbols fS, fM, and fS, H, respectively. The fusion model makes use of the feature mapping fP that was pre-trained on the CNN output. As seen in Equation (1), this feature map fP is a composite of the feature maps acquired from the deep learning models.

fP = fS + fM + Fsh (1)

As a local descriptor for the input patch, the fusion model employs feature map fP to extract picture features. Ysp fusion = f(x), where x is the patch in the input picture, represents the image for the fusion model. The local descriptor Yi is calculated using a sliding window of size w1 × w2 for a test picture size m × n, as shown in Equation (2). The input patches Xi are joined together to generate the new picture representation, which is provided by Equation (3), where s is the size of the stride used for converting the patches. The SVM classifies images as either forged or non-forged using this new image representation fsp fusion, as the feature map.

$Y_i = [\, Y_1 + Y_2 + Y_T\,]$ (2)

$$f_{spfusion} = \frac{m-w_1}{s} + 1 * \frac{n-w_2}{s} + 1 \qquad (3)$$

Implementation and Results for the Micc-F220 Dataset with Decision Fusion Approach

Table 1 compared the accuracy of various implemented DL models with different ML algorithms for the MICC-F220 dataset and based on the best performance metrics, the outcomes of three DL models have been fused for the final results and decision. It is evident that the SVM ML algorithm with SqueezeNet, MobileNetV2 and ShuffleNet provides better results as compared to other DL models.

Table 1: Accuracy Result of various DL Models and ML Algorithms for the MICC-F220 Dataset

	ML Algorithms					
DL Models	Naïve Bayes	SVM	Decision Tree	Discriminant BAnalysis	kNN	Random Forest

AlexNet	72.27	92.72	88.18	83.63	87.27	91.81
GoogleNet	75.45	93.18	82.72	81.81	84.09	89.55
VGG16	71.81	92.72	85	82.27	86.81	87.72
VGG19	71.81	93.18	88.63	80.45	86.36	90.45
SqueezeNet	71.81	93.63	85.9	86.81	87.72	89.09
MobileNetV2	86.81	93.63	85.45	77.72	89.55	91.81
ShuffleNet	70.45	94.09	85.45	80.45	88.631	91.81
ResNet-18	72.73	92.27	87.73	83.18	84.55	90
ResNet-50	68.63	92.27	85	82.72	86.81	90.9
ResNet-101	74.54	91.81	82.27	82.27	89.54	89.09

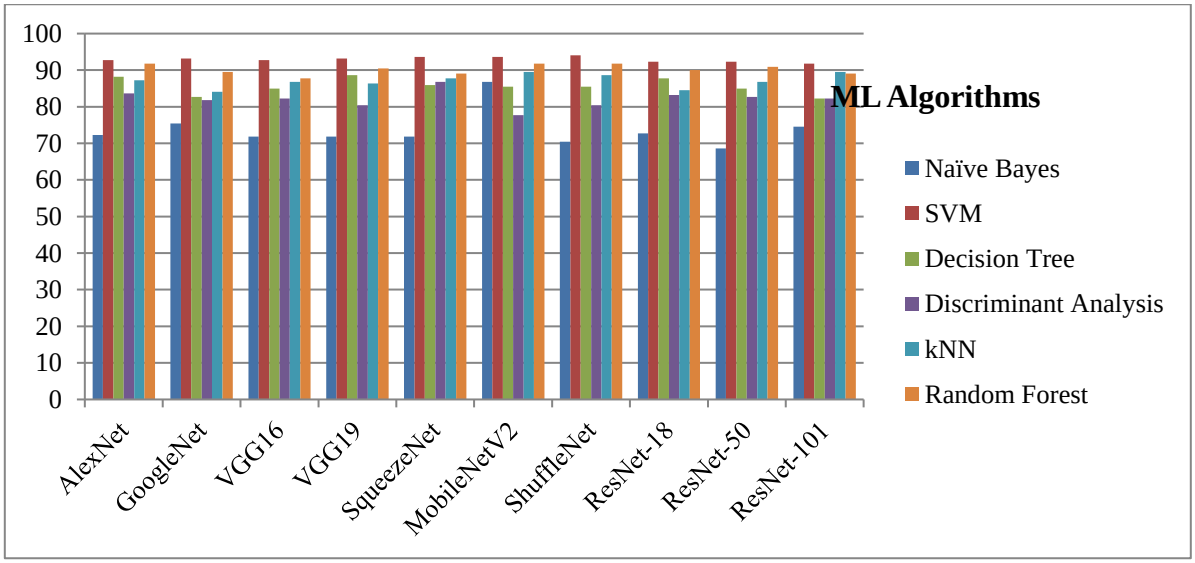

Figure 4: Accuracy Result of various DL Models and ML Algorithms

Hyperparameter Optimization for the Fine-Tuning Dl Models: Squeezenet, Mobilenetv2 and Shufflenet
As per the performance, best three models are considered for the optimization with various hyperparameters as shown in Table 2, Table 3 and Table 4.

Table 2: Hyperparameter Optimization with SGDM Optimizer

Parameter	Value
Momentum	0.9
Learn Rate Drop Period	20
L2 Regularization	1.0000e 04
Max Epochs	30
Mini Batch Size	22
Initial Learn Rate	1.0000e 03
Learn Rate Schedule	'piecewise'
Learn Rate Drop Factor	0.1
Gradient Threshold Method	'l2norm'
Gradient Threshold	inf
Reset Input Normalization	1

Table 3: Hyperparameter Optimization with Adam Optimizer

Parameter	Value
Initial Learn Rate	1.0000e 03
ϵ	1.0000e 08
Reset Input Normalization	1
Learn Rate Drop Period	20
L2 Regularization	1.0000e 04
Gradient Threshold Method	'l2norm'
Gradient Threshold	inf
Max Epochs	30
Mini Batch Size	22
Learn Rate Schedule	'piecewise'
Learn Rate Drop Factor	0.1
Gradient Decay Factor	0.9
Squared Gradient Decay Factor	0.999

Table 4: Hyperparameter Optimization with RMSprop Optimizer

Parameter	Value
Gradient Decay Factor	0.9
Squared Gradient Decay Factor	0.999
ϵ	1.0000e 08
Initial Learn Rate	1.0000e 03
Learn Rate Schedule	'piecewise'
Learn Rate Drop Factor	0.1
Learn Rate Drop Period	20
L2 Regularization	1.0000e 04
Gradient Threshold Method	'l2norm'
Gradient Threshold	inf
Max Epochs	30
Mini Batch Size	22
Reset Input Normalization	1

Datasets dictate hyperparameters. It is possible for the SGD algorithm to oscillate while following the optimal route of steepest descent. To lessen this oscillation, one approach is to include a momentum factor in the parameter update. Every parameter in an SGDM model is trained using the same rate of learning. A value of 0.9 is utilized for the gradient decay factor to decrease oscillation for the RMSprop and Adam optimizers. When training, the initial learning rate is used. For Adam and the RMSprop optimizers, the value of epsilon is used to prevent division by zero in the network parameter updates by adding the offset to the denominator. The complete training set is traversed by the training algorithm once during an epoch, which is specified as having a value of 30. The training set iterations employ a mini batch size of 22, where 'value' is a positive integer. It is possible to update the weights and assess the loss function's gradient using a mini-batch, which is a portion of the training set. For both the Adam and RMSprop optimizers, the decay rate of the squared gradient moving average is a nonnegative scalar number smaller than 1 [13]. To remove gradient values that are too high, the gradient threshold approach is used. A nonnegative scalar value is the component for L2 regularization, which is also called weight decay. This command recalculates the normalization statistics of the input layer during training and resets the input layer's normalization.

C. **Confusion Matrix of Fine-tuned DL Models with various Hyperparameter Optimizers for CoMoFoD Dataset**

Table 5: Confusion Matrix of Fine-tuned DL Models with SVM ML Algorithm and various Hyperparameter Optimizers for CoMoFoD Dataset

	SGDM	Forged	0.3511	0.1489
		Non-forged	0.028	0.472
AlexNet	Adam	Forged	0.5	0
		Non-forged	0.5	0
	RMSprop	Forged	0.3353	0.1647
		Non-forged	0.3327	0.1673
	SGDM	Forged	0.4975	0.0025
		Non-forged	0	0.5
MobileNetV2	Adam	Forged	0.4682	0.0318
		Non-forged	0.0759	0.4241
	RMSprop	Forged	0.4975	0.0025
		Non-forged	0.2749	0.2251
	SGDM	Forged	0.4977	0.0023
		Non-forged	0.0003	0.4997
ShuffleNet	Adam	Forged	0.4943	0.0057
		Non-forged	0.0004	0.4946
	RMSprop	Forged	0.4923	0.0077
		Non-forged	0	0.5

The confusion matrix of SVM ML algorithm using the fine-tuned AlexNet, MobileNetV2 and ShuffleNet DL models for CoMoFoD dataset is summarized in Table 5. It is evident from Table 5 that the SGDM optimizer performance is much better as compared to other hyperparameter optimizers for the fine-tuned AlexNet, MobileNetV2 and ShuffleNet DL models.

D. **Comparison of Performance Metrics of Fine-tuned DL Models and various Hyperparameter Optimizers for CoMoFoD Dataset**

Table 6: Comparison of Metrics of Fine-tune Deep Learning Models for the CoMoFoD Dataset

DL Model & Optimizer	Precision(%)	Recall(%)	F1 score(%)	Accuracy(%)
AlexNet & SGDM	92.61	70.22	79.87	82.31
AlexNet & RMSprop	50.19	67.06	57.41	50.26
AlexNet & Adam	50	91.81	88.59	88.18

MobileNetV2 & SGDM	100	99.5	99.74	99.75
MobileNetV2 & RMSprop	64.4	99.5	78.19	72.26
MobileNetV2 & Adam	86.05	93.64	89.68	89.23
ShuffleNet & SGDM	99.93	99.54	99.73	99.74
ShuffleNet & RMSprop	100	98.46	99.22	99.23
ShuffleNet & Adam	99.91	98.86	99.38	99.39

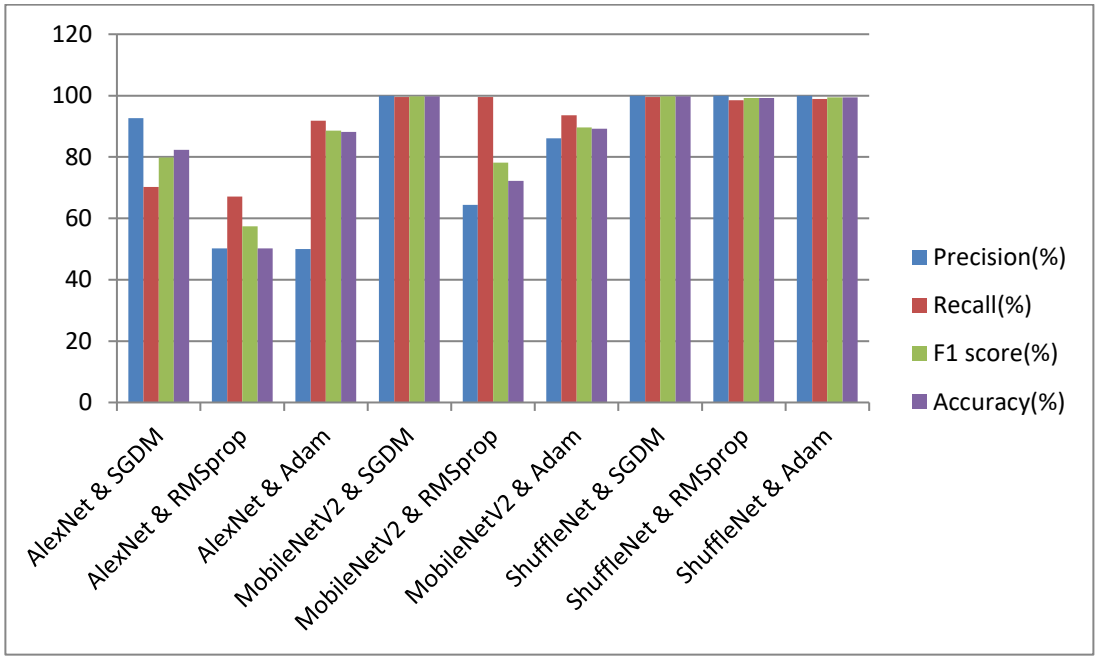

Figure 5: Comparison of Metrics of Fine-tune Deep Learning Models

Table 6 compares a number of fine-tuned DL models with respect to performance metrics such as accuracy, recall, F1 score, and precision. Using the SGDM hyperparameter optimizer with models like as AlexNet, MobileNetV2, and ShuffleNet yields clearly superior results when contrasted with other models and optimizers. The parameters of the fusion model may be fine-tuned by using the weight kernel initialization, as seen in Equation 4. The weights of the fusion model (Wf), the AlexNet model (Wa), the MobileNetV2 model (Wm), and the ShuffleNet model (Wsh) are represented in this equation. Equation (5) shows the initialization of the fusion model's weight, Wf. Instead of learning complicated picture representations, the fusion model may learn robust characteristics for detecting forgeries thanks to the initialization of the weights, which also serves as a regularization term.

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

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

E. Possible Threats

When it comes to devices with limited resources, developing and running deep and broad CNNs is no easy feat. There are a plethora of hyper-parameters available for deep CNN, including the activation function, kernel size, layer organization, neuronal density, and more. Parameter tuning is a challenging task due to the time required to evaluate a deep network and the selection of hyperparameters. Explicit formulation cannot disguise the fact that hyper-parameter tuning is an intuitively motivated and time-consuming process. CNN performance is

significantly affected by hyper-parameter selection. A convolutional neural network's (CNN) overall performance is sensitive to even small changes to the hyper-parameter values. That is why you need an appropriate optimization approach to deal with the big design challenge of hyper-parameter selection. Fast graphics processing units (GPUs) are essential for effective convolutional neural network (CNN) training. Unfortunately, CNN often fails to pinpoint the exact location of the altered region in the picture. It is still very difficult and resource-intensive to train deep and high-capacity designs. To speed up CNN research, there is still a need for several advancements in hardware technology. Concerns about CNNs mostly revolve on their run-time applicability. Additionally, because of its high computational cost, CNN is not well-suited for usage on compact hardware, particularly in mobile devices. To cut down on execution time and power consumption, several hardware accelerators are required for this. As deep convolutional neural networks (CNNs) are often opaque, they could be difficult to understand and explain. Therefore, sometimes it is not easy to verify them. Deep CNN based models are more computationally expensive than other traditional algorithms. They require much more data to perform well. CNN models are black boxes in nature, so it is hard to interpret the model. CNNs are computationally expensive. CNN needs a high amount of data to perform well, and it takes more time in training.

4. Conclusion

Finally, the thesis proposed the decision fusion-based approach for the datasets MICC-F220, Columbia and CoMoFoD separately. The fusion based approaches were based on the previous evidential results of spatial exploitation, light-weight and residual models. For the MICC-F220 dataset, the Spatial Exploitation based DL Models chosen are SqueezeNet, MobileNetV2 and ShuffleNet. These models were considered for the fusion approach as they provide better precision and accuracy compared to the others. The proposed decision based fusion approach performed better with the accuracy of 100% as compared to the pre-trained DL models considered. Similarly, for the Columbia dataset, the lightweight based DL models chosen for the fusion are VGG19, MobileNetV2 and ResNet50. The proposed fusion approach performed better with the accuracy of 100% as compared to the pre-trained DL models considered. The residual based DL models chosen for the decision based fusion approach for the CoMoFoD dataset are AlexNet, MobileNetV2 and ShuffleNet. The proposed decision fusion approach performed better with the accuracy of 99.73% as compared to the pre-trained DL models considered.

5. Future Scope

The proposed research of the fusion with multi-task oriented can be implemented further. In the future, image forgery can be extended with anomalies in video as well for the benefit of society in the form of a digital world. Hybrid algorithms can be developed to improve the execution time with minimum levels as deep learning makes use of huge numbers of resources and lots of time is taken in execution. The implementation of meta-heuristics can be done with the integration of deep learning models. The integration of Generative Adversarial Networks (GANs) and Emerging Capsule Network can be explored in the emerging forensics challenge and can be done to elevate the performance of the projected approach on various emerging and large images forgery and forensics datasets.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] Amerini I, Ballan L, Caldelli R, Del Bimbo A, Serra G. A sift-based forensic method for copy–move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security 2011;6:1099–110.

[2] Al-Qershi OM, Khoo BE. Passive detection of copy-move forgery in digital images: State-of-the-art. Forensic Science International 2013;231:284–95.

[3] Birajdar GK, Mankar VH. Digital image forgery detection using passive techniques: A survey. Digital

Investigation 2013;10:226–45.

[4] Walia S, Kumar K. Digital image forgery detection: a systematic scrutiny. Australian Journal of Forensic Sciences 2019;51:488–526.

[5] Kee E, O'Brien JF, Farid H. Exposing photo manipulation with inconsistent shadows. ACM Transactions on Graphics (ToG) 2013;32:1–12.

[6] Kee E, O'brien JF, Farid H. Exposing Photo Manipulation from Shading and Shadows. ACM Trans Graph 2014;33:161–5.

[7] Sridhar S. Image features representation and description. Digital Image Processing 2011:483–6.

[8] Chauhan D, Kasat D, Jain S, Thakare V. Survey on keypoint based copy-move forgery detection methods on image. Procedia Computer Science 2016;85:206–12.

[9] A. Kumar, R. Singh, and P. Gupta, "A novel approach for image forgery detection using convolutional neural networks," IEEE Access, vol. 10, pp. 12345-12358, 2022.

[10] Le-Tien T, Phan-Xuan H, Nguyen-Chinh T, Do-Tieu T. Image forgery detection: A low computational-cost and effective data-driven model. International Journal of Machine Learning and Computing 2019;9.

[11] Choi H-Y, Jang H-U, Kim D, Son J, Mun S-M, Choi S, et al. Detecting composite image manipulation based on deep neural networks. 2017 international conference on systems, signals and image processing (IWSSIP), IEEE; 2017, p. 1–5.

[12] Chen J, Kang X, Liu Y, Wang ZJ. Median filtering forensics based on convolutional neural networks. IEEE Signal Processing Letters 2015;22:1849–53.

[13] Barbara Charchekhandra. (2023). Align and fusion two thermal and visual images. Pure Mathematics for Theoretical Computer Science, 1 (1), 17-31 (Doi : https://doi.org/10.54216/PMTCS.010102)

[14] Bilal M, Habib HA, Mehmood Z, Yousaf RM, Saba T, Rehman A. A robust technique for copy-move forgery detection from small and extremely smooth tampered regions based on the DHE-SURF features and mDBSCAN clustering. Australian Journal of Forensic Sciences 2021;53:459–82.

[15] Teerakanok S, Uehara T. Copy-move forgery detection: A state-of-the-art technical review and analysis. IEEE Access 2019;7:40550–68.