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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124148

Image Forgery Detection based on Fusion of Lightweight Deep Learning Models

Mrs. SVTSAV Ramya[1], Sai Chetan Panathukula[2], Keshav Kamtam[3], Gujjar Sai Praharshith[4]

Assistant Professor, Department of Information Technology, Matrusri Engineering College, Hyderabad, India[1]

Student, Department of Information Technology, Matrusri Engineering College, Hyderabad, India[2-4]

Abstract: The popularity of capturing images has increased in recent years, as images contain a wealth of information that is essential to our daily lives. Although various tools are available to improve image quality, they are often used to falsify images, leading to the spread of misinformation. This has resulted in a significant increase in image forgeries, which is now a major concern.

To address this, a decision fusion method is proposed in this project, which uses lightweight deep learning-based models for detecting image forgery. The proposed approach involves two phases that utilize pretrained and fine-tuned models, including SqueezeNet, MobileNetV2, and ShuffleNet, to extract features from images and detect image forgery. In the first phase, lightweight models are used to extract features from images without regularization, while in the second phase, fine-tuned models with fusion and regularization are employed to detect image forgery.

Keywords: Image Forgery, Deep Learning, Lightweight models, Convolutional Neural Networks (CNN)

I. INTRODUCTION

Images and videos are widely used as evidence in various contexts, including trials, insurance fraud, and social media. However, the easy accessibility of digital editing tools has given rise to questions about the authenticity of images. [1]Image forensics authorities aim to develop technological innovations to detect image forgeries, which can be classified into copy-move and splicing categories. [2]Various image forgery detection techniques have been proposed over the years, including those that exploit the artifacts left by multiple JPEG compression and camera-based methods. Detecting forged images is essential as they can mislead people and threaten individuals' lives. Previous studies have attempted to identify copy-paste or splicing of forged areas in images by extracting various properties such as lighting, shadows, sensor noise, and camera reflections [3].Several researchers [4-9] have assessed the credibility of images by determining whether they are authentic or forged. There are currently numerous techniques [7-15] available for identifying forged regions in images that rely on detecting artifacts left by multiple JPEG compressions and other image manipulation techniques. Camera-based methods [16] have also been explored, where detection is based on demosaicing regularity or sensor pattern noise. The irregularities in the sensor pattern are extracted and compared for anomalies [17].

Using lightweight models is motivated by the need to prevent overfitting of convolutional neural network (CNN) architectures, as well as their ability to be easily deployed on resource-constrained hardware and learn enriched representations.[19-23] ShuffleNet [24] is particularly efficient as it generates more feature map channels for a given computation complexity budget, which encodes more information and is crucial for the effectiveness of small networks. MobileNet [21] utilizes deep-separable convolutions and has achieved state-of-the-art results, demonstrating its effectiveness across a wide range of tasks. SqueezeNet, [25] on the other hand, is optimized for fast processing speed in CNN systems with significantly fewer parameters than AlexNet, while maintaining standard accuracy. The utilization of lightweight models not only enables effective deployment on resource-restricted hardware but also helps in learning enriched representations.

This paper proposes a decision fusion method that uses lightweight deep learning models for detecting image forgery. The method consists of two phases: feature extraction from images using SqueezeNet, [25] MobileNetV2, [22] and ShuffleNet [24] without regularization in the first phase, and detection of image forgery using fine-tuned models with fusion and regularization in the second phase. The main contributions of this paper include the proposed decision fusion-based system using lightweight models for image forgery detection, the two-phase implementation of the fusion system using pretrained and fine-tuned weights, and the reduction of false matches, false positive rate, and ultimately increasing the accuracy of the approach due to the utilization of lightweight models.

DOI: 10.17148/IJARCCE.2023.124148

II. LITERATURE SURVEY

Amerini et al. made progress in identifying and pinpointing single or double JPEG compression through the use of convolutional neural networks (CNNs). They tested different types of input for the CNN and conducted experiments to uncover any potential problems that require further study.

Xiao et al. developed a method for detecting splicing forgery using two components: a coarse-to-refined convolutional neural network (C2RNet) and diluted adaptive clustering. C2RNet involves two convolutional neural networks (C-CNN and R-CNN) that analyze image patches of different scales to identify differences in image properties between tampered and un-tampered regions. To reduce computational complexity, an image-level CNN replaces patch-level CNN in C2RNet, enabling the method to learn differences in various image properties for stable detection performance while reducing computational time.

Zhang et al. conducted a study on two stages. In the first stage, they used a Stacked Autoencoder model to learn complex features for each patch. In the second stage, they integrated contextual information for each patch to improve detection accuracy.

Goh et al. proposed a hybrid evolutionary framework for performing a quantitative study to assess all features involved in image tampering in order to identify the best feature set. Following the evaluation and selection of features, the classification mechanism is optimized for improved performance. The hybrid framework can also determine the optimal multiple classifier ensembles for the best classification performance in terms of accuracy and low complexity for detecting image tampering.

Change et al. proposed a new algorithm to detect tampered inpainting images, consisting of two stages: suspicious region detection and forged region identification. The method searches for similar blocks in the image and uses a similarity vector field to eliminate false positives. It identifies forged regions using the multi-region relation (MRR) method and can identify tampered areas even in images with uniform backgrounds. The algorithm's computational speed is improved by a two-stage searching algorithm based on weight transformation.

Lamba et al. developed a method for identifying duplicated regions in an image using discrete fractional wavelet transform. The approach involves dividing the image into fixed-sized overlapping blocks and applying the transform to each block to extract features. The feature vectors are then arranged in a lexicographical order and subjected to block matching and filtering to identify any replicated blocks. The method is capable of detecting both single and multiple duplicated regions in an image.

Lin et al. developed a method to detect tampered images by analyzing the double quantization effect in the discrete cosine transform (DCT) coefficients. This approach has several advantages, including the ability to locate the tampered region automatically, fine-grained detection, insensitivity to different types of forgery methods, ability to work without fully decompressing JPEG images, and fast speed. The experimental results on JPEG images are promising.

III. PROPOSED SYSTEM

The proposed decision fusion architecture utilizes lightweight deep learning models, including SqueezeNet, MobileNetV2, and ShuffleNet, implemented in two phases: pre-trained and fine-tuned. In the pre-trained model implementation, pre-trained weights are used without regularization, whereas regularization is applied in the fine-tuned implementation to detect image forgery.

The system consists of three stages: data pre-processing, classification using SVM, and fusion. The image in the query is pre-processed based on the required dimensions of the deep learning models. The paragraph explains the use of deep learning models and the implementation strategy for regularization to identify image forgery.

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124148

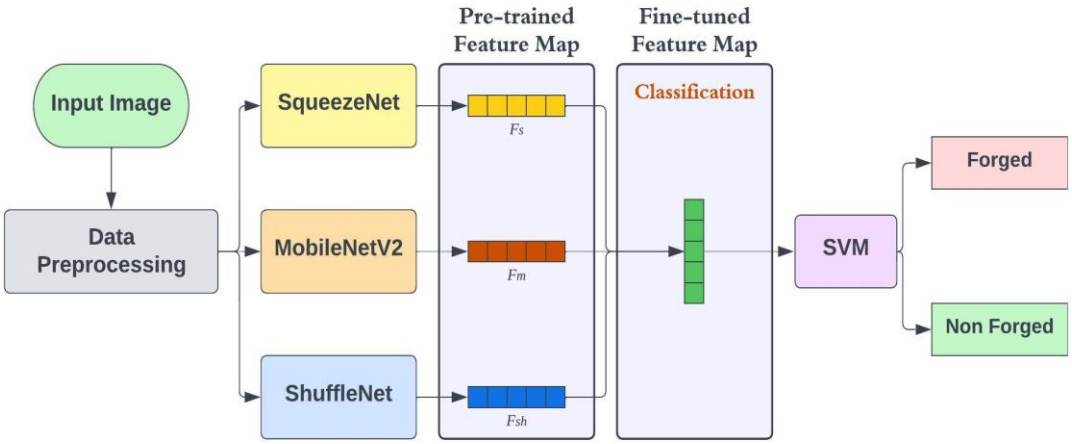

Fig. 1 Fusion based decision model for Forgery Detection

Data Preprocessing:

The first stage of the forgery detection process involves pre-processing the query image to determine if it is authentic or fake. The dimensions of the input image are adjusted to meet the requirements of the specific model being used (227x227 for SqueezeNet, 224x224 for MobileNetV2 and ShuffleNet). The image is then pre-processed based on the required dimensions before being passed to each model, which generates a feature vector in subsequent stages.

Lightweight Deep Learning Models:

The Several lightweight deep learning models, including SqueezeNet [25], MobileNetV2 [21], and ShuffleNet [24], have been evaluated for image classification fusion. These models have been widely used for image classification, and in this section, they are briefly discussed. A summary of the models, including their depth, parameters, and required image input size, is presented in Table 1.

TABLE I PARAMETERS OF LIGHTWEIGHT DEEP LEARNING MODELS

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

Classifier:

The proposed approach uses SVM as a classifier, which is known for its popularity and efficiency in binary classification. The performance of the approach is evaluated at the image level using various performance metrics, such as precision, recall (TPR), false positive rate (FPR), F-score, and accuracy.

Fusion and Regularization:

The proposed system uses lightweight deep learning models with pretrained weights for image forgery detection. The system is implemented as a fusion of the decision of these models. The input image is first passed to the lightweight models to obtain their respective feature maps. The feature maps from SqueezeNet, MobileNetV2, and ShuffleNet are denoted as f_s, f_m, and f_{sh}, respectively. The output feature map from the pretrained lightweight deep learning model is used for the fusion model, which is a combination of the feature maps obtained from the lightweight models. This feature map, denoted as f_p, is obtained using Equation (1).

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

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124148

Design Flow:

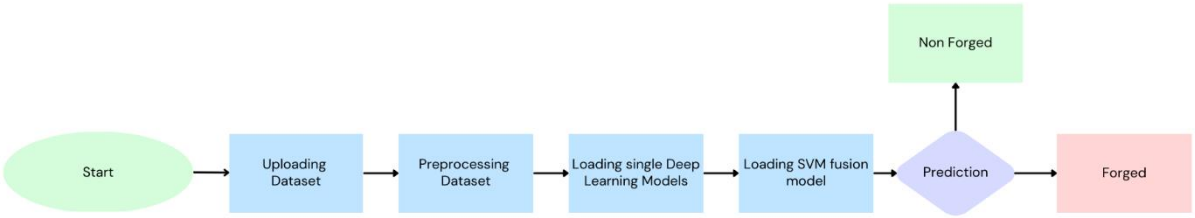

Fig. 2 Design flow

IV. IMPLEMENTATION

Baseline Modules:

This system comprises several modules aimed at optimizing the performance of image classification algorithms. The first module enables the upload of the MICC-F220 dataset to the application. The dataset is pre-processed in the second module, which involves reading all the images, normalizing their pixel values, and resizing them to a consistent size. The third module involves training three algorithms - SqueezeNet, MobileNetV2, and ShuffleNet - and extracting features from them to train the fusion model. The prediction accuracy of all three algorithms is evaluated on test data. In the fourth module, features are extracted from all three algorithms to create a fusion model, which is then trained with SVM to improve accuracy. The fifth module involves extracting SIFT features from the images using the existing technique, training them with SVM, and evaluating prediction accuracy. The sixth module plots the accuracy graph for all the algorithms, while the seventh module displays the performance table for all the algorithms. Overall, these modules work together to enhance the accuracy of image classification algorithms and make them more effective for practical applications.

Dataset:

The study employed the publicly available MICC-F220 dataset, which consists of 110 nonforged and 110 forged images in color format with 3 channels and dimensions ranging from 722 × 480 to 800 × 600 pixels. Figure 7.1 displays the images, with Figures 2a-2j representing forged images manipulated using 10 different combinations of geometrical and transformational attacks, and Figure 2k representing a nonforged image. The researchers randomly selected 154 images from the dataset for training and reserved the remaining images for testing.

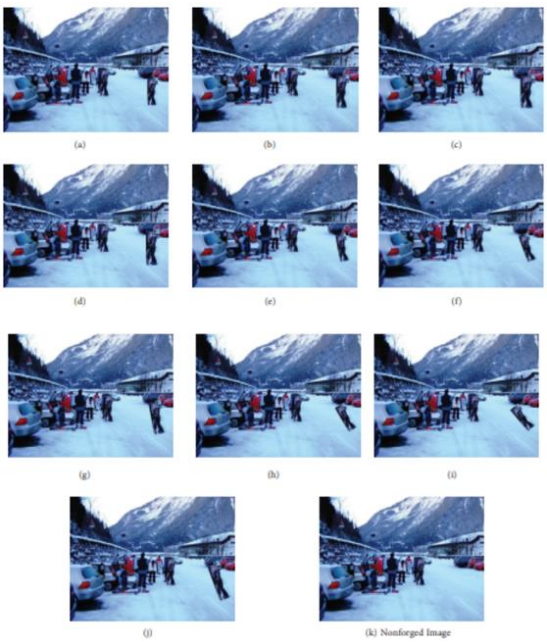

Fig. 3 Dataset with 10 different combinations of geometrical and transformation attacks; (a–j), forged; (k), nonforged images.

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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124148

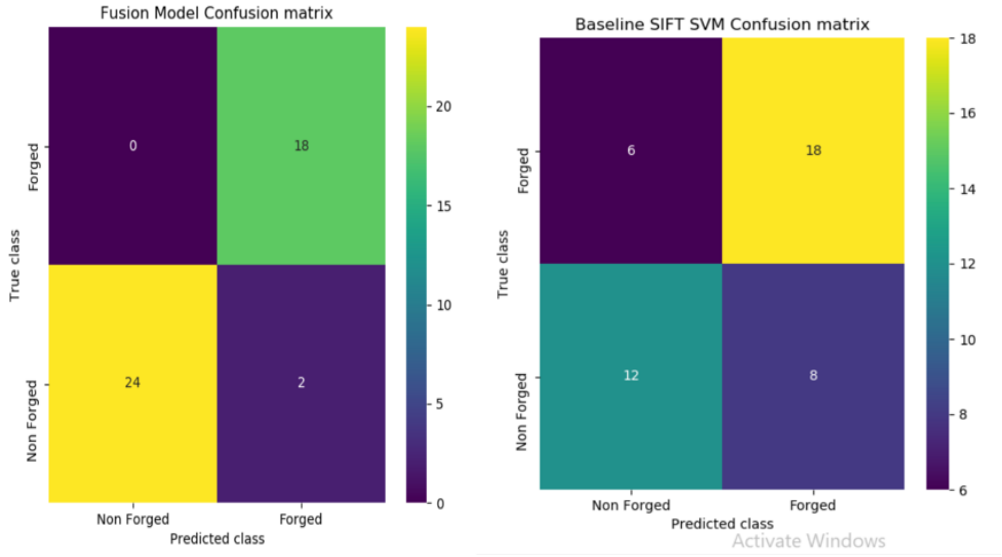

Fig. 4 Confusion matrixes of fusion model and baseline SIFT SVM.

TABLE 2 PERFORMANCE COMPARISION

Method	Accuracy	Precision	Recall	F Score
Existing SFIT 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
Only MobileNetV2	81.8	82.9	81.8	81.6
Proposed Fusion Model SVM	95.4	95	96.1	95.3

V. CONCLUSION

Image forgery detection helps to differentiate between the original and the manipulated or fake images. In this paper, 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

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 4, April 2023

DOI: 10.17148/IJARCCE.2023.124148

[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. 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.