



Image Splicing Detection Using Depth-Wise Convolution Neural Network

Mohammed S. Khazaal^{1,2*}, Mohamed Elleuch³, Monji Kherallah⁴, Faiza Charfi⁴

¹ National School of Electronics and Telecoms of Sfax, University of Sfax, Sfax 3018, Tunisia

² Engineering College, Al-Nahrain University, Baghdad 10072, Iraq

³ National School of Computer Science (ENSI), University of Manouba, Manouba 2010, Tunisia

⁴ Faculty of Sciences of Sfax, University of Sfax, Sfax 3000, Tunisia

Corresponding Author Email: mohammed.saeb@nahrainuniv.edu.iq

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijcmem.120401>

ABSTRACT

Received: 25 July 2024

Revised: 9 September 2024

Accepted: 19 September 2024

Available online: 27 December 2024

Keywords:

image splicing, deep learning, CNN, CASIA v1.0, CASIA v2.0, DWCNN, HSV color space

Images play a pivotal role in documenting real-life events. With the rapid evolution of digital technology, there has been a significant increase in both the creation and dissemination of photographs. The accessibility of picture editing software has simplified the process of altering images, thereby reducing the time, costs, and expertise needed to create and manage visually manipulated content. Unfortunately, digitally altered photographs have become a primary medium for disseminating misinformation, which affects individuals and society at large. Consequently, the need for effective methods to detect and identify forgeries is more pressing than ever. One prevalent form of picture fraud, image splicing, has been thoroughly examined. In this study, we present a Depth-Wise Convolutional Neural Network (DWCNN) model specifically designed to accurately detect spliced forged images. By converting input RGB images to the HSV color space, known for its ability to withstand color and lighting variations, our model achieves high accuracy in identifying manipulated images. Furthermore, our proposed model is lightweight, based on the MobileNet architecture with seven bottleneck blocks, making it suitable for a wide range of scenarios with constrained resources. To evaluate the model's performance, we tested it on the CASIA v1.0 and CASIA v2.0 datasets. Our model accurately identified forgeries with 99.23% accuracy on the CASIA v1.0 dataset and achieved a remarkable accuracy of 99.37% on the CASIA v2.0 dataset.

1. INTRODUCTION

Every day, millions of digital files, including photos, movies, and audio recordings, are published to social networks. This highlights the significant role that digital media plays in modern communication. However, as image editing technologies continue to advance, the ease of image manipulation has increased, enabling the creation of sophisticated and convincing forgeries. Unfortunately, with the widespread availability of advanced image-editing software, it has become increasingly challenging for users to manually detect modified photos [1]. A new field of image processing called 'digital image forensics' seeks to verify the authenticity and source of a digital image. One of the most crucial obligations in picture forensics is figuring out photo alteration. Digital tampering calls for expertise of image homes in addition to expertise in picture enhancing.

Image tampering occurs for diverse reasons, including the introduction of bogus evidence or the delight of digital works [2]. Detecting such manipulations normally entails two principal processes referred to as passive and lively methods. Passive strategies involve studying intrinsic features of the photograph, along with visual artifacts and inconsistencies, without changing the picture. These features consist of

versions in brightness, texture discontinuities, and irregularities in excellent information, which can suggest regions of the image which have been spliced. Active techniques, alternatively, contain embedding markers or auxiliary statistics into the photograph at some stage in its creation or transmission. These markers can be virtual signatures, QR codes, invisible watermarks, or other statistics that identifies the photograph's foundation or manipulation. During next evaluation, those markers may be detected to confirm the image's authenticity and become aware of any spliced areas [3]. Figure 1 illustrates the 2 categories of digital photo forensics.

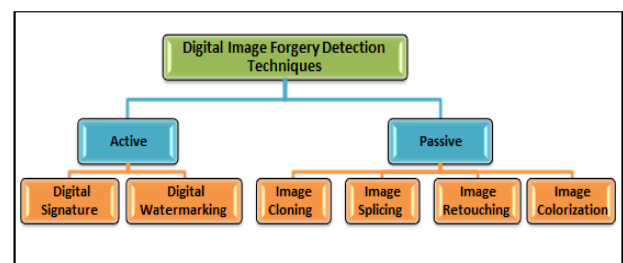


Figure 1. Image forgery techniques [2]

In this study, we explicitly address the detection of splicing forgery in images. Splicing occurs when a section of one image is copied and placed onto another. Therefore, creating a spliced image involves using at least two images. If the merged images have contrasting backgrounds, it becomes very difficult to make the borders and boundaries seamless. Digital photomontages are often created by merging two images together using software such like Adobe Photoshop and others. Figure 2 illustrates an example of an image splicing operation [3].

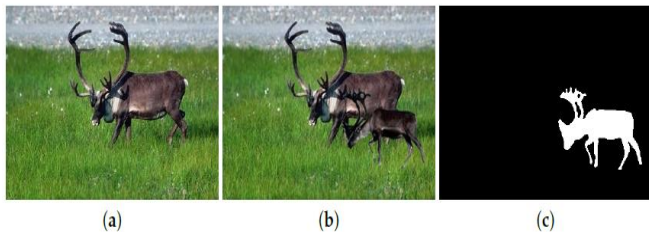


Figure 2. Image splicing example, (a) host image, (b) forgery image, (c) ground-truth

Image splicing is a critical issue because it facilitates the creation of misleading and deceptive visuals that can spread misinformation, erode public trust, manipulate opinion, and damage reputations. It poses significant ethical, legal, and privacy challenges, with spliced images being used for propaganda, defamation, and fraud. The manipulation of images can distort reality, influencing political outcomes, and public perceptions, and can compromise the integrity of legal evidence. As detection techniques struggle to keep up with sophisticated manipulations, the potential for harm in sectors like media, law, and personal privacy continues to grow.

Many approaches have been proposed to address the splicing forgery problem. These approaches can be categorized into two main categories: Deep Learning (DL) and hand-crafted techniques. Hand-crafted algorithms, based on classical Machine Learning (ML), aim to differentiate between genuine and spliced photos by relying on specific characteristics that highlight differences between unaltered portions and tampered areas. However, the gesture has limitations and is not always representative. Because of its ability to efficiently extract image features, Deep Learning algorithms analyze images end-to-end, producing better results in image fusion recognition [4] especially Convolution Neural Networks (CNNs) a based on local and semantic invariance in computer vision processing such as semantic segmentation and object classification]. This has been very successful and has led to the development of many CNN-based splicing detection methods that outperform more established methods [5]. One of CNN’s most popular models is MobileNet. The main idea of MobileNetV1 is to replace conventional diffraction with depth-wise (DW) separable diffraction [6]. This is achieved by dividing regular diffraction into two types, depthwise and pointwise diffraction used for filtering and linear combinations, respectively MobileNetV1 consists of two layers: a depth-wise (DW) convolution layer for light filtering, a convolution filter is applied for each input channel of a 1×1 convolution (or point-wise) layer input channel construction [6]. However, MobileNetV2 consists of two blocks: a residual block with stride 1, and another block without residual connections and strides 2 on a depth-wise 3×3 convolutional layer [7]. Each of these blocks is made up of three layers: 1×1 convolution layer with a rectified linear unit

(ReLU6), a depth-wise convolution layer with ReLU6, and another 1×1 convolution layer with no non-linearity. Figure 3 depicts the architectures of MobileNet V1 and V2.

In this work, we propose a new pattern recognition algorithm for image interpolation. Our contributions in this area include developing a custom architecture model specifically designed to detect and detect image splicing forgeries, using the power of DWCNN To ensure the robustness and accuracy of our model we use two datasets largely uses CASIA v1.0 and CASIA v2.0 [8] and available. We use these two, which enables a thorough and accurate test under different circumstances Furthermore, we evaluate the performance of our proposed model using several alternative methods, and show how effective and superior in merged image recognition.

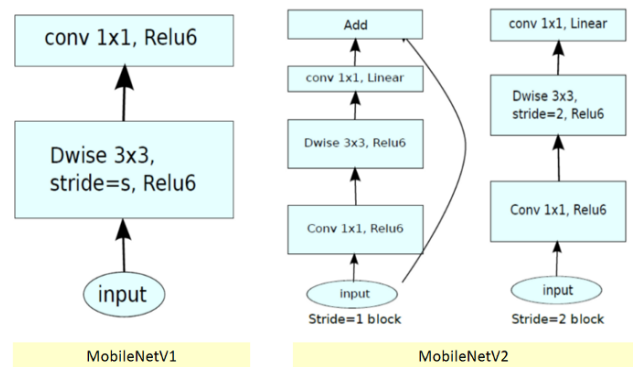


Figure 3. MobileNet architecture [7]

This paper is organized as follows: Section 2 provides a detailed description of the methods used to analyze images. and presents the methods for rendering image grids. In Section 3 we provide an overview of previous related work. Section 4 presents our proposed image splicing detection scheme. The experimental results and discussion are presented in Section 5. Finally, Section 6 presents the conclusion of this work.

2. TECHNIQUES FOR ANALYSING And IDENTIFYING IMAGE FORGERY

Digital picture forensics can be categorized into two main categories [3-5]:

A) Authentication and integrity analysis:

This class focuses on verifying the authenticity and authenticity of digital images. The methods under this category aim to determine if an image has been altered, processed, or updated. The most common methods used in this regard are as follows:

- Metadata analytics: widely used to provide valuable information about the origin and history of an image, including information such as the recording device, time stamp and location information.
- Error level analysis: typically used to identify potential areas of variation by analysing compression artefacts and changes in error rates in an image.
- Pixel-based analysis: A commonly used method that involves analysing individual pixels or groups of pixels to detect irregular changes, allowing detailed analysis of the image at the pixel level.
- Watermark Identification: Usually used to identify visible or hidden watermarks to trace the source of the image,

especially in cases where the authenticity of the image needs to be determined.

B) Content analysis and source identification:

This phase involves analyzing features in digital images and identifying their sources in order to extract information from them. The methods under this category aim to reveal details about the image itself, such as the objects, people, or events depicted, and the context in which they were taken, and they are methods commonly used in this case:

- Feature recognition: The use of computer vision techniques and Machine Learning algorithms to identify features, faces, or features that stand out in an image.
- Contextual analysis: analyzing environmental, visual, and other contextual factors to gather information about the originality and authenticity of the image.
- Image retrieval: searching and comparing images between databases or the Internet to identify similar or similar images, thus providing insight into their source and authenticity.

The courses described cover a wide range of approaches used in digital image forensics to address various aspects of image analysis, verification and source identification.

Below we describe the main techniques that have been used in identifying image forgery:

2.1 Cloning forgery

Cloning forgery involves copying parts of one image and pasting them into the same or another image to create a deceptive or altered visual. This manipulation is done to mislead or create false representations, often making it difficult to distinguish between the original and edited content. In the context of digital media, cloning forgery frequently involves manipulating or changing photos, motion pictures, or other multimedia content to create misleading or false representations. Techniques utilized in cloning forgery can include copying and pasting elements from one image to another, altering the appearance of individuals or gadgets, or developing absolutely fabricated content material. Cloning forgery is often associated with photograph manipulation software program and superior modifying strategies, making it an increasing number of tough to stumble on and prevent. Cloning forgery will have extreme results, ranging from misinformation and propaganda to identity robbery and economic fraud. To fight cloning forgery, efforts involve the improvement of superior virtual forensics equipment and techniques for detecting and authenticating virtual content. Additionally, raising consciousness about the impact of cloning forgery can help higher defend towards such fraudulent activities [2].

2.2 Image splicing

Image fusion is the use of digital images in which pieces of multiple images are combined to create a new composite image. This technique is often used in image editing and graphics to combine the best features of multiple images. But image integration is especially important in digital forensics because it can be used to create fraudulent or deceptive images, raising concerns of authenticity and integrity in contexts ranging from news reports to legal evidence. If discovering splicing can be challenging, especially as repair tools become more sophisticated. Digital forensics researchers develop algorithms to detect errors in image metadata, lighting, shadows, or edge artifacts that can suggest exploitation.

Advanced techniques include analyzing noise patterns, pixel-level irregularities, and pattern recognition through Machine Learning models [4].

2.3 Image retouching

Image retouching is a widely used process in digital photography and graphic design to enhance and enhance the quality of images. This involves adjusting various features of the image, from simple corrections to complex adjustments, to correct deficiencies. This approach is especially common in advertising and graphic design, where the demand for high-quality, high-quality images is important but too much creativity can lead to fake images. Thus, restraint and disclosure have been required, especially in advertising when images change dramatically [9].

2.4 Image colorization

Image coloring is a digital technique for adding color to black and white photographs, making them visually appealing and realistic. This approach uses a variety of methods from manual methods such as Adobe Photoshop that rely on historical knowledge and design interpretation to fully automated methods using artificial intelligence Machine Learning models with color generation actual work indicates the appropriate color for grayscale painting. With advancements in technology, particularly in AI, automated colorization has become increasingly sophisticated. It enables high-quality colorizations of historical footage, classic films, and archival photographs. However, these tools carry responsibilities concerning historical accuracy and cultural sensitivity, balancing between enhancing visual information and preserving integrity [2].

3. RELATED WORKS

The related work for image splicing detection using standard ML-based models and DL-based models is described in this part. Starting with conventional ML models, He et al. [10] proposed an effective method for image splicing detection based on Markov characteristics in the DCT and DWT domain. The superior performance of their technique in comparison to other approaches is supported by experimental data. A method for splicing images that relies on inter-color channel data has been developed in the study [11]. This method, which seeks to identify the best suitable chroma-like channel, is computationally challenging.

Su et al. [12] propose an enhanced approach of Markov state selection, which matches coefficients to Markov states base on well-performed function model. Experiments and analysis show that the improved Markov model can employ more useful underlying information in transformed coefficients and can achieve a higher recognition rate as results compared to the previous version [13, 14]. Moghaddasi et al. [15] introduced an improved version for Image Splicing Forgery Detection (ISFD) using principal component analysis (PCA) and kernel PCA. PCA and Support Vector Machine (SVM) were employed to demonstrate the effectiveness of the prior merging, as indicated by El-Alfy et al. [16]. Li et al. [17] proposed an effective method for color ISFD. To perform the quaternion discrete cosine transform (QDCT), the authors utilized Markov features and then exploited SVM for

classification of the Markov feature vector. Zeng et al. [18] presented an efficient method based on PCA algorithm and K-means technique. The analysis of the study, compared to the original blocks and spliced blocks, showed that ISFD had better results.

In the same context several DL-based methods have been proposed to handle the image interpolation recognition task. Salloum and so on. Salloum et al. [19] provided a successful method for ISFD based entirely on convolutional networks (FCN). The authors initially introduced a single FCN (SFCN), and then implemented a multifunctional FSN (MFSN). Xiao et al. [20] presented a different ISFD method. The proposed method is based on diluted adaptive clustering and coarse-to-fine constrained neural networks (C2RNet). Experimental data have shown that the proposed method is significantly superior to current alternatives. However, the proposed detection method, which is an effective blind ISFD method, focuses on one modified part of the image due to the limitations of the postprocessing method and fails to detect other distorted paths. They also used the ResNet-Conv Deep Learning algorithm recommended by Ahmed et al. [21]. A computerized dataset for image splicing was used to train and test the recommended model, which was found to be more effective than the previous model. Besides, Nath and Naskar [22] used blind ISFD method was proposed, using a fully coupled classifier network and a residual convolutional neural network (R-CNN). When the method was tested with the CASIA v2.0 database, good results were obtained.

Using the dual-channel U-Net, or DCU-Net, Ding et al. [23] proposed an effective ISFD. The resilience of the suggested approach is demonstrated by experimental findings. Additionally, Kadam et al. [24] presented several ISFD methods, employing the Mask R-CNN with MobileNet V1 as the backbone architecture. The suggested technique was evaluated using a variety of cutting-edge datasets, including CASIA, Wild Web, MISD, and Columbia Gray. The outcomes demonstrated significant superiority. However, the suggested model is not put to the test against more attacks and assessment results, with and without these challenges, is not contrasted. Hosny et al. [25] presented a simple architecture based on CNN for copy-move forgery detection. When compared to other previously published approaches, the given methodology demonstrates advantages in terms of speed and accuracy. When it comes to image splicing fraud, it is not particularly effective.

Another study for Hosny et al. [26] proposed a convolutional neural network (CNN) model for detecting splicing forged images in real-time, with a small number of parameters. The model presented is lightweight, comprising only four convolutional layers and four max-pooling layers, making it suitable for environments with resource constraints. The sensitivity and specificity of the proposed model across CASIA v1.0, CASIA v2.0, and CUISDE datasets were evaluated. The model achieved an accuracy of 99.1% in detecting forgery on the CASIA v1.0 dataset, 99.3% on the CASIA v2.0 dataset, and 100% on the CUISDE dataset.

Al-Shamasneh and Ibrahim [27] proposed a method that uses a new feature extraction model based on deep features combined with Sonine functions convex features. The proposed CNN was used to automatically generate the deep features from the color image, while Sonine functions convex was used to extract the texture features from the input images. Finally, the Support Vector Machine (SVM) technique was utilized for classification. The proposed model achieved an

accuracy of 98.93% when tested with the CASIA v2.0 dataset. Nguyen et al. [28] proposed a new Deep Learning model for splicing image detection by implementing residual network in modified VGG-16 architecture to accommodate the limited resources of constraint machines. Compared to ResNet-50, the proposed model performs superior performance on computers with low memory and using a smaller batch size. Experimental results show that the proposed model achieves higher accuracy and lower loss across ResNet-50 at the training, validation and test sets. The test accuracy of the revised model is 92.5%, while the ResNet-50 gives 85.6% after 20 epochs of training 9319 images from the CASIA v2.0 dataset.

4. PROPOSED APPROACH

Our system's primary objective is to enhance the accuracy of the image splicing detection model. To achieve this goal, the system is divided into two steps. The first stage involves pre-processing, which reduces the number of parameters needed to describe the input image. This is achieved by converting RGB images to HSV and resizing input images to [128×128×3]. In the second step, we suggested using a Depthwise Separable (DWS) Convolution Neural Network based on MobileNet V2 to address the issue of image splicing detection. Instead of using 2D convolution layers, the suggested network utilizes of depth-wise separable convolution layers (DWCNN). Hence, using a network architecture, DWS-based MobileNetV2 reduces the number of trainable parameters while improving learning performance.

4.1 Preprocessing stage

As the HSV color space is more sensitive to color changes and more resistant to changes in illumination, RGB images are initially converted to HSV in the pre-processing step. The HSV color model, which comprises hue, saturation, and value components, closely mimics human perception of color. For this reason, it is common to request users to select colors.

The significance of the three components is explained as follows [19]:

- Hue (H): Represents the intrinsic property of color, indicating red, green, etc.
- Saturation (S): Indicates the degree of white added to the color. Saturation is low when a color contains more white.
- Value (V): Reflects a color's brightness.

The transformation from RGB to HSV space is described by a system of three equations, as follows:

$$V = \max(R, G, B) \tag{1}$$

$$S = \begin{cases} \frac{\max(R,G,B) - \min(R,G,B)}{\max(R,G,B)} & \text{if } \max(R, G, B) \neq 0 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

$$H = \begin{cases} \text{undefined} & \text{if } S = 0 \\ \frac{G - B}{\max(R, G, B) - \min(R, G, B)} & \text{if } R = \max(R, G, B) \\ 2 + \frac{B - R}{\max(R, G, B) - \min(R, G, B)} & \text{if } G = \max(R, G, B) \\ 4 + \frac{R - G}{\max(R, G, B) - \min(R, G, B)} & \text{if } B = \max(R, G, B) \end{cases} \tag{3}$$

As depicted in Figure 4, it's easy to distinguish between

sections that resemble each other and those that appear distinct in an image produced in HSV; however, this distinction is challenging to make in an RGB image. To reduce the number of parameters needed to represent the input image, it's resized to $128 \times 128 \times 3$.

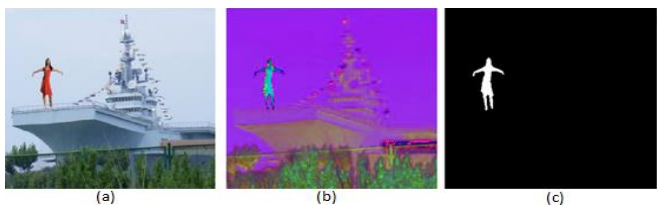


Figure 4. Image splicing, (a) RGB, (b) HSV, (c) ground-truth

4.2 Custom DWCNN model

Depth-wise Convolutional Neural Networks are a specialized form of convolutional neural networks designed for computational efficiency, making them well-suited for mobile and embedded vision applications. Unlike standard convolutions that apply filters across all input channels simultaneously, depth-wise convolutions operate separately on each channel, and significantly reducing the number of computations and parameters. This technique, central to architectures like MobileNets, splits the convolution into a depth-wise layer that performs lightweight filtering by applying a single filter per channel, followed by a point-wise convolution (1×1 convolution) that combines these outputs to produce new features. This approach not only enhances computational efficiency and model execution speed but also reduces the risk of overfitting, making depth-wise CNNs particularly suitable for devices with limited processing capabilities such as smartphones and IoT devices, without significantly compromising the model's performance.

In Figure 5, we depict the suggested model architecture.

After pre-processing, a custom CNNs model is fed image data with a size of $128 \times 128 \times 3$ for classification. Our concept consists of seven interconnected bottleneck blocks. Each block consists of three convolution layers, batch normalization, and ReLU6 activation. A description of each layer is provided in Table 1. The rectified linear unit, also known as ReLU6, allows a maximum of six activation values. This results in improved robustness when employing low-precision calculations.

The DWCNN model comprises a residual block with a stride of 1 and a block without a residual link with a stride of 2. Following these blocks, ReLU6 and a global average pooling layer are attached to the network, followed by a fully connected (FC) layer with 2 neurons. The final layer consists of two neurons: one for spliced prediction and the other for real prediction. Predicted probabilities are generated using the softmax function. All these layers contribute to the formation of the categorization layer, which is responsible for producing the final result.

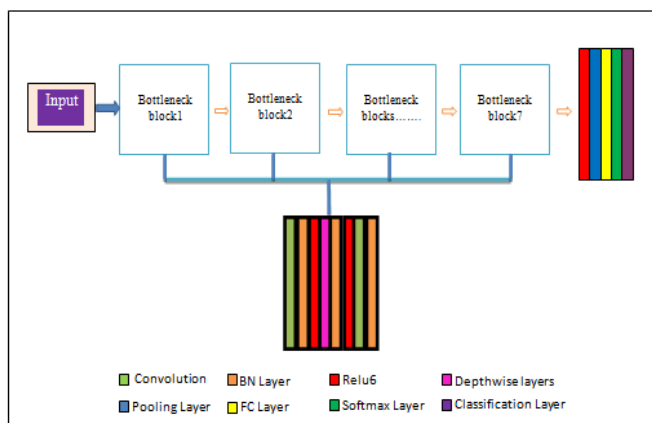


Figure 5. The proposed DWCNN model architecture

Table 1. Structure of the proposed model

Block Name	Conv			Size	DW			Conv		
	Size	Filter	Stride		Filter	Stride	Size	Filter	Stride	
Bottleneck1	1×1	96	1	3×3	96	2	1×1	24	1	
Bottleneck2	1×1	144	1	3×3	144	1	1×1	24	1	
Bottleneck3	1×1	144	1	3×3	144	2	1×1	32	1	
Bottleneck4	1×1	192	1	3×3	192	1	1×1	32	1	
Bottleneck5	1×1	192	1	3×3	192	1	1×1	32	1	
Bottleneck6	1×1	192	1	3×3	192	2	1×1	64	1	
Bottleneck7	1×1	384	1	3×3	384	1	1×1	64	1	

5. EXPERIMENTAL RESULTS AND DISCUSSION

The experiment utilized a PC equipped with an Intel Core i7 CPU, 8 GB of RAM, and running Windows 10. MATLAB R2022b was employed for conducting the experiment. Additionally, two datasets were used: CASIA v1.0, which consists of 800 real photographs and 921 color images spliced together in JPEG format, each with dimensions of 384×256 pixels; and CASIA v2.0, containing 7491 real images and 5123 altered images in JPEG, BMP, and TIFF formats, with dimensions ranging from 240×160 to 900×600 pixels, as shown in Table 2. In this work, we divided the datasets to 60% for training, 10% for validation and 30% for testing.

Our suggested model for identifying spliced images was trained using stochastic gradient descent with momentum

(SGDM) with an initial learning rate of 0.01. A minimum batch size of 128 and a maximum of 30 epochs were chosen for executing the training phase. Figures 6 and 7 show the training/ validation model results using CASIA v1.0 and v2.0 dataset respectively. The systems' performance was assessed using multiple metrics such as accuracy, recall, precision, and F1 score. These metric values were calculated from the confusion matrix produced by the systems. The confusion matrix offers valuable insights into classification results, differentiating between true positives (TP), which are correctly identified manipulated images; true negatives (TN), which are correctly identified non-manipulated images; false positives (FP), where authentic images are incorrectly classified as manipulated; and false negatives (FN), where manipulated images are incorrectly classified as non-

manipulated. Accuracy was computed to evaluate the performance of the proposed image splicing detection model. It can be calculated through the following equations [3]:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

$$Recall = \frac{TP}{TP + FN} \quad (5)$$

$$Precision = \frac{TP}{TP + FP} \quad (6)$$

$$F1\ Score = 2 \times \left(\frac{Precision \times Recall}{Precision + Recall} \right) \quad (7)$$

Table 2. Components of the CASIA v1.0 and v2.0 dataset

Dataset	Authentic	Tampered	Total	Image Type	Image Size
CASIA v1.0	800	921	1721	JPEG	384×256
CASIA v2.0	7491	5123	12614	JPEG, BMP, TIFF	240×160 to 900×600

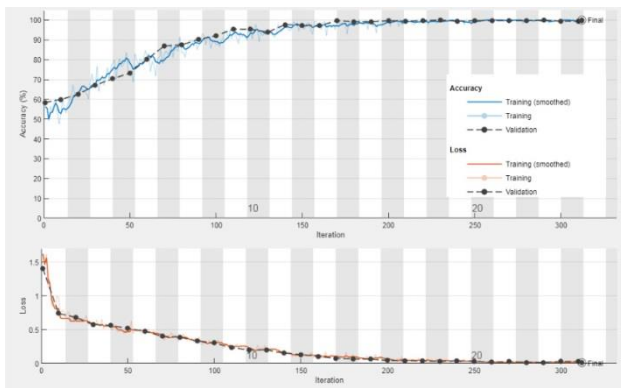


Figure 6. Accuracy and loss curve vs. iterations using CASIA v1.0

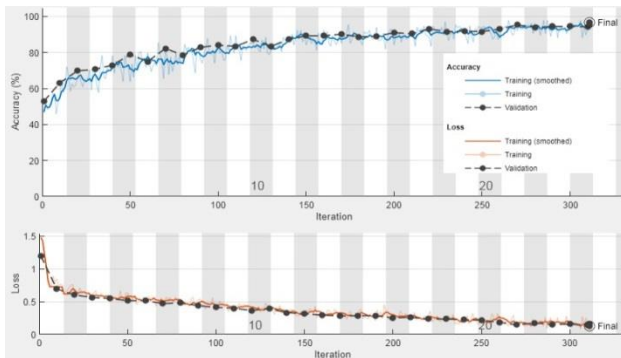


Figure 7. Accuracy and loss curve vs. iterations using CASIA v2

The impact of employing the HSV color space instead of RGB has been examined to assess the performance of the suggested model with both options. The comparison results, utilizing the CASIA v1.0 and v2.0 datasets, are depicted in Figure 8. The findings indicate that our suggested model achieves higher accuracy when the input images are converted to the HSV color space compared to RGB.

Figures 6 and 7 show plots of the evaluation metrics for our DWCNN architecture, which achieved accuracies of 99.23% and 99.37% using CASIA v1 and CASIA v2 respectively. These figures offer insights into the model's performance during training and validation. Typically, metrics such as validation accuracy, validation loss, and the confusion matrix (Figures 9 and 10) are plotted alongside accuracy. Table 3 displays the performance evaluation metrics for the proposed model in both datasets.

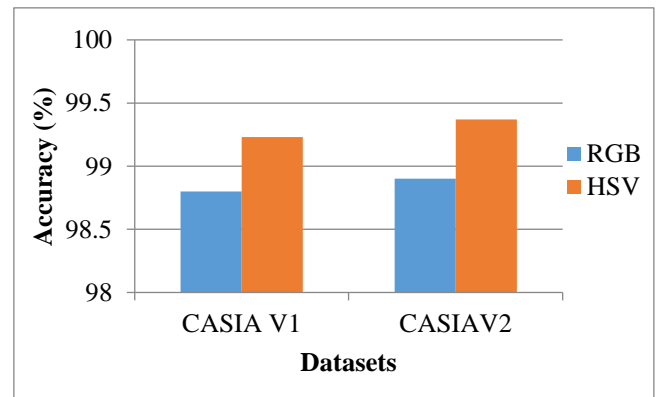


Figure 8. Accuracy comparison between RGB and HSV color spaces models

Table 3. Performance metrics of the proposed system

Metrics	CASIA v1.0	CASIA v2.0
Accuracy	99.23%	99.37%
Recall	99.64%	99.78%
Precision	98.92%	99.15%
F1-Score	99.28%	99.46%

Figure 9 and 10 present the confusion matrices generated for the image slicing detection task using CASIA v1.0 and CASIA v2.0 respectively.

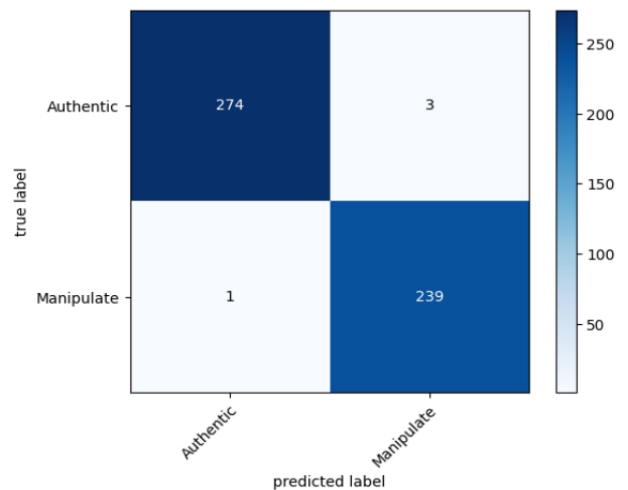


Figure 9. Confusion matrices using CASIA v1.0

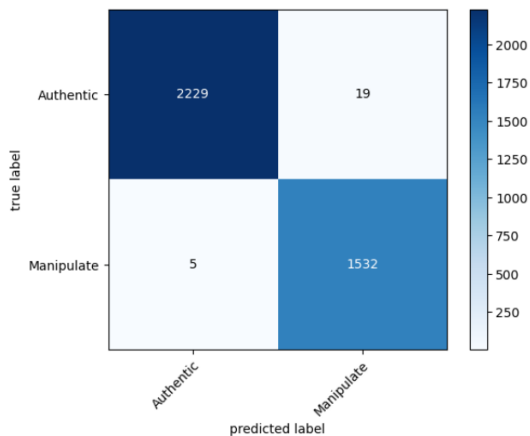


Figure 10. Confusion matrices using CASIA v2.0

Furthermore, given the importance of time as a crucial metric for assessing a model's efficacy, we compared the runtime of our model with that reported in recently published articles. Table 4 shows that the suggested model's reduced testing time, which is related to the number of parameters, making it an excellent option for high-volume picture classification as it doesn't call for a high-performance device.

Table 4. Image splicing detection time (in seconds)

Methods	CASIA v1.0	CASIA v2.0
Alahmadi et al. [13]	156	326
Kadam et al. [24]	280	-
Hosny et al. [25]	15.7	220
Proposed method	10	189

Experimental comparisons were conducted between our suggested model and cutting-edge techniques for classification accuracy. Table 5 presents all testing findings and demonstrates that, when evaluated on benchmark datasets, our method surpassed the current state of the art. The accuracy of our suggested model is significantly higher than that of all other proposed methods and previous works, whether they rely on manual processes or Deep Learning [13, 24-26].

Table 5. Accuracy comparison with state-of-the-art models

Methods	Accuracy	
	CASIA v1.0	CASIA v2.0
Alahmadi et al. [13]	97%	97.77%
Hosny et al. [26]	98.25%	96.66%
Kadam et al. [24]	64%	-
Hosny et al. [25]	99.1%	99.3%
Proposed method	99.23%	99.37%

6. CONCLUSIONS

This work introduces a novel image splicing detection approach employing the DWCNN model architecture. Two distinct color spaces, RGB and HSV, were utilized to assess the impact of different color spaces on model performance. HSV color space demonstrates superior sensitivity to color changes and robustness to lighting variations. Based on these observations, it yielded better results compared to the RGB color space. For future work, we propose evaluating other types of CNN structures, which are more advanced such as YOLO for addressing real-time image splicing detection tasks.

REFERENCES

- [1] Park, C.S., Choeh, J.Y. (2018). Fast and robust copy-move forgery detection based on scale-space representation. *Multimedia Tools and Applications*, 77: 16795-16811. <https://doi.org/10.1007/s11042-017-5248-y>
- [2] Salman, K.A., Shaker, K., Al-Janabi, S. (2023). Fake colored image detection approaches: A review. *International Journal of Image and Graphics*, 23(6): 2350050. <https://doi.org/10.1142/S021946782350050X>
- [3] Peng, J., Li, Y., Liu, C., Gao, X. (2023). The circular unet with attention gate for image splicing forgery detection. *Electronics*, 12(6): 1451. <https://doi.org/10.3390/electronics12061451>
- [4] Khazaal, M.S., Kherallah, M., Charfi, F. (2022). An overview on detecting digital image splicing. In *2022 International Arab Conference on Information Technology (ACIT)*, pp. 1-4. <https://doi.org/10.1109/ACIT57182.2022.9994194>
- [5] Yan, C., Li, S., Li, H. (2023). TransU 2-Net: A hybrid transformer architecture for image splicing forgery detection. *IEEE Access*, 11: 33313-33323. <https://doi.org/10.1109/ACCESS.2023.3264014>
- [6] Howard, A. G., Zhu, M., Chen, B., Kalenichenko, D., Wang, W., Weyand, T., Andreetto, M., Adam, H. (2017). Mobilenets: Efficient convolutional neural networks for mobile vision applications. *arXiv preprint arXiv:1704.04861*. <https://doi.org/10.48550/arXiv.1704.04861>
- [7] Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., Chen, L.C. (2018). Mobilenetv2: Inverted residuals and linear bottlenecks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 4510-4520.
- [8] Dong, J., Wang, W., Tan, T. (2013). Casia image tampering detection evaluation database. In *2013 IEEE China Summit and International Conference on Signal and Information Processing*, pp. 422-426. <https://doi.org/10.1109/ChinaSIP.2013.6625374>
- [9] Hsu, Y.F., Chang, S.F. (2006). Detecting image splicing using geometry invariants and camera characteristics consistency. In *2006 IEEE International Conference on Multimedia and Expo*, pp. 549-552. <https://doi.org/10.1109/ICME.2006.262447>
- [10] He, Z., Lu, W., Sun, W., Huang, J. (2012). Digital image splicing detection based on Markov features in DCT and DWT domain. *Pattern Recognition*, 45(12): 4292-4299. <https://doi.org/10.1016/j.patcog.2012.05.014>
- [11] Zhao, X., Li, S., Wang, S., Li, J., Yang, K. (2012). Optimal chroma-like channel design for passive color image splicing detection. *EURASIP Journal on Advances in Signal Processing*, 2012: 1-11. <https://doi.org/10.1186/1687-6180-2012-240>
- [12] Su, B., Yuan, Q., Wang, S., Zhao, C., Li, S. (2014). Enhanced state selection Markov model for image splicing detection. *EURASIP Journal on Wireless Communications and Networking*, 2014: 1-10. <https://doi.org/10.1186/1687-1499-2014-7>
- [13] Alahmadi, A., Hussain, M., Aboalsamh, H., Muhammad, G., Bebis, G., Mathkour, H. (2017). Passive detection of image forgery using DCT and local binary pattern. *Signal, Image and Video Processing*, 11: 81-88. <https://doi.org/10.1007/s11760-016-0899-0>

- [14] Sunitha, K., Krishna, A.N. (2020). Efficient keypoint based copy move forgery detection method using hybrid feature extraction. In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 670-675. <https://doi.org/10.1109/ICIMIA48430.2020.9074951>
- [15] Moghaddasi, Z., Jalab, H.A., Md Noor, R., Aghabozorgi, S. (2014). Improving RLRN image splicing detection with the use of PCA and kernel PCA. *The Scientific World Journal*, 2014(1): 606570. <https://doi.org/10.1155/2014/606570>
- [16] El-Alfy, E.S.M., Qureshi, M.A. (2015). Combining spatial and DCT based Markov features for enhanced blind detection of image splicing. *Pattern Analysis and Applications*, 18: 713-723. <https://doi.org/10.1007/s10044-014-0396-4>
- [17] Li, C., Ma, Q., Xiao, L., Li, M., Zhang, A. (2017). Image splicing detection based on Markov features in QDCT domain. *Neurocomputing*, 228: 29-36. <https://doi.org/10.1016/j.neucom.2016.04.068>
- [18] Zeng, H., Zhan, Y., Kang, X., Lin, X. (2017). Image splicing localization using PCA-based noise level estimation. *Multimedia Tools and Applications*, 76: 4783-4799. <https://doi.org/10.1007/s11042-016-3712-8>
- [19] Salloum, R., Ren, Y., Kuo, C.C.J. (2018). Image splicing localization using a multi-task fully convolutional network (MFCN). *Journal of Visual Communication and Image Representation*, 51: 201-209. <https://doi.org/10.1016/j.jvcir.2018.01.010>
- [20] Xiao, B., Wei, Y., Bi, X., Li, W., Ma, J. (2020). Image splicing forgery detection combining coarse to refined convolutional neural network and adaptive clustering. *Information Sciences*, 511: 172-191. <https://doi.org/10.1016/j.ins.2019.09.038>
- [21] Ahmed, B., Gulliver, T.A., alZahir, S. (2020). Image splicing detection using mask-RCNN. *Signal, Image and Video Processing*, 14(5): 1035-1042. <https://doi.org/10.1007/s11760-020-01636-0>
- [22] Nath, S., Naskar, R. (2021). Automated image splicing detection using deep CNN-learned features and ANN-based classifier. *Signal, Image and Video Processing*, 15(7): 1601-1608. <https://doi.org/10.1007/s11760-021-01895-5>
- [23] Ding, H., Chen, L., Tao, Q., Fu, Z., Dong, L., Cui, X. (2023). DCU-Net: A dual-channel U-shaped network for image splicing forgery detection. *Neural Computing and Applications*, 35(7): 5015-5031. <https://doi.org/10.1007/s00521-021-06329-4>
- [24] Kadam, K., Ahirrao, S., Kotecha, K., Sahu, S. (2021). Detection and localization of multiple image splicing using MobileNet V1. *IEEE Access*, 9: 162499-162519. <https://doi.org/10.1109/ACCESS.2021.3130342>
- [25] Hosny, K.M., Mortda, A.M., Fouda, M.M., Lashin, N.A. (2022). An efficient CNN model to detect copy-move image forgery. *IEEE Access*, 10: 48622-48632. <https://doi.org/10.1109/ACCESS.2022.3172273>
- [26] Hosny, K.M., Mortda, A.M., Lashin, N.A., Fouda, M.M. (2023). A new method to detect splicing image forgery using convolutional neural network. *Applied Sciences*, 13(3): 1272. <https://doi.org/10.3390/app13031272>
- [27] Al-Shamasneh, A.A.R., Ibrahim, R.W. (2024). Image splicing forgery detection using feature-based of sonine functions and deep features. *Computers, Materials & Continua*, 78(1): 795-810. <http://dx.doi.org/10.32604/cmc.2023.042755>
- [28] Nguyen, H.L., Huynh, K.T. (2024). A deep learning model for splicing image detection. *REV Journal on Electronics and Communications*, 13(3-4): 45-53.