Image Tamper Detection using the Fusion CMFD Model with Advanced VGG16 Features

Smruti Dilip Dabhole
Dept of CS
KSAWU, Vijayapura
Karnataka, India -586108

G.G. Rajput
Dept of CS
KSAWU, Vijayapura
Karnataka, India -586108

Rajendra Hegadi
Dept of DSAI
IIIT, Dharwad
Karnataka, India

Prashantha
Dept of CS
RCU Belagavi,
Karnataka, India

ABSTRACT
Due to the widespread availability of the internet and the abundance of devices capable of capturing images, there has been a significant increase in the number of images shared online. These images are easily manipulated using advanced software tools like Adobe Photoshop, leading to the creation of fake visuals. As the sophistication of image and video editing tools continues to advance, distinguishing between authentic and altered images has become increasingly challenging. Thus, it is crucial to verify the authenticity of images before deriving any significant insights from them. In this paper we present a novel method for detecting and categorizing tampered and genuine regions within images, without reliance on reference images. The proposed novel approach called 'Fusion CMFD' 'Copy Move Forgery Detection (CMFD)', model includes fusion of 'Manipulation CMFD' model and 'Similarity CMFD' model. Features are extracted in both models using VGG16 neural network architecture where, features from convolutional layers are intelligently concatenated to enhance discriminative power and facilitate more accurate identification of genuine and tampered regions within an image. 'Similarity CMFD' model employs the VGG16 architecture, utilizing self-correlation to assess feature similarity between the input image and its corresponding mask. Potential features are aggregated using Percentile Pooling, and then a Mask Decoder is utilized to upscale feature maps to the original image dimensions. 'Manipulation CMFD' includes feature extraction using VGG16 and mask decoder. The proposed innovative approach promises enhanced accuracy and robustness in detecting tampered and genuine regions within images, opening up new avenues in the field of image forensics and enhancing overall security measures in digital content authentication. Experiments are performed on images from the MICC-F2000 [1] dataset. The results are compared against existing methodologies reported in the literature and cross verified with MICC-F220 dataset. Performance has been analyzed using parameters namely, accuracy, precision and recall.

General Terms
Digital Image Processing, Computer Vision, Pattern Recognition

Keywords
VGG16, CNN, Deep learning, Correlation, Image tamper detection

1. INTRODUCTION
Images present a substantial concern across industries reliant on digital photography for multifaceted applications. From suspect identification to crime scene documentation and biometric data, images have entrenched themselves in forensic and public safety domains. The advent of digital photography has markedly escalated their prevalence in these sectors. While digital image processing has facilitated more facile manipulation, it has also catalyzed the evolution of innovative forensic methodologies. The veracity of digital images is now under scrutiny due to the ubiquitous availability of diverse image alteration programs, furnishing compelling evidence in myriad criminal investigations and serving as documentation for multifarious purposes. The availability of image editing and processing software tools has made the process of modifying original images more efficient and they are accessible to everyone. Notably, image splicing and copy-move forgeries emerge as the most prevalent forms of image manipulation.

The 'copy-move' technique involves extracting a segment from an image and replicating it somewhere in the same image. This process effectively duplicates specific regions within the image, resulting in the creation of new content. Due to the preservation of key image characteristics such as illumination, proportion, and focus, images manipulated using the copy-move technique often exhibit minimal visible evidence of tampering [2]. Patterns present in textured surfaces like grass, foliage, gravel, or fabric serve as ideal camouflage for digital manipulation techniques. The irregular patterns found in these surfaces facilitate seamless blending with the background, making it challenging for the human eye to detect any inconsistencies. Moreover, since the copied segments originate from the same image, they maintain uniformity in noise, color, and other essential properties, ensuring compatibility with the overall image [13]. Content forgery also includes certain kinds of orientations like scaling, rotation and transformations resulting in image blurring, noise addition and contrast enhancement [26].

Many methods have been proposed to detect copy move forgery, ranging from block matching techniques like DCT domain analysis and keypoint-based methods like Scale Invariant Features Transform (SIFT), Speeded Up Robust Features (SURF), AKAZE [8] gradient analysis, multi-resolution techniques, and deep learning approaches [5, 6, 7, 24]. Integrating multiple techniques or devising hybrid methodologies holds the potential to bolster the accuracy and resilience of copy-move forgery detection systems. Many of the methods are effective at identifying copied regions within an image; they often face challenges in distinguishing between genuine and tampered areas within the same image [24, 3,5, 6, 10, 21].

In this paper, proposed method present neural network approach to identify tampering within an image and classify the genuine and tampered region within the image. The proposed novel methodology uses fusion of 'Manipulation CMFD' and 'Similarity CMFD' viz., 'Fusion CMFD' which utilize VGG16 for extracting the features by concatenating the convolution layers of VGG16. And Mask Decoder is utilized to upscale

feature maps to the original image dimensions, which predicts the tampered and genuine region within an image.

The remaining paper is organized as follows, section 2 describes literature survey, section 3 focuses on the proposed methodology, and section 4 presents experiments results. Next section 5 about discussion and limitations whereas, section 6 describes the conclusion and future work.

2. LITERATURE SURVEY

In this section we explore several existing approaches for detecting copy-move forgery, which encompass pixel-based, patch-based, and neural network-based methods.

Amerini et al. [7] introduced a novel approach based on the J-Linkage algorithm that identifies regions in an image exhibiting similar patterns or textures, indicating potential tampering. Experimental evaluations conducted on diverse dataset of images demonstrate the superiority of the proposed method over comparable state-of-the-art techniques in terms of both copy-move forgery detection reliability and precision in localizing manipulated patches. The keypoint based approach proposed by Ibrahim A et.al. [4] models keypoints as whole regions rather than single points and utilizes the intersection over union measure to address image continuity. False matches caused by image self-similarity are mitigated by combining cross-matching tests with a modified distance ratio test, enabling the detection of multiple cloning instances. A support vector machine is employed to learn thresholds for determining the occurrence of CMF. Comparative evaluations of the proposed method on Coverage and MICC-F220 datasets highlight the methodology's ability to handle geometric transforms and multiple cloning instances while efficiently managing image continuity without the need for external methods. Chengyou Wang et al. [11] presented an innovative strategy merging Accelerated-KAZE (A-KAZE) and SURF techniques to enhance forgery detection. Traditional keypoint-based methods often struggle to capture adequate points in smoother image regions. To address this limitation, the approach sets low response thresholds for both A-KAZE and SURF feature detection stages. A correlation coefficient map integrating filtering and mathematical morphology operations delineate duplicated regions. Extensive experiments demonstrate the method's efficacy in detecting duplicated areas and its robustness against diverse distortions and post-processing techniques, including noise injection, rotation, scaling, image blurring, JPEG compression, and hybrid image manipulation.

Kaur, N. et al. [23] introduced a novel framework for copy move forgery detection leveraging deep learning techniques. The prposed framework combines contrast-limited adaptive histogram equalization (CLAHE) with a convolutional neural network (CNN) to discern images as pristine or tampered. The integration of CLAHE enhances the visibility of latent features within the image, facilitating the detection of specific elements characteristic of CMF. Evaluation of the proposed framework extends to various benchmark datasets, including GRIP, MICC-F2000, IMD, and MICC-F220, underscoring its efficacy and robustness across diverse scenarios.

K. M. Hosny et.al. [9] presented a CNN architecture tailored for the precise detection of copy-move image forgery. The proposed architecture is designed to be computationally lightweight, featuring an optimal number of convolutional and max-pooling layers. The proposed system utilizes feature vectors extracted from image features and leverages full connection layers to identify feature correspondences and dependencies automatically. A rapid and accurate testing process, taking only 0.83 seconds per test, is presented. Extensive empirical experiments conducted on MICC-F2000, MICC-F600, and MICC-F220 datasets demonstrate the efficacy of the proposed model in terms of both accuracy and efficiency, achieving 100% accuracy across all experiments. Detection methodology based on deep neural learning is capable of accurately recognizing tampered images and classifying them into forged or original image categories. The disadvantage of proposed model is it does not identify the forged regions within the classified tampered image. Prabakar [3] proposed a hybrid method to detect tampering from noisy images. Initially, sample images from MICCF2000 are extracted and resized. A filtering technique is applied to eliminate any noise that might have been present in the tampered image and finally, integrated CNN and Support Vector Machine (SVM) is used to construct a hybrid model to detect copy move forgery.

Ye, W., Zeng et.al.[25] presented two-stage forgery detection approach integrating parallel fusion features and an adaptive threshold generation algorithm comprising coarse-grained and fine-grained detection phases. Initially, in the coarse-grained detection phase, the SLIC algorithm is employed to preprocess images and partition them into irregular super pixels, addressing issues related to local regional correlation attenuation resulting from uniform segmentation. Subsequently, in the fine-grained detection phase, parallel fusion features are utilized to bolster the expressive capacity of local regions. An adaptive threshold generation algorithm based on the HOG level is devised to produce suitable thresholds tailored to the characteristics of distinct local regions for the final detection of suspected tampered areas. Experimental validation and comparative analysis against other methodologies confirm the superior accuracy and robustness of the proposed method, demonstrating its effectiveness in withstanding common attacks such as noise and brightness alterations. Nonetheless, there remains a scope for enhancing the method's resistance against fuzzy attacks, necessitating further investigation. Moreover, while the proposed method exhibits limitations in precisely pinpointing tampered regions compared to deep learning approaches, its integration with such methods could enable more accurate detection and localization.

Khurshid Asghar et.al. [16] presented an image forgery detection method based on DRLBP and SVM. Features are extracted by dividing the chrominance components of an input image into overlapping blocks and calculating the DRLBP code for each block. These features, represented by histograms of all blocks from both Cb and Cr components, are then used for classification using SVM classifier. Extensively evaluated across eight benchmark datasets viz. DVMM, CASIA v1.0, CASIA v2.0, CoMFoD, MICC-F220, MICC-F2000, UNISA, FRITH, Set-A and Set-B, including cross-dataset validation, the proposed method consistently outperforms state-of-the-art approaches. Its effectiveness in modeling structural changes in tampered images, attributed to the DRLBP texture descriptor, contributes to its robustness against various post-processing operations, file types, and image resolutions.

Nagaveni K et al. [15] introduced a methodology leveraging pre-trained models through transfer learning for the classification of counterfeit images. The initial step involved preprocessing the images using Error Level Analysis (ELA) to detect tampered pixels. The results revealed that deepening the network did not lead to performance improvement; instead,

performance deteriorated, primarily due to model overfitting. To address this issue, DenseNet and ResNet50 were utilized, as they incorporate feature maps from earlier layers into subsequent layers, mitigating overfitting. Notably, these models demonstrated superior performance compared to those employing image patches. Additionally, the complexity and processing time of the network were reduced, as it was trained using the entire image dataset without the need for patches. Among the six models evaluated, ResNet50 exhibited the most favorable performance. Rodriguez-Ortega Y. et.al. [2] proposed two deep learning approaches: a custom architecture model and a transfer learning (TL) model to detect tampering in images. The model is evaluated using parameters precision, recall, and F1 score for each approach across diverse datasets and their performance metrics and computational efficiency are analyzed. The results suggest that while the TL model based on VGG-16 achieves higher metrics than the custom architecture, it requires longer inference times.

From literature review, we observe that many of the methods perform effectively in restricted constraints such as duplication of the object limited to one or two, dynamic range of intensity values in the image is limited. Further, the presence of outliers leads to wrong results and in certain cases computational time is high. The methods performance affects in case of orientations. Majority of the work are able to detect image forgeries. However, only few attempts have been found to classify the regions of an image as original and tampered.

3. METHODOLOGY

This section describes the proposed approach for mage forgery detection. The proposed approach is presented in two stages. Detecting the tampered region from an image viz. 'Manipulation CMFD' and next, detecting both similar regions from an image viz. 'Similarity CMFD' (Figure 1). Then Fusion of both the classification method identifies tampered and genuine region from an image viz. 'Fusion CMFD'. The contribution of the proposed method lies is in extracting the features using VGG16 architecture, where features are concatenated from the convolutional layers of VGG16 and the fusion of proposed classification to identify the tampered and genuine region within the image. The details are given below.

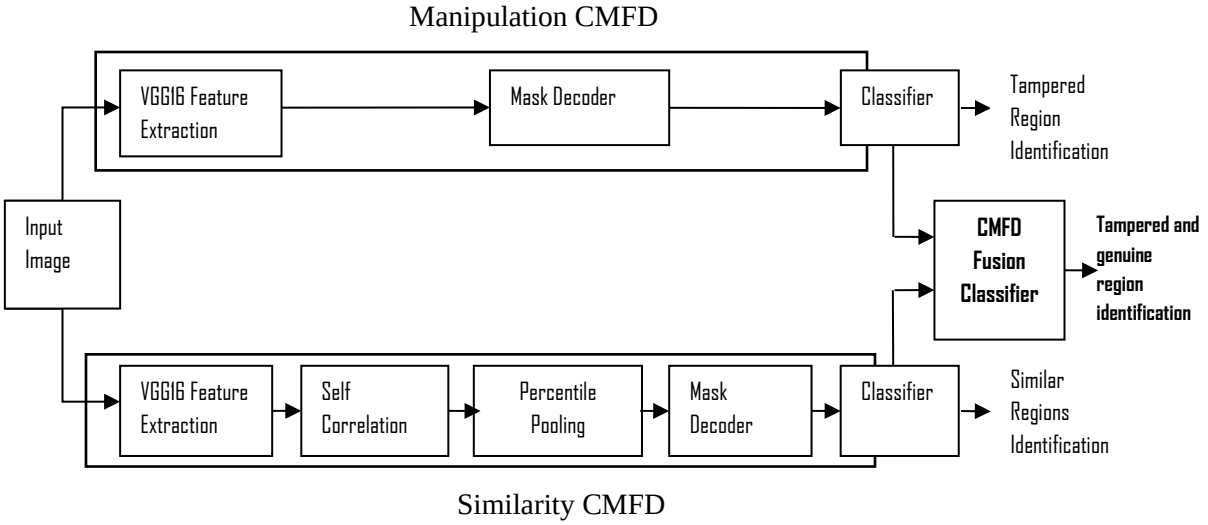

Fig1 : Proposed Architecture for Copy Move Forgery Detection

3.1 Dataset

The dataset utilized in the network is MICC-F2000, consisting of 1300 authentic images and 700 tampered images, all having a resolution of 739 × 492[7,8]. This dataset is employed to gauge the effectiveness of the proposed method against geometric alterations, including translation, rotation, and stretching, as well as various combinations of these transformations. Tampered images are used for training the model. The method's resilience is assessed based on the degrees of rotation, stretching, and translation, each posing distinct challenges to its performance. Since the dataset lacks in binary masks, binary masks for tampered images are generated by comparing genuine and tampered versions of the images from the dataset using VGG Image Annotator (VIA). The dataset is divided into training and validation sets with proportions of 70% and 30%, respectively. The image data is then input into the proposed model. The proposed fusion model comprises of two components: the first being 'Manipulation CMFD,' which involves generating binary masks using tampered images from the dataset. As a result, the generated binary masks exclusively encompass the tampered regions of the image, as illustrated in Figure 2. Subsequently, the second model, 'Similarity CMFD,' is tasked with identifying cloned regions within the image. This model utilizes the binary masks generated from the previous step to facilitate training, as depicted in Figure 3.

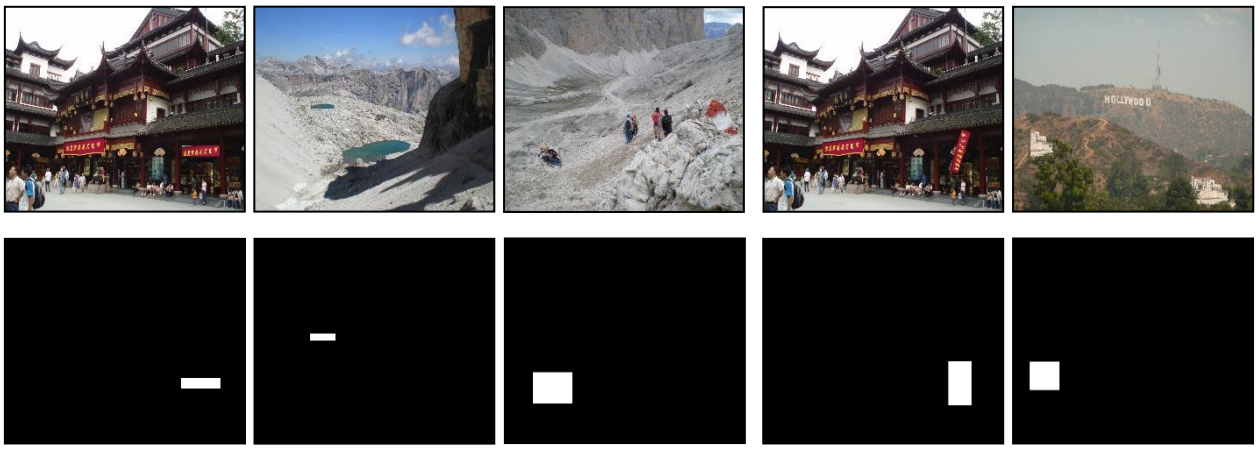

Fig 2 : row 1: Tampered images row 2 : Mask images created using VGG image annotator for 'Manipulation CMFD' model

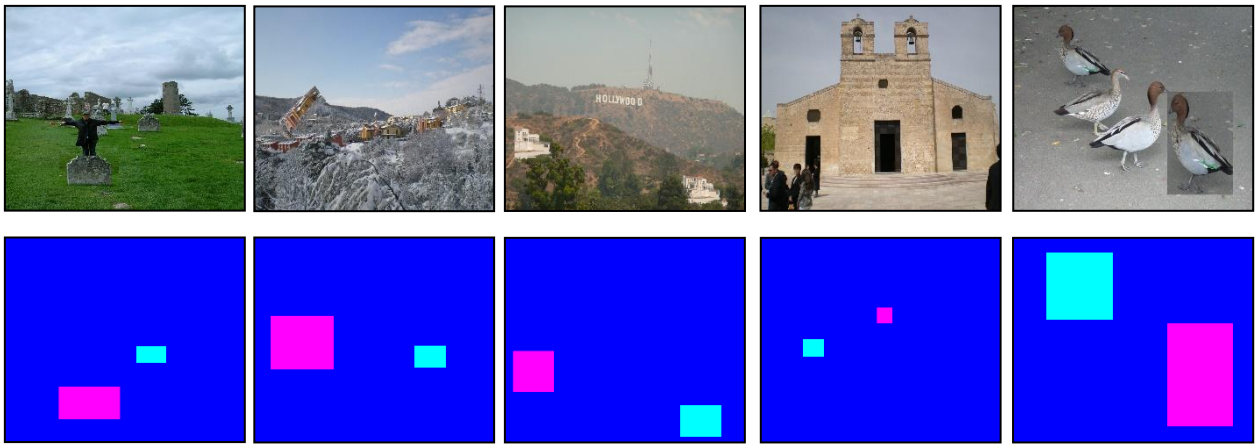

Fig 3 : Row 1: Tampered images row 2 : Mask images created using VGG image annotator for 'Fusion CMFD' model

3.2 Feature Extraction

The CNN is a deep learning algorithm, widely used in image recognition, object detection, and image segmentation tasks due to their ability to automatically learn spatial hierarchies of features from raw pixel data. For proposed methodology, VGG16 architecture is used for feature extraction. It is characterized by its simplicity and uniformity, consisting of a series of convolutional layers followed by max-pooling layers, with fully connected layers at the end. VGG16 consists of 13 convolutional layers grouped into five blocks, where each block is followed by a max-pooling layer. The convolutional layers uses 3x3 filters with a stride of 1 and "same" padding, and it is responsible for extracting features from the input image. MaxPooling is a down sampling operation used to reduce the spatial dimensions of feature maps while retaining the most important information [2]. The 'ReLU' activation function used in architecture replaces negative pixel values with zero and leaves positive values unchanged. 'ReLU' helps alleviate the vanishing gradient problem, which can occur in deep neural networks during back propagation [22]. The last two layers of VGG16 are fully connected layers, consisting of 4096 neurons each, followed by a final output layer with 1000 neurons (corresponding to 1000 ImageNet classes) and a 'softmax' activation function [19]. In proposed methodology first 4 blocks of VGG16 are used (figure 4). Here, input image of size (256, 256, 3) with corresponding binary masks of same size is input to the model. Each convolutional block consists of multiple convolutional layers followed by activation functions (ReLU) and max-pooling layers. These layers help in extracting hierarchical features from the input images. The features are extracted, in Block 1, using two convolutional layers (Conv2D) with 64 filters applied to the input images. The outputs of these layers are concatenated with the original input and then passed through a max-pooling layer. Similar operations are repeated in subsequent blocks, Block 2, Block 3, and Block 4 with increasing numbers of filters 128, 256 and 512, respectively. The features extracted from the convolutional layers are concatenated with the features from the previous layers, and at third and fourth block, first and third convolution layers features are concatenated. This approach helps in preserving both low-level and high-level features throughout the network.

3.3 Manipulation CMFD

The 'Manipulation CMFD' model introduced is designed to precisely detect tampered regions within images. The model trained on input images paired with corresponding 'tampered binary masks', which specifically mark the areas of tampering within an image. The visual representation of input images and binary masks is illustrated in Figure 2. The process entails feature extraction via a VGG16 Feature Extractor, followed by up sampling of the feature maps to match the original image dimensions using a Mask Decoder. Subsequently, a Binary Classifier is applied to accomplish the auxiliary task of generating a manipulation mask as shown in Figure 1. ('Manipulation CMFD').

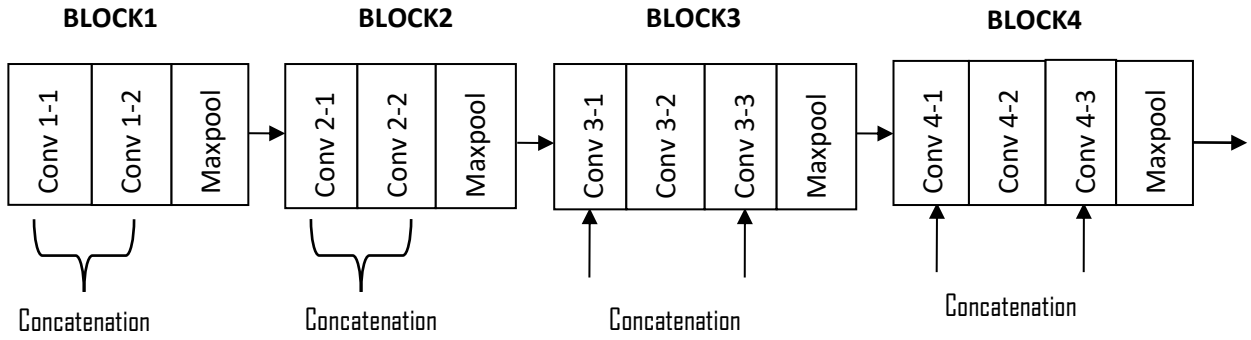

Fig 4: Proposed VGG16 Architecture for feature extraction

3.3.1 VGG16 Feature Extraction

In proposed approach, any CNN architecture can function Feature Extractor. In proposed approach, features are extracted VGG16 architecture as described in section 3.2. The resulting features at the fourth block are of size 16×16×512 tensor, possessing a considerably lower resolution than that required for the manipulation mask.

3.3.2 Mask Decoder

After feature extraction, a decoding process becomes imperative to restore the feature map to its original resolution i.e. 'upsampling'. This is achieved through deconvolution, as illustrated in Figure 3. The 16-fold increase in spatial dimensions is a consequence of employing upsmapling four times (i.e., 24=16). Furthermore, the output filter dimension of 6 is attributed to the final BN-Inception layer, which incorporates three Conv2D responses, each with 2 output filters and distinct kernel sizes of 5×5, 7×7, and 11×11 resulting in a concatenation of 3×2=6 filters [17]. After each upsampling operation, the number of filters is reduced gradually from 8 to 2. The final output of the deconvolution blocks is a tensor of size (256, 256, 6). Classification takes place at the prediction layer. Finally, the pixel-level manipulation is predicted through a Binary Classifier, implemented as a single Conv2D layer with 1 filter and a kernel size of (3,3) followed by sigmoid activation. This results in a final output tensor representing the predicted mask with a size of (256,256,1)

3.4 Similarity CMFD

The 'Similarity CMFD' model is developed to identify similar/ identical regions within images. During the training phase, the model receives input images along with corresponding binary masks, depicted in Figure 3. The model's workflow encompasses feature extraction, self-correlation, percentile pooling, and mask decoding processes, all aimed at classifying similar regions within the images.

3.4.1 VGG16 Feature Extraction

VGG16 pre-trained model is utilized for feature extraction, focusing on the first four blocks as shown in figure 1. Features are extracted as described in section 3.2. Feature extraction results in a tensor of size 16×16×512, representing patch-like features with 512 dimensions. Given the objective of identifying potential copy-move regions, it becomes imperative to extract pertinent information for discerning matched patch-like features. To achieve this, all-to-all feature similarity scores are computed using Self-Correlation, and meaningful statistics are gathered to identify matched patches via Percentile Pooling.

3.4.2 Correlation and Pooling

A self-correlation task is employed to compute feature similarity across the extracted features. Self-correlation calculates similarity scores across all feature pairs, resulting in a tensor of size 16×16×256. Percentile pooling is then applied to gather significant data, standardizing the score vector and removing input size dependency. Specifically, the Pearson correlation coefficient ρ is employed to quantify feature similarity between two patch-like features. The computation involves normalization of the features by subtracting the mean and dividing by the standard deviation. Consequently, Self-Correlation outputs a tensor of dimensions 16×16×256. Next, to effectively identify matched features, Percentile Pooling sorts the score vector in descending order and selects scores at predefined percentile ranks. This standardization not only removes the dependency on input size but also facilitates dimension reduction by retaining only a subset of scores.

3.4.3 Mask Decoder

Following Percentile Pooling, the Mask Decoder gradually upsamples [18] the pooled feature to the original image dimensions because the resulting feature tensor from correlation is of lower resolution than the manipulation mask requires, while the Binary Classifier generates a copy-move mask to fulfill the auxiliary task. Again, both the Mask Decoder and Binary Classifier maintain the same architecture as those in the 'Manipulation CMFD' but possess distinctive weights. This process generates a tensor of shape 256×256×6, with 6 filters representing concatenated Conv2D responses. Finally, a binary classifier, consisting of a single Conv2D layer followed by sigmoid activation predicts the pixel-level 'Similarity detected mask'. The model effectively detects tampered regions within images through feature extraction, correlation, and mask decoding. It provides a robust framework for identifying potential copy-move regions and generating accurate manipulation masks combining feature extraction, correlation, and mask decoding, the 'Similarity CMFD' model demonstrates strong performance in image similarity detection tasks.

3.5 Fusion CMFD

In the Fusion CMFD module (Figure 1) the Mask Decoder features from both branches, are utilized collectively to make the final Copy-Move Forgery Detection (CMFD) prediction which classifies genuine and tampered region, respectively. The process involves several steps, Fusion of features from 'Manipulation CMFD' and 'Similarity CMFD'. Firstly, the features obtained from the Mask Decoder of the 'Manipulation CMFD' and 'Similarity CMFD' branches, respectively, are concatenated. This concatenation combines the information extracted from both branches into a single feature representation. Then, the concatenated features undergo fusion using specific parameter set of 3[1,3,5]. The module integrates information from the concatenated features to enhance the representation by capturing both spatial and channel-wise dependencies. This fusion process ensures that relevant

information from both branches is effectively incorporated into the final feature representation. Finally, the fused features are used to predict the three-class CMFD mask. This prediction is accomplished using a Conv2D layer with a single filter of kernel size 3×3, followed by the softmax activation function. The softmax activation function normalizes the output probabilities across the three classes, namely background (blue color), genuine (green color), and tampered (red color), ensuring that the predicted mask accurately reflects the likelihood of each pixel belonging to each class. Even while training the 'Fusion CMFD' model follows the input images and binary masks are shown in figure 3. And the feature extraction model is given in figure 4 and section 3.2.

4. EXPERIMENTAL SETUP

The proposed novel approach is implemented using Python programming language, specifically version 3.11. for deep learning tasks, TensorFlow 2.0 is utilized. The system specifications include Windows 11, an Intel i5 12th generation processor, and 16GB of RAM.

Through extensive training and testing, the model has been fine-tuned to accurately discern tampered regions even amidst complex transformations such as rotation and scaling. These transformations mimic real-world scenarios where adversaries may attempt to obfuscate tampered regions through spatial alterations. By effectively identifying tampered and genuine areas despite such transformations, the model underscores its robustness and adaptability in combating forgery in digital imagery. The experimental results presented in Figure 6 and 7 not only validate the model's efficacy in detecting left-aligned tampering and cross validation but also emphasize its versatility in handling multiple types of image manipulations.

Following experimentation with various numbers of epochs, it is empirically observed that, proposed 'Manipulation CMFD', 'Similarity CMFD' and 'Fusion CMFD' model employing 100 epochs yields optimal results. The model's learning rate is fixed at 1e-2, and the loss function employed for computation is 'binary_crossentropy' for 'Manipulation CMFD', and 'Similarity CMFD' whereas, 'categorical_crossentropy' for 'Fusion CMFD'. Throughout the training process, the model iteratively adjusts its parameters to minimize the cross-entropy loss, leveraging the 'Adam' optimizer.

5. RESULTS

The experiment conducted using images from the MICC-F2000 dataset. Figure 5 illustrates the experimental outcomes. The first and second rows display the original images and their corresponding tampered versions from the dataset, respectively. The third and fourth rows highlight the ground truth and predicted masks, respectively. In the predicted mask, the red-colored regions represent the tampered areas within the image, while the green-colored regions indicate genuine areas. Furthermore, the last row provides evidence that the predicted masks accurately identify both genuine and tampered regions within the image. The accuracy of this identification is demonstrated by overlaying the predicted masks onto the input images.

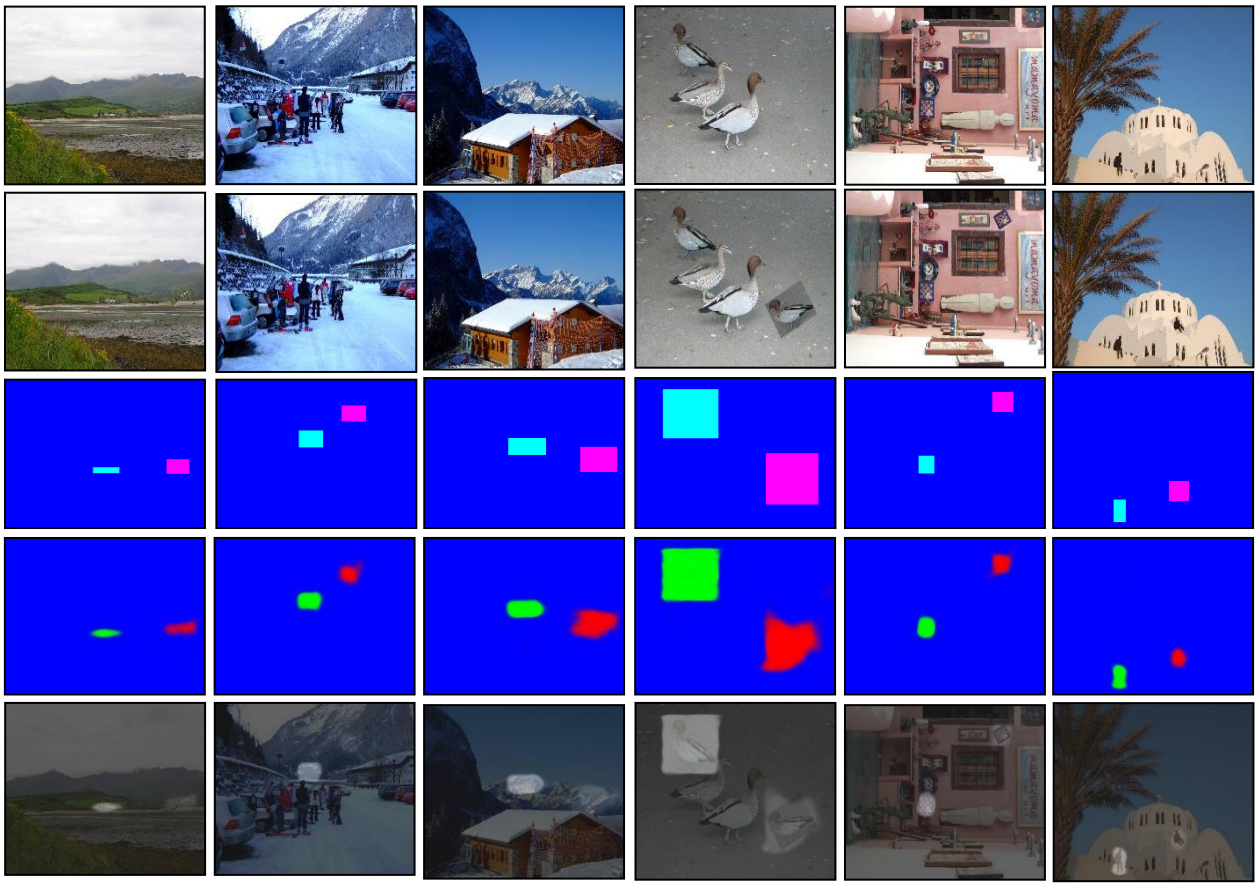

Fig 5: Experimental results performed on MICC-F2000 dataset

The proposed model is trained to detect various forms of forgery attacks, including rotation, scaling, and tampering across different regions of the image. It demonstrates efficiency in identifying a wide range of forgery attacks in images. The evaluation involved testing the model's performance against different scenarios, including right alignment tampering, left

alignment tampering, large scaling, minimum scaling, and combinations of rotation and scaling. Figure 5 presents sample images illustrating forgery with right alignment, scaling, and rotation. The tampered regions are situated to the right side of the image, as well as in the top and bottom regions.

Figure 6 illustrates the identification of left-aligned tampered regions, coupled with rotation and scaling, showcasing the comprehensive capabilities of the proposed model in detecting various forms of image manipulation.

Figure 7 is sample results of the proposed model where the model is trained on MICC-F2000 dataset and tested on MICC-F220 [2]. The manipulated section of the duplicated image appears randomly as either a rectangle or square within the image, with forgery attempts typically involving rotation or scaling techniques. Proposed model yields better testing results for MICC-F220 with all possible copy move forgery attacks given in image dataset.

6. DISCUSSION

Afterwards, the novel proposed method's performance analysis given in figure 8. Where (a) is training and validation accuracy and (b) is training and validation loss for 'Fusion CMFD' model. Whereas, (c) is training and validation accuracy and (d) is training and validation loss for 'Similarity CMFD' Model.

The 'Manipulation CMFD' model is specifically trained to identify tampered regions within an image, while the 'Similarity CMFD' model focuses on detecting cloned regions. The training and validation accuracy for the 'Similarity CMFD' model are notably high, reaching 99% and 98.11%, respectively. On the other hand, the 'Fusion CMFD' model not only detects tampered regions but also classifies them as genuine or tampered. Demonstrating robust performance, the Fusion CMFD model achieves training and validation accuracies of 99.28% and 98.30%, respectively, as illustrated in Figure 8.

The next step involves testing the proposed 'Fusion CMFD' model. Two cases are considered for testing. Case 1 entails determining whether an image has been tampered with, as well as accurately identifying genuine and tampered regions within the image. For this evaluation, a total of 100 images are employed, comprising 80 tampered and 20 non-tampered images. Figure 9 depicts the confusion matrix generated during the testing phase to discern tampered images. This is called as "anomaly detection" or "one-class classification". Remarkably, out of the 100 images, only one tampered image is erroneously classified as non-tampered, while all non-tampered images are correctly identified. The proposed model achieves an impressive accuracy of 99%, with a recall rate of 98.75% and precision reaching 100%.

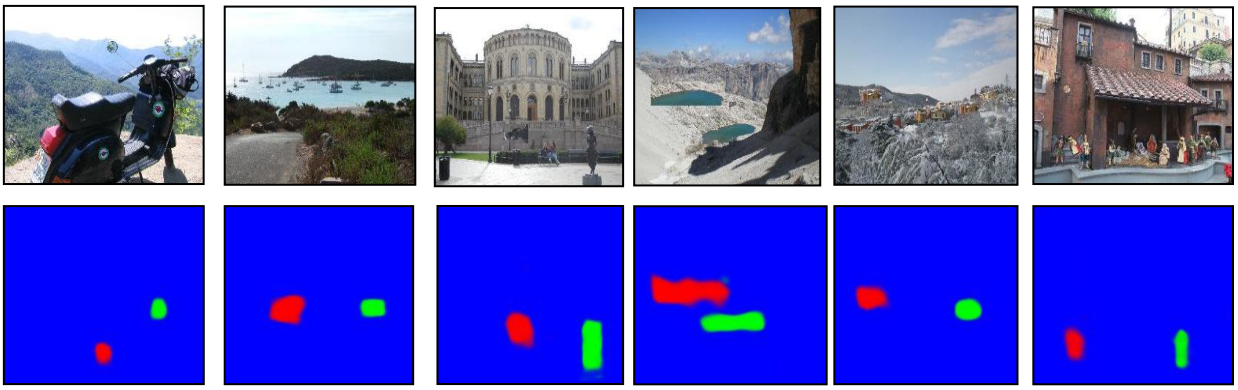

Fig 6: Left aligned tampering detected images from MICC-F2000 dataset (Row 1: Input Tampered image and Row 2: Predicted output image)

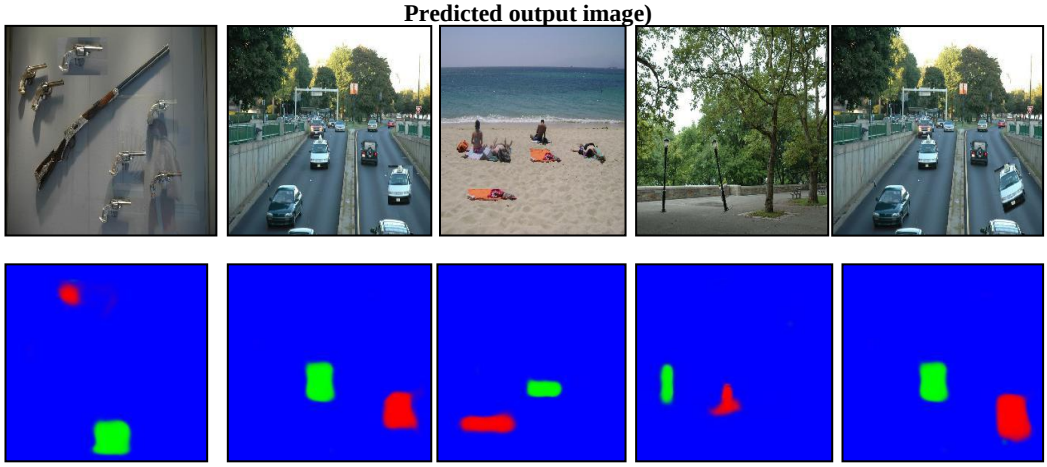

Fig 7: Sample images for cross validation from MICC-F220 dataset (Row 1: Input Tampered image and Row 2: Predicted output image)

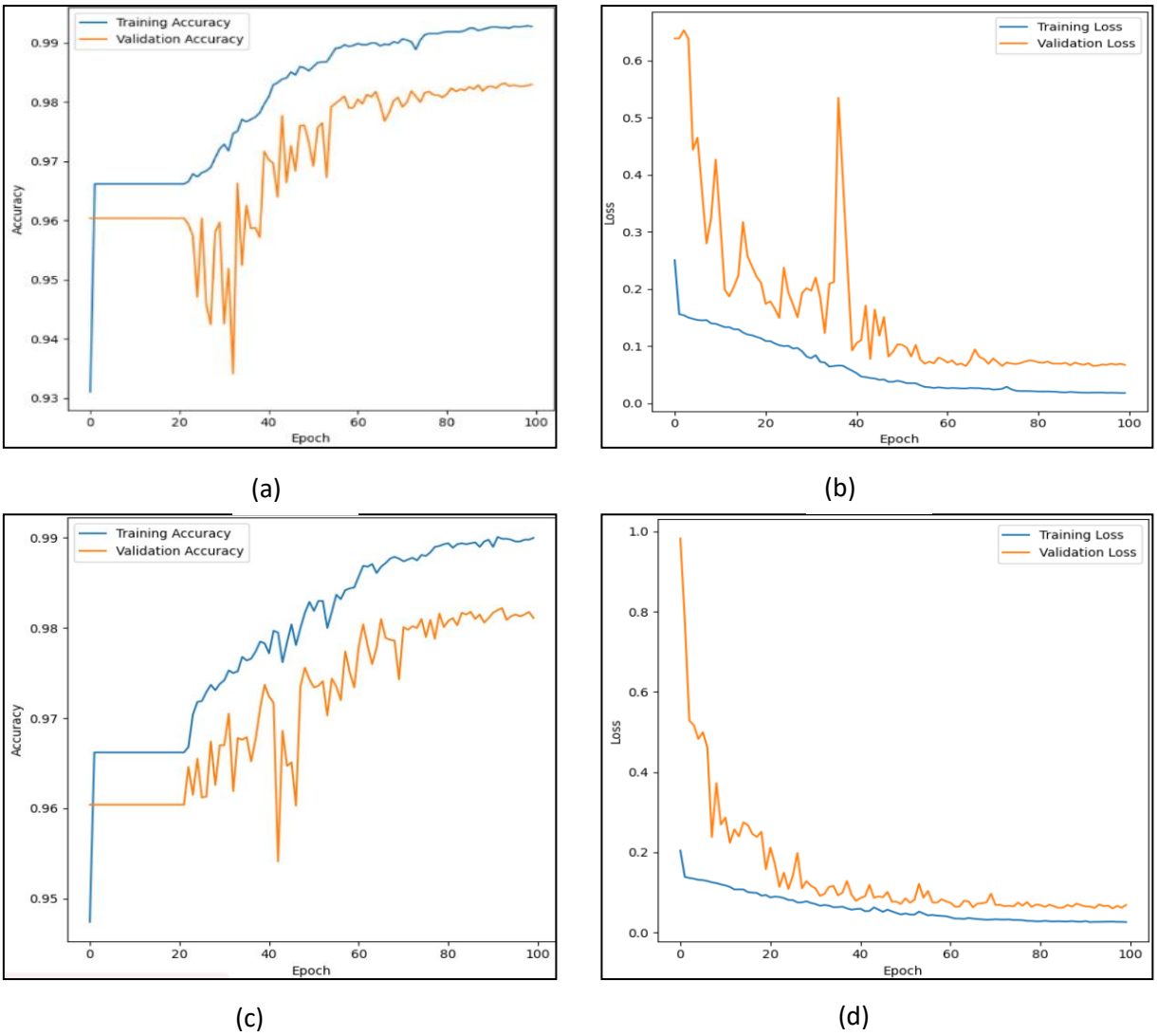

Fig 8 : Performance analysis of novel proposed approach for genuine and tampered region identification within an image

After successfully classifying between tampered and non-tampered regions, the next case, Case 2, involves precisely identifying the genuine Regions of Interest (ROIs) and delineating them in green, while marking tampered ROIs in red in the predicted binary mask. In this test scenario, the novel 'Fusion CMFD' model is evaluated using a dataset comprising 100 tampered images. Figure 10 illustrates the confusion matrix for discerning genuine and tampered regions within an image, a task commonly known as 'binary classification'. The confusion matrix reveals that out of the 100 images, only 2 exhibit discrepancies in identifying the genuine and tampered regions. Specifically, some genuine regions are misclassified as tampered, and vice versa, leading to a color swap in the predicted binary mask where green denotes tampered regions and red signifies genuine regions. Here, the labels '0' and '1' represent tampered and genuine regions within an image, respectively. The results of the proposed model's testing showcase an impressive 98% accuracy.

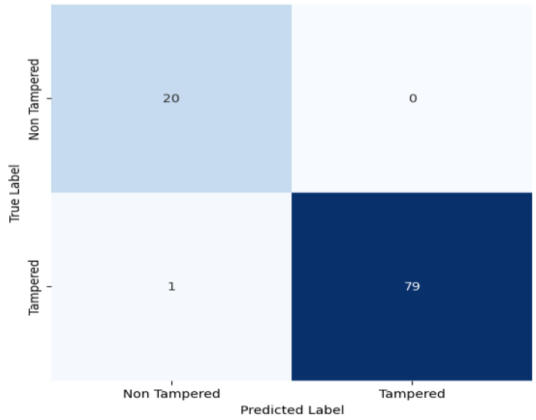

Fig 9: Confusion Matrix for classifying whether image is tampered or not

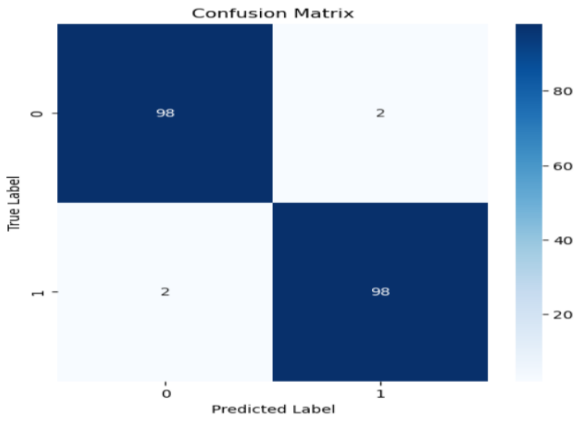

Figure 10. Confusion matrix for identifying genuine and tampered region within an image

For testing both the cases MICC-F2000 image dataset is used including various forgery attacks such as scaling and rotation. Afterwords the proposed method is compared with other existing methods The proposed method yields higher accuracy for the corresponding datasets. In Table 1, the proposed methods are compared with both single image forgery detection and deep learning-based forgery detection. The methods [24, 20, 25 and 31] refer to single image forgery and remaining represent the neural network approach. However, these methods only identify cloned regions within an image as 'Similarity CMFD' model.

Table 1 : Comparative Analysis for MICC-F2000 dataset

Author	Accuracy
Amerini [1]	94.86
Amerini [24]	93.42
Elaskily et. al [20]	98.40
Ye et.al. [25]	98.5
Ahmed Sedik et. al [28]	94
Vaishali, Sharma et. al [29]	97.63
Selvaraj et. al. [27]	69.75
Nidhi Goel et. al [14]	96
Thiiban M et.al [30]	76
Rajeev Rajkumar [12]	99
Elaskily et. al [31]	98.14
Proposed Method (Fusion CMFD)	**99**

In the Table 2, The other parameters as precision and recall are considered and compared with other state of art methods and proposed methods yields better result.

Table 2 : Analysis for MICC-F2000 dataset

Author	Precision	Recall
Nidhi Goel et al. [14]	89	100
Selvaraj et.al. [27]	89	94
Rodriguez-Ortega Y. et.al. [2]	78	79
Thiiban M et.al [30]	76	69
Rajeev Rajkumar [12]	97.84	99
Proposed Method (Fusion CMFD)	**100**	**98.75**

7. CONCLUSION AND FUTURE WORK

This study introduces an advanced approach to Copy-Move image forgery detection and image region classification, leveraging the powerful VGG16 architecture without the need for any reference image. The methodology proposed herein demonstrates significant potential in the realm of image forensics. By fusing the capabilities of 'Manipulation CMFD' and 'Similarity CMFD', the novel 'Fusion CMFD' model emerges, representing a robust solution to detect and classify tampered and genuine regions within images. The novel feature extraction technique, as illustrated in Figure 4, harnesses the deep learning capabilities of VGG16, where concatenated features from convolution layers and the initial four blocks of the network are utilized. The comprehensive methodology, outlined in Figure 1, underscores the systematic approach adopted in this study. Experimental evaluation, conducted on the MICC-F2000 tampered image dataset, showcases the superiority of the proposed method over existing techniques, demonstrating resilience against various Copy-Move image forgery detection (CMFD) attacks as scaling and rotation. Furthermore, the model's robustness is validated through cross-verification with the MICC-F220 dataset. With its demonstrated efficacy in handling large datasets, future research avenues may explore its application to diverse datasets and special case of copy move forgery where the uniform background regions without any objects has been copy pasted and provides robust methods in the field of forensic image analysis.

8. ACKNOWLEDGMENTS

The research work presented in this paper is supported by KFIST L2 project sanctioned to us by VGST, GoK.

9. REFERENCES

[1] Zanardelli, Marcello, et al. "Image forgery detection: a survey of recent deep-learning approaches." Multimedia Tools and Applications 82.12 (2023): 17521-17566.

[2] Rodriguez-Ortega, Y.; Ballesteros, D.M.; Renza, D. Copy-Move Forgery Detection (CMFD) Using Deep Learning for Image and Video Forensics. J. Imaging 2021, 7, 59. https://doi.org/10.3390/ jimaging7030059

[3] D. Prabakar, R. Ganesan, D. L. Rani, P. Neti, N. Kalyani and S. K. Mudradi, "Hybrid Deep Learning Model for Copy Move Image Forgery Detection," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 1023-1028, doi: 10.1109/I-SMAC55078.2022.9987319.

[4] Ibrahim A. Zedan, Mona M. Soliman, Khaled M. Elsayed, Hoda M. Onsi, "A New Matching Strategy for SIFT Based Copy-Move Forgery Detection", International Journal of Intelligent Engineering and Systems · June 2023 DOI: 10.22266/ijies2023.0831.34

[5] Wenyu Chen, Yanli Zhao, Wenzhi Xie and Nan Sang, "An improved SIFT algorithm for image feature-matching," 2011 International Conference on Multimedia Technology, Hangzhou, 2011, pp. 197-200, doi: 10.1109/ICMT.2011.6003022.

[6] G. G. Rajput and S. B. Ummapure, "Script identification from handwritten documents using SIFT method," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 2017, pp. 520-526, doi: 10.1109/ICPCSI.2017.8392348

[7] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Luca Del Tongo, Giuseppe Serra, Copy-move forgery detection and localization by means

of robust clustering with J-Linkage, Signal Processing: Image Communication 28(2013) 659–669

[8] Deb, P., Kar, N., Hassan, K.L. et al. Advanced copy-move forgery detection: utilizing AKAZE in conjunction with SIFT algorithm for image forensics. Microsyst Technol (2024). https://doi.org/10.1007/s00542-024-05773-1

[9] K. M. Hosny, A. M. Mortda, M. M. Fouda and N. A. Lashin, "An Efficient CNN Model to Detect Copy-Move Image Forgery," in IEEE Access, vol. 10, pp. 48622-48632, 2022, doi: 10.1109/ACCESS.2022.3172273.

[10] Azra Parveen, Zishan Husain Khan, Syed Naseem Ahmad, "Block-based copy–move image forgery detection using DCT", Iran Journal of Computer Science https://doi.org/10.1007/s42044-019-00029-y, Received: 22 June 2018 / Accepted: 8 January 2019 © Springer Nature Switzerland AG 2019

[11] Chengyou Wang , Zhi Zhang and Xiao Zhou, "An Image Copy-Move Forgery Detection Scheme Based on A-KAZE and SURF Features", Symmetry 2018, 10, 706; doi:10.3390/sym10120706

[12] Rajkumar, R., 2023. Deep Learning Feature Extraction Using Attention-Based DenseNet 121 for Copy Move Forgery Detection. International Journal of Image and Graphics, 23(05), p.2350042.

[13] Esha Tripathi, Upendra Kumar, Surya Prakash Tripathi, "Comparative Analysis of Techniques Used to Detect CopyMove Tampering for Real-World Electronic Images", INTERNATIONAL JOURNAL OF INTEGRATED ENGINEERING VOL. 15 NO. 4 (2023) 201-225

[14] Nidhi Goel, Samarjeet Kaur, Ruchika Bala, Dual branch convolutional neural network for copy move forgery detection, IET Image Processing

[15] Nagaveni K. Hebbar and Ashwini S. Kunte, "Transfer Learning Approach For Splicing And Copy-Move Image Tampering Detection", Ictact Journal On Image And Video Processing, MAY 2021, VOLUME: 11, ISSUE: 04ISSN: 0976-9102 (ONLINE) DOI: 10.21917/Ijivp.2021.0348

[16] Asghar, Khurshid & Sun, Xianfang & Rosin, Paul & Khatana, Mubbashar & Hussain, Muhammad & Habib, Zulfiqar. (2019). Edge–texture feature-based image forgery detection with cross-dataset evaluation. Machine Vision and Applications. 30. 10.1007/s00138-019-01048-2.

[17] Noh, H., Hong, S., Han, B.: Learning deconvolution network for semantic segmentation. In:Proceedings of the IEEE International Conference on Computer Vision. pp. 1520–1528 (2015)

[18] Wojna, Z., Ferrari, V., Guadarrama, S., Silberman, N., Chen, L.C., Fathi, A., Uijlings, J.: The devil is in the decoder (2017)

[19] Long, J., Shelhamer, E., Darrell, T.: Fully convolutional networks for semantic segmentation. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. pp. 3431–3440 (2015)

[20] Elaskily, M.A., Elnemr, H.A., Dessouky, M.M. et al. Two stages object recognition based copy-move forgery detection algorithm. Multimed Tools Appl 78, 15353–15373 (2019). https://doi.org/10.1007/s11042-018-6891-7

[21] Osamah M. Al-Qershi,Bee Ee Khoo, "Enhanced block-based copy-move forgery detection using k-means clustering", Multidimensional Systems and Signal Processing, © Springer Science+Business Media, LLC, part of Springer Nature 2018

[22] Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. CoRR abs/1409.1556 (2014)

[23] Kaur, N., Jindal, N. & Singh, K. A deep learning framework for copy-move forgery detection in digital images. Multimed Tools Appl 82, 17741–17768 (2023). https://doi.org/10.1007/s11042-022-14016-2

[24] Irene Amerini; Lamberto Ballan; Roberto Caldelli; Alberto Del Bimbo; Giuseppe Serra ,"A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery", IEEE Transactions on Information Forensics and Security (Volume: 6, Issue: 3, September 2011)

[25] Ye, W., Zeng, Q., Peng, Y. et al. A two-stage detection method of copy-move forgery based on parallel feature fusion. J Wireless Com Network 2022, 30 (2022). https://doi.org/10.1186/s13638-022-02112-8

[26] Tralic D., Zupancic I., Grgic S., Grgic M., "CoMoFoD - New Database for Copy-Move Forgery Detection", in Proc. 55th International Symposium ELMAR-2013, pp. 49-54, September 2013

[27] Selvaraj, Arivazhagan & Shebiah, Newlin & M, Saranyaa & R, Shanmuga. (2024). CNN-based Approach for Robust Detection of Copy-Move Forgery in Images. Inteligencia Artificial. 27. 80-91. 10.4114/intartif.vol27iss73pp80-91.

[28] Ahmed Sedik, Yassine Maleh, Ghada M. El Banby, Ashraf A.M. Khalaf, Fathi E. Abd El-Samie, Brij B Gupta, Konstantinos Psannis, Ahmed A. Abd El-Latif, AI-enabled digital forgery analysis and crucial interactions monitoring in smart communities, Technological Forecasting and Social Change, Volume 177, 2022, 121555, ISSN 0040-1625,

[29] Vaishali, Sharma & Neetu, Singh. (2023). Enhanced copy-move forgery detection using deep convolutional neural network (DCNN) employing the ResNet-101 transfer learning model. Multimedia Tools and Applications. 1-25. 10.1007/s11042-023-15724-z.

[30] Muniappan, T. ., Abd Warif, N. B. ., Ismail, A. . and Mat Abir, N. A. . (2023) "An Evaluation of Convolutional Neural Network (CNN) Model for Copy-Move and Splicing Forgery Detection", International Journal of Intelligent Systems and Applications in Engineering, 11(2), pp. 730–740.

[31] Elaskily, M.A., Alkinani, M.H., Sedik, A. and Dessouky, M.M., 2021. Deep learning based algorithm (ConvLSTM) for copy move forgery detection. Journal of Intelligent & Fuzzy Systems, 40(3), pp.4385-4405.