International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

Image Forgery Detection Using Deep Learning-Based Stable Keypoint Feature Extractor and Multiscale Caswide Residual Networks

X. Tubax[1], Dr. A. Yesu Raja[2]

Submitted: 10/04/2024 **Revised:** 27/05/2024 **Accepted:** 08/06/2024

Abstract: Today, when the advancement of manipulation techniques has great speed, the ability to detect the image forgery becomes extremely important for maintaining the probity and reliability of the digital content. In this work, we propose a Deep Learning (DL) framework composed of a Stable Keypoint Feature Extractor to effectively select robust features, and Multiscale CASWide Residual Networks for accurate and dependable classification. Additionally, the Stable Keypoint Feature Extractor designed to reliably detect forgery prone regions, and the multiscale architecture to learn intricate global and local patterns for better forgery type detection encompassing copy-move, splicing and AI generated manipulations. The system is found to be resilient to noisy and compressed speech, compression artifacts, and various geometric transformations and in doing so, outperforms current methods in terms of robustness and scalability. Its efficiency is validated by extensive experimental results on benchmark datasets to achieve improved accuracy with reduced false positives. Proposed methods achieve 91.45 % accuracy in feature selection and 92.46% accuracy in classification. These results demonstrate the promise of using this adaptable and computationally efficient framework to deploy digital forensics, content authentication, and real time forgery detection in security critical applications.

Keywords: *Classification, Feature selection, Image forgery, Multiscale analysis, Residual network*

I Introduction

In today's technologically booming digital age, visual content has exploded in growth and accessibility. With this proliferation comes also a large concern, as is the authenticity of visual content. Trust in visual evidence is critical, so journalism, forensic investigation, and social media are especially susceptible. Altering minor elements down to wholly constructing new scenes are all possible image manipulations, forcing offers to guarantee authenticity of visual content. The complexity of image forgery detection has been further amplified by copy-move forgeries, splicing, as well as more advanced Generative Adversarial Networks (GANs) [1], [2]. The problem of reliably detecting forged images has proven to be difficult and efforts continue to this day [3-5]. At the same time, notwithstanding various solutions offered so far, the problem of detecting forged images grows more challenging as the tampering techniques become increasingly sophisticated.

To solve this problem, researchers looked into several feature extraction and classification strategies that are being developed in the field of computer vision and Machine Learning (ML) [6], [7]. In terms of feature extraction, from keypoints [8], these methods create stable and invariant features of the fundamental characteristics of an image [9]. They aim to be resilient to being scaled, rotated, and noisy. However, these extracted features are being used by the classification models to identify the authentic images from manipulated ones [10–13]. Yet, existing techniques often generalize poorly, especially at scale [14], [15].

We propose a new framework for image forgery detection, combining advanced feature selection and classification algorithms with state of the art performance. The proposed framework includes the Deep Learning Based Stable Key point

Research Scholar (Reg. No: 21213092281007)

Assistant Professor

1,2PG & Research Department of Computer Science, Muslim Arts College,

Thiruvithancode, Kanyakumari -629174, India (Affiliated by Manonmaniam Sundaranar University, Tirunelveli)

Email 1, 2: tubaxon@gmail.com; a_yesuraja@yahoo.co.in

Feature Extractor (DLSK) as its first core component. For detecting and describing stable keypoints in images highly repetitively, DLSK uses Deep Convolutional Neural Networks (CNNs). The proposed method obtains robust feature representation which is invariant for geometric transformations and noise; it solves the issues that have been apparent in traditional keypoint detection methods [16-18].

Multiscale CASWide Residual Networks (MCWRNs) are the second component, classification architecture. Multiscale feature extraction combined with widened residual network architecture allows MCWRNs to take advantage of both fine grained details and global features of the image. The proposed architecture consists of cascaded wide residual blocks working at different scales, enabling comprehensive study of the forged image content. Thus, MCWRNs avoid drawbacks of the traditional classifiers, which usually miss some subtle hints to tampering [19-21].

We present a framework based on the integration of DLSK and MCWRNs that provides a consistent and accurate image forgery detection system. We evaluate it extensively on benchmark datasets and demonstrate significant improvement of its precision, recall, and classification accuracy over state-of-the-art methods. Previous research has been conducted on feature extraction or classification in contrast, this research shows how utilizing the feature selection approaches and the sophisticated classification systems intertwined provide a complete solution to the picture fraud detection problem [22-24]. This work provides support for the need to deploy novel techniques to preserve the integrity of digital images amid a proliferating corruption of our world.

Contribution of the paper: In this paper, we present an innovative framework for image forgery detection based on Deep Learning based Stable Keypoint feature extraction (DLSK) for feature selection robustness and Multiscale CASWide Residual Networks (MCWRNs) for feature classification effectiveness. Existing methods are shown to be bounded by limitations and the methodology offered is resistant to transformations and captures fine-grained and overall patterns in forgeries. Extensive evaluations on benchmark datasets show superior performance and make for a reliable system for digital image authenticity verification.

Organization of the paper: In this paper the related work and problem identifications are discussed in section 2. In section the feature selection and classification methods are discussed in detail. In section 4 the results and discussed are added. In section 5 the conclusions are discussed.

II Background Study

Agarwal & Chand [25] one approach to image fraud detection using an entropy filter and a Local Phase Quantization (LPQ) texture operator has been covered by Authors. The entropy filter helps to highlight unpredictable picture changes to aid identify the fake component. The internal statistics of this entropy filtered image is computed using the LPQ operator and it helps in classification of forged and non forged images. Their technique can successfully degrade both copy-move and spliced images.

Agarwal & Jung [26] Due to advanced computational technology and software applications, fake images forensics proved to be rather complex. Authors have retrieved characteristics in the spatial and frequency domains after transforming Red (R), Green (G), and Blue (B) (RGB) permutations into Y: Luminance, Cb: Chroma Blue, Cr: Chroma Red YCbCr colour space. An application of a shift-invariant non-decimated wavelet transform domain was made in the frequency domain. The feature vector dimension was reduced and efficiency improved using the infinite feature selection approach. Authors tested the suggested method on four different images forgeries datasets to see how it worked.

Ahmed et al. [27] Copy move image detection utilizing various texture feature extraction techniques and classifiers was the main emphasis of their work. The procedure begins with image preprocessing, continues with image splitting, and finally applies algorithms for texture feature extraction. The three texture features extraction techniques are Segmentation based fractal texture analysis, local binary pattern and Haralick. The given feature values are given to these three distinct classifiers as being classified between forged and authentic images using K Nearest Neighbors (KNN), Naïve Bayesian, and Logistic classifiers.

With no attacks, random feature selection is not too inefficient, but it greatly improves security determined by Chen et al [28]. Some theoretical findings in a simplified model were provided initially by authors. The next step was to use Support Vector Machine (SVM) classification with the Subtractive Pixel Adjacency Matrix (SPAM) feature set to apply their technique to the identification of two image manipulations: Computed mean value, adaptive histogram equalization and median filtering. The security study, which involves targeting those two detectors in both the feature and pixel domain, demonstrates that random feature selection can enhance security, doing so in fact better than the more elementary theoretical analysis shows.

Guo et al. [29] authors create a solution that works in the fields of Convolutional Neural Network (CNN) synthesis and image editing forgeries. In order to categories the individual forgery methods of provided photos, the algorithm must forecast the complete hierarchical route; this was how authors construct the Image Forgery Detection and Localization (IFDL) as a hierarchical fine-grained classification issue.

This modern era threats of digital image alteration are tackled by Kaushik & Kandali [30] in these authors research study by developing a reliable method for detection of copy move image forgeries. By combining CNN based deep features with gray level co occurrence matrix (GLCM) features, this innovative method performs better than previous methods in identifying copy move forgeries. Using the Neighborhood Component Analysis (NCA)-selected hybrid features on maximizing the discriminative capability of the set of features. Next, the SVM classifier is able to successfully sort the de-emphasized hybrid characteristics to ensure accurate fraud detection.

Meena & Tyagi [31] authors take a look at some of the current approaches to blind image fraud detection. Image forgery detection methods are categorized broadly. Image splicing, copy-move, resampling, and retouching detection are the four primary methods of forgery detection that are detailed in this article. After looking at a variety of ways in each area, authors can see that current strategies have at least one of these drawbacks. First, good detection accuracy; second, complicated processing required; and third, susceptible to a variety of techniques, including scaling, rotation, blurring, Joint Photographic Experts Group (JPEG) compression, brightness change, and scaling.

Novel feature selection method was refined such as to tackle the categorization of manually made fake - face photos as reported by Mitral et al. [32]. First, the pre-trained AlexNet, in suggested method’s deep learning model, is used to extract an image’s characteristics. The extracted features are assessed through the proposed enhanced quantum inspired evolutionary algorithm in order to determine the best subset of characteristics. Finally, the evoked feature subset was classified by the KNN classifier with 10-fold cross validation.

Saleh et al. [33] authors provided a comprehensive review of an approach for detecting image forgeries that was based on multi-scale Weber local descriptors (WLD). Colour images' chrominance channels are mined for WLD characteristics. SVMs are used for the purpose of classification. Results obtained by the counterfeit detection approach using CASIA v1.0, CASIA v2.0, and Columbia colour image databases are as follows: 94.19%, 96.61%, and 94.17%, respectively. In comparison to other findings published in these databases, their accuracies are superior. With the exception of CASIA v2.0, the results obtained by fusing Cb and Cr channels are competitive with one another.

Walia et al. [34] DL methods are well known to be able to tackle classification problems by offering the information required to generate high-level features. Furthermore, hand-crafted and painstakingly thought out elements taken from hand-crafted images provide quite good outcomes. Nevertheless, after much testing, attackers still have the advantage in terms of forgery detection over modern DL methods and manually built features. Their work so proposes a novel approach used RGB colour space and brightness channels to identify digital photo forgeries by feature fusion.

Table 1: Comparison table on Feature selection and classification for image forgery Detection

Reference	Methodology/Algorithm	Dataset Used	Advantages	Key Contributions
Balasubramanian et al. [35]	Cascaded Deep Sparse Auto-Encoder	Custom dataset for deep fakes	Handles high-dimensional data efficiently, improves feature selection for deep fakes.	Novel feature selection mechanism for deep fake detection using cascaded sparse auto-encoders.
Luo et al. [36]	Localized Forgery Detection in Hyperspectral Images	Hyperspectral document datasets	High accuracy in detecting forgeries in document images with hyperspectral data.	Focused on hyperspectral document images for detecting localized forgery regions.
Qazi et al. [37]	Deep Learning-Based Detection System	CASIA v2.0, Columbia Image Splicing	Robust to cross-dataset variations, handles diverse types of forgeries.	Developed a CNN-based forgery detection system and evaluated cross-dataset performance.
Sudiatmika et al. [38]	Error Level Analysis and Deep Learning	Custom dataset, MICC-F220	Effectively integrates error-level analysis with deep learning for better results in forgery detection.	Integrated error-level analysis with a CNN-based deep learning model for improved forgery detection.
Deep Kaur & Kanwal [39]	Analysis of Detection Techniques	NA	Provides a comprehensive understanding of forgery detection techniques.	Comprehensive analysis and comparison of existing forgery detection techniques.
Rhee [40]	Ground Truth Generation for Copy-Move Forgery Detection	CASIA, MICC-F600	Generates accurate ground truth for forgery detection using semantic segmentation.	Introduced a method for generating ground truth with image classification and semantic segmentation.
Li et al. [41]	Residual-Based Features	CASIA, CoMoFoD	Highly effective in detecting subtle manipulations in images.	Proposed a residual feature-based system for identifying image manipulations.

2.1 Problem Identification

With new advanced image manipulation techniques, such as deep fakes, splicing, and copy move forgeries, we are extremely limited in our ability to ensure the authenticity of digital images. Existing detection methods tend to be no robust and lack scalability to general datasets and to design schemes with subtle tampering patterns.

III Materials And Methods

In this paper we are using image forgery dataset for detecting forgeries. For feature selection we are using Deep Learning-Based Stable Keypoint Feature Extractor and for classification we using Multiscale CASWide Residual Networks in image forgery detection process. The process is shown in figure 1.

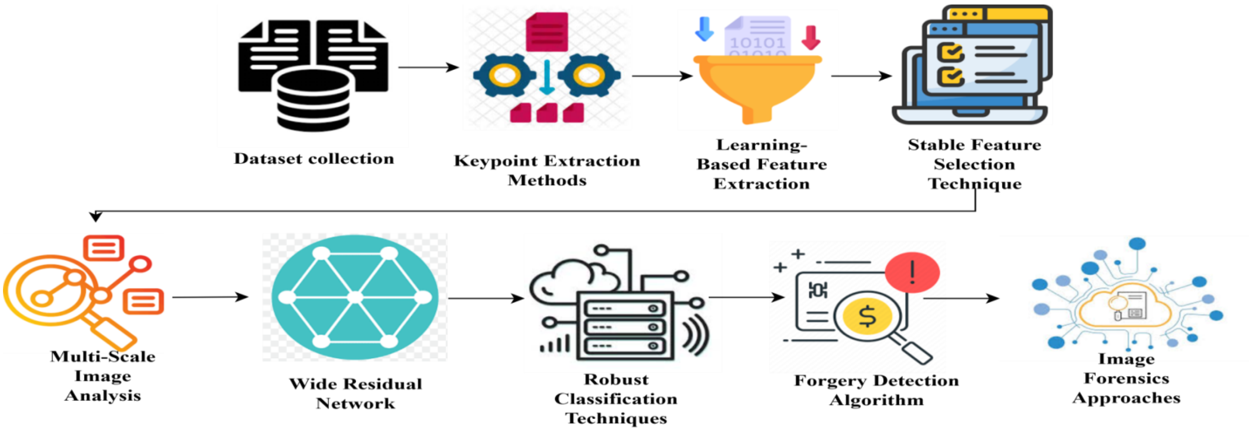
Dataset collection
Keypoint Extraction Methods
Learning-Based Feature Extraction
Stable Feature Selection Technique
Multi-Scale Image Analysis
Wide Residual Network
Robust Classification Techniques
Forgery Detection Algorithm
Image Forensics Approaches

Figure 1: Overall Image forgery detection process

3.1 Dataset

In the Kaggle "Image Forgery Detection" dataset, there is a collection of images (original and tampered alike) for modeling and testing image forgery detection models. It provides a varied set of manipulation techniques (copy move and splicing) that provide plenty of data to train and to evaluate on forgery detection tasks.

Dataset: https://www.kaggle.com/datasets/labid93/image-forgery-detection

3.2 Preprocessing

In the Deep Learning Based Stable Keypoint Feature Extractor (DLSK), one very important step in preprocessing is preparing image *I* ready for further analysis. Normalization normalizes the pixel intensity values to a normal behave like their values lie within a particular range like in let's take [0, 1] and [-1, 1] to prevent Illumination variation and contrast differences. The image can even be resized to be compatible with the input dimensions of our neural network. In order to get some better quality of image some additional techniques (like noise reduction for example implementation Gaussian Blur) or histogram equalization can be implemented. The intended of these steps include making the features consistent (to reduce variations), discard elements that are unimportant and adjust the image with a focus of making CNN able to detect key point.

3.3 Feature Selection using Deep Learning-Based Stable Keypoint Feature Extractor (DLSK)

As a breakthrough technique for detecting forgeries, the Deep Learning-Based Stable Key point (DLSK) Feature Extractor was developed to identify and analyze image features. It differs from classic feature extraction methods like SIFT (Scale Invariant Feature Transform) or SURF (Speeded Up Robust Features), that depend on hand crafted techniques, and instead utilize deep learning to discover stable key points and create robust feature descriptors. These are descriptors invariant under scaling, rotation, illumination variations and noise, so they are especially useful in detecting complex forgery types such as copy move, splice and retouch.

According to Bayar & Stamm [42] deep neural network is used to detect keypoints in DLSK, mostly Convolutional Neural Networks (CNNs). The CNN does not require image gradients (as traditional methods do); the CNN learns feature representations directly from the data. A region of interest in an image that exhibits distinctive patterns, e.g., corners or texture rich areas, is called keypoints. A descriptor is allocated to each keypoint that is detected. Local image properties, for example intensity gradients and texture, are encoded in a descriptor—a vector. Traditional descriptors are more representative and discriminative than the descriptors used by DLSK in which DLSK uses a CNN to obtain these. As a result, when DLSK decides to learn only the most relevant descriptors, computational load is reduced, and accuracy is improved. The discrepancies between the query and reference image are matched on selected features between the two. It can then check in some similarity metrics such as Euclidean distance or some more advanced one like cosine similarity.

Feature selection process:

Convert the input image to grayscale if necessary, normalize pixel values, and resize to a fixed resolution (e.g., 256×256 pixels). Apply filters (e.g., Gaussian filter) to remove noise without losing important details. A CNN processes the image and generates a feature map (e.g., F of size 64×64×128). Keypoints are identified as local maxima or regions of interest in the feature map, determined by:

$$K = \{(a, b) | F(a, b) > F(a + i, b + j), \forall\, i, j \in \{-1,0,1\}\} \text{ -------- } (1)$$

Here, (a, b) are the coordinates of the keypoint, and $F(a, b)$ is the response at that location. Stability is ensured by filtering keypoints based on their response strength and invariance to transformations. Equation (1) allows identifying the stable and distinct points (key points) of the image that remains constant even under scaling, rotation, and illumination transformation. This way ensure only select good points in the image that will hopefully never change, for instance at edges, corners and distinctive textures. These key points are stable under transformation resulting in the usefulness for forgery detection.

For each detected key point, a descriptor is extracted using a CNN. The CNN processes the region surrounding the key point to produce a vector D_k:

$$D_k = F_{CNN}(I, K_k) \text{ ------- } (2)$$

Where the input image is I , K_k is the keypoint, and F_{CNN} is the descriptor generation function. Descriptors are typically high-dimensional (e.g., 512 or 1024 elements), representing local patterns like texture and gradient information. These descriptors are invariant to transformations and are the core representation used for matching and forgery detection.

Dimensionality reduction (Van & Hinton [43]) techniques, such as Principal Component Analysis (PCA), are applied to minimize descriptor size while retaining important information:

$$D_k' = PCA(D_k) \text{ --------- } (3)$$

Where D_k' is the reduced descriptor. Criteria such as entropy, variance, or stability are used to select the most relevant descriptors. It reduces the computational costs and noise while preserving the discriminative power of the descriptors. Given two descriptors D_i and D_j:

$$similarity = 1 - \frac{D_i \cdot D_j}{||D_i||||D_j||} \text{ --------- } (4)$$

Equation (4) compares the orientation of two descriptors in the feature space and, based on this feature, to measure the similarity between two descriptors. Because this does not make use of absolute values but concentrates on relative orientation, it is very useful for comparing descriptors and insensitive to scale changes. A lower similarity score indicates higher likelihood of forgery.

This detects inconsistencies by comparing descriptors that come from input image and descriptors of a reference dataset. Matching is done using a similarity metric, typically the Euclidean distance:

$$Distance\ (D_i, D_j) = \sqrt{\sum_{k=1}^{n}(D_{i,k} - D_{j,k})^2} \text{ ------- } (5)$$

A threshold τ is applied to the distance values. Matches with distances above τ are flagged as potential forgeries. Detected discrepancies are mapped back to the image, highlighting manipulated regions. If $Distance\ (D_i, D_j) > \tau$ the flag is forgery. A clear decision boundary to classify descriptor matches is offered by thresholding of that score, trading off sensitivity and specificity in forgery detection.

However, DLSK is a change in approach to image forgery detection relying on deep learning that gets around traditional methods' problems. It provides a robust feature extraction and selection process which guarantees high and scalability and adaptability capabilities to modern forensic challenges.

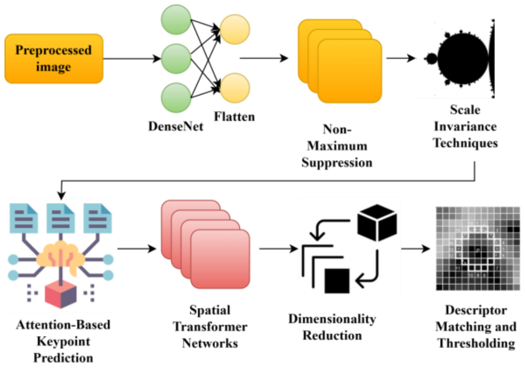
Preprocessed image
DenseNet
Flatten
Non-Maximum Suppression
Scale Invariance Techniques
Attention-Based Keypoint Prediction
Spatial Transformer Networks
Dimensionality Reduction
Descriptor Matching and Thresholding

Figure 2: Deep Learning-Based Stable Key point workflow

Figure 2 presents a Deep Learning-Based Stable Key point (DLSK) Feature Extractor workflow. First we have the preprocessed input image and then we extract features using layers such as denseNet, flatten, and fully connected layers to spot the key points. Then, stable key points are filtered by non-maximum suppression. For these key points, CNN based descriptors are created, which are then further decriptorised. Matching and comparison are used to detect manipulated regions or inconsistencies, and stability and invariance to transformations are provided to ensure it.

Algorithm 1: Deep Learning-Based Stable Keypoint Feature Extractor

```
Input: Image I
Process:
Step 1: Preprocess Image:
    I' = Normalize (I)
Step 2: Keypoint Detection:
    F = CNN (I')
    $K = \{(a,b) | F(a,b) > F(a+i, b+j), \forall\, i,j \in \{-1,0,1\}\}$
    Filter $K$ for stable key points under transformations.
Step 3: Descriptor Generation:
    for each $K_k$ in K:
        $P_k$ = ExtractPatch(I', $K_k$)
        $D_k$ = CNN ($P_k$)
Step 4: Dimensionality Reduction:
    Apply PCA on all $D_k$ to get $D_k'$
Step 5: Descriptor Matching:
    for each pair ($D_i'$, $D_j'$):
        Compute Similarity = 1 - ($D_i'$ •$D_j'$) / (||$D_i'$|| ||$D_j'$||)
        Compute Distance = $\sqrt{\sum_{k=1}^{n}(D_{i,k} - D_{j,k})^2}$
Step 6: Forgery Detection:
    if Distance > τ:
        Flag as forgery.
Step 7: Forgery Localization:
    Map mismatched descriptors back to image regions.
Return R (manipulated regions)
Output: Forgery detection map R
```

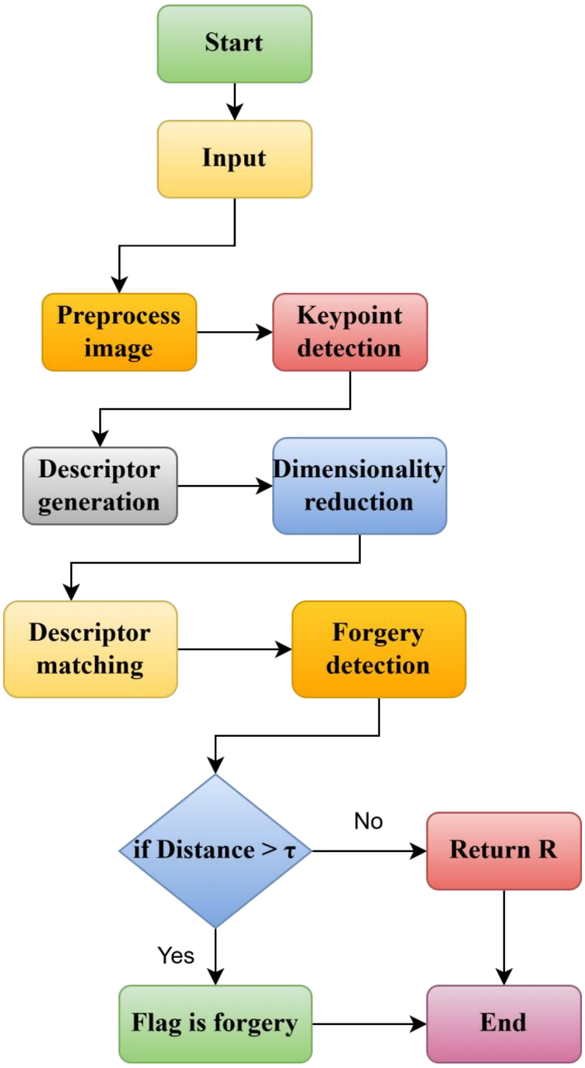

Figure 3: Flowchart of Deep Learning-Based Stable Keypoint Feature Extractor

Algorithm 1 and figure 3 depicts the Deep Learning Based Stable Keypoint Feature Extractor

(DLSK) suggests this for detecting and localizing image forgeries. It starts with normalizing the input image and detects the stable keypoints using a CNN and a non maximum suppression. CNN based patches are used to generate keypoint descriptors reduced by PCA and matched using similarity and distance metrics. If any discrepancies are greater than some threshold τ are flagged as forgeries and the mismatched descriptors are mapped back to the image to locally detect the forgeries, producing a forgery detection map R.

3.4 Classification using Multiscale CASWide Residual Networks (MCWRNs).

The contribution is advanced deep learning architectures for high accuracy and robustness on image forgery detection and classification, known as Multiscale CASWide Residual Networks (MCWRNs). To be able to detect such faint manipulation clues, they use multiscale processing and observe global and local patterns in different resolutions. CAS, by assigning attention weights to identify different feature channels, utilizes discriminative feature information (edges, textures and gradients) to disambiguate. Residual Connections provide the ability to learn, and keep, and refine features that are discarded in previous layers in traditional designs, whilst the Wide Residual Learning enables efficient training on these wider feature maps. The features extracted from multi–scales are combined to obtain a comprehensive representation for the purposes of classification tasks. Such real world forgery detection scenarios appear to favor the architecture, which is computationally efficient, resistant to multiple types of forgeries (splicing, retouching, copy-move), and feasible for different image sizes and resolutions.

The input image I undergoes preprocessing, including normalization and resizing. The preprocessed image is then split into multiscale patches:

$$I_s = Resize\ (I, s), s \in \{1,21,41\} \quad \text{-------} (6)$$

Each scale captures features at a different level of detail. In equation (6) the input image I is resized to different scales (s) to create multiscale patches (I_s), capturing features at various levels of detail. This equation is address forgeries that occurs at different spatial resolutions

In particular, we exploit the fact that many forgeries currently in the wild, such as splicing, copy-move and retouching, generally occur at different spatial resolutions, which we analyze at. In MCWRN:

- The image is processed at multiple scales (e.g., full resolution, half, and quarter resolution).
- Conv2D filters are applied at each scale to extract features FsF_sFs, ensuring both coarse and fine-grained patterns are captured.

Multiscale processing enables the network to (Simonyan [45]):

- Identify global inconsistencies (e.g., lighting variations across the image).
- Detect local irregularities (e.g., pixel-level mismatches in spliced regions).

Each resized image I_s is passed through a series of conv2D layers to select features:

$$F_s = Conv_{k\times k}(I_s) \text{ -------- } (7)$$

Where, the kernel size is k. F_s is the feature map for the scale s. Equation (7) is to detect patterns such as edges, textures, or gradients at both coarse and fine levels.

According to Wang et al. [44] the Channel Attention Mechanism focuses on emphasizing the most relevant feature channels while suppressing less important ones:

- A global representation of each feature map is computed using Global Average Pooling (GAP).
- Fully connected (FC) layers process this global information to generate channel weights (α).
- These weights are applied to the feature map, recalibrating it by amplifying important channels and diminishing irrelevant ones.

This selective focus ensures the network prioritizes features that are critical for forgery detection, such as textures, edges, and gradients associated with manipulations.

Each feature map F_s undergoes the CAS module:

$$v_c = \frac{1}{h \cdot w} \sum_{i=1}^{h} \sum_{j=1}^{w} F_s(i, j, c) \text{ ------------ } (8)$$

In equation (8) a global representation of each feature map channel is computed by averaging its spatial dimensions ($h \times w$). To distill global information from feature maps, enabling the network to focus on critical channels.

Fully connected layers generate attention weights:

$$\alpha_c = \sigma(FC_2(ReLu(FC_1(v_c)))) \text{ ---------- } (9)$$

The channel-wise global representation v_c is processed through two fully connected layers with a ReLU activation and a sigmoid function (σ) to generate channel attention weights (α). Equation (9) is used to prioritize important channels by amplifying their features while suppressing less relevant ones.

Feature recalibration:

$$F_s^{'} = \alpha_c \cdot F_s \text{ ---------- } (10)$$

The real feature map F_s is recalibrated by multiplying it with the attention weights (α) generated earlier. Equation (10) is used to ensure the network focuses on features most relevant to detecting forgeries, such as manipulated textures or gradients.

Deep learning architectures such as ResNet, are rife with residual connections, as they provide a means for training: the vanishing gradient problem. MCWRN uses wide residual connections, which differ in two ways:

- Wider Feature Maps: The architecture processes feature maps with more channels instead of narrow residual layers. Networks grow in their capacity to learn complex patterns, when they have this.
- Efficient Gradient Flow: The residual connections keep the network learn more of earlier learned features for refinement, and also effectively use low and high level features.

The recalibrated features are combined using residual connections:

$$R_s = F_s^{'} + F_{prev} \text{--------- } (11)$$

Where, F_{prev} is the outcome of the prior residual block. R_s is residual connection.The recalibrated feature map $F_s^{'}$ is added to the output of the previous residual block (F_{prev}).

Equation (11) is used to facilitate efficient gradient flow during training, mitigating the vanishing gradient problem. To refine the features by combining low and high level information.

The outputs from different scales are concatenated:

$$F_{fused} = Concat\ (R_1, R_2, R_3) \text{ ------------- } (12)$$

Outputs from all scales (R_1, R_2, R_3) are concatenated into a single feature map F_{fused}.

Equation (12) is used to merge multiscale features, capturing both global and local inconsistencies in the image.

The fused feature map is flattened and passed through fully connected layers for classification:

$$P(C = i|I) = \frac{\exp(Z_i)}{\sum_{j=1}^{k} \exp(Z_j)} \text{ ------------ } (13)$$

The network assigns probabilities $P(C = i|I)$ to each class iii using the softmax function, where Z_i is the activation for class i. Equation (13) is used to model the likelihood of the image belonging to each forgery class.

The predicted class $Pc^{'}$ is:

$$Pc^{'} = \arg\max_{i} P(C = i|I) \text{ ------- } (14)$$

The class with the highest probability (P) is selected as the predicted class $Pc^{'}$. Equation (14) is to determine the final classification outcome of the network.

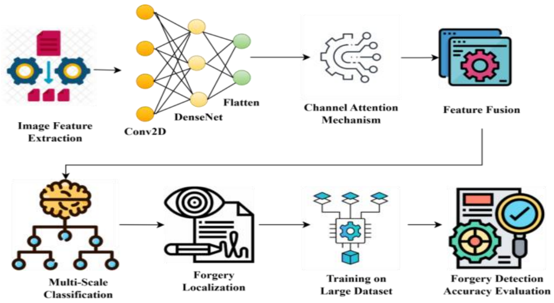
Image Feature Extraction
Conv2D
DenseNet
Flatten
Channel Attention Mechanism
Feature Fusion
Multi-Scale Classification
Forgery Localization
Training on Large Dataset
Forgery Detection Accuracy Evaluation

Figure 4: Multi-Scale Wide Residual Network workflow

Figure 4 showing the workflow of an image forgery detection system using a Multi Scale Wide Residual Network. Then we are going to start with the data preprocessing, normalization and augmentation in order to improve model robustness. The features extracted are global and local inconsistencies features, by utilizing denseNet and flatten layers to extract features at multiple scales.

Dropout layers introduce regularization to prevent overfitting by randomly deactivating neurons during training. Residual connections enable efficient gradient flow and attention mechanisms are identified to select features to be processed for detection of forgery. The system outputs a heatmap to visualize the tampered regions and is able to classify images to determine if they are forgeries. Second, the refined model is used to refine the model performance to ensure detection of equally reliable manipulations.

Algorithm 2: Multi-Scale Wide Residual Network

Input: Image I

Process:

Step 1: Image Preprocessing

Normalize and resize the image to capture coarse-to-fine details at different resolutions

Step 2: Feature Extraction

For each scale s, pass the scaled image through a conv2D layer to detect features such as edges, textures, and gradients

Step 3: Channel Attention Mechanism

Compute global representations; generate channel attention weights and Recalibrate feature maps to focus on features most relevant to forgery detection.

Step 4: Residual Connection

To combine low- and high-level features while ensuring efficient gradient flow.

Step 5: Multiscale Feature Fusion

Concatenate outputs to integrate multiscale information for robust detection of global and local inconsistencies.

Step 6: Classification

Step 7: Forgery Localization

Map features corresponding to mismatched descriptors back to their spatial regions in the image. Generate a heatmap highlighting manipulated areas.

Output: Forgery localization map R.

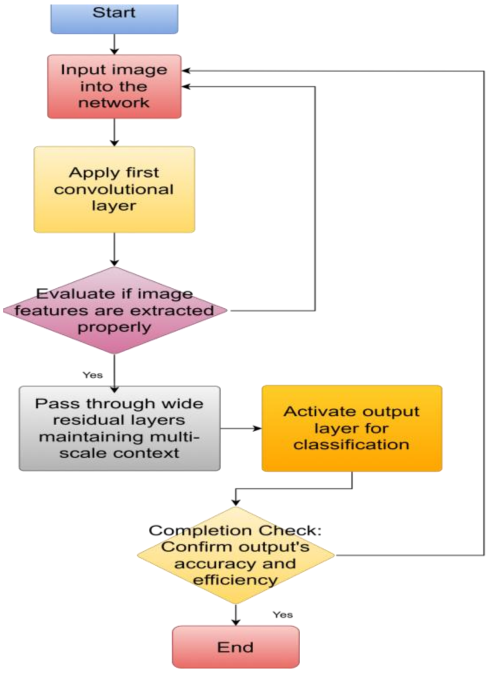
Start
Input image into the network
Apply first convolutional layer
Evaluate if image features are extracted properly
Yes
Pass through wide residual layers maintaining multi-scale context
Activate output layer for classification
Completion Check: Confirm output's accuracy and efficiency
Yes
End

Figure 5: Flowchart of Multi-Scale Wide Residual Network

Algorithm 2 and figure 5 shows the forgery detection and localization via multi scale analysis, design the Multi Scale Wide Residual Network. For coarse and fine details respectively we utilize coarse and fine resolutions over the input, we preprocess the input image by normalizing and resizing it. Through conv2D layers it is able to extract features of edges, textures, and gradients at each scale. The channel attention mechanism allows important features for forgery detection to be prioritized, whilst only focusing on manipulated regions. Residual connections ensure the effective combination of low and high level feature and gradient flow for training. Finally, we borrow ideas of fusing features at different scales, and detect inconsistencies robustly to produce a localization heatmap informing which spatial regions are forging.

VI Results And Discussions

Results show the proposed framework yields high accuracy and robustness with respect to different datasets and forgery types, namely, copy move, splicing, and GAN based manipulations. The feature is precisely selected by the Stable Keypoint Feature Extractor; the Multiscale CASWide Residual Networks help the classification ensure reliability. Experiments demonstrate noise, compression, and geometric distortion resilience and a big improvement over earlier methods in terms of false positives. The system's adaptability and scalability make it a promising solution to real world digital forensics and content authentication problems. In future work, we desire to integrate advanced techniques such as attention mechanisms and real time optimization into our pipeline so that it can be deployed on edge devices.

Table 2: Feature selection comparison

	Accuracy	**Precision**	**Recall**	**F-measure**
CNN	89.93	89.57	89.93	89.34
SIFT	90.97	90.37	90.67	90.22
VIT	91.12	90.97	91.02	90.89
AutoEncoders	91.32	91.11	91.21	90.95
DLSK	91.45	91.23	91.35	91.04

Table 2 shows the performance metrics of different models in image feature selection and classification. These metrics are Accuracy, Precision, Recall, and F–measure. In all metrics, the Deep Learning–Based Stable Keypoint Feature Extractor (DLSK) model has the highest values with an Accuracy score of 91.45%. The results indicate that DLSK achieves better classification performance than other models, like CNN, SIFT, VIT and AutoEncoders, while keeping certain key features identified and balancing precision and recall. This implies that DLSK is the most stable as well as the most effective model for this task.

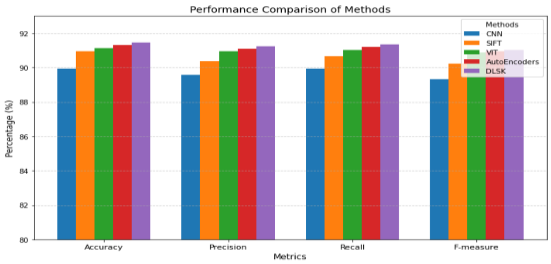

Figure 6: Performance comparison of Feature selection

Figure 6 shows the accuracy, precision, recall and f-measure comparison of various algorithms (CNN, SIFT, ViT, Auto encoders and proposed DLSK) for feature selection. In this chart key metrics values are shown in x-axis and the y-axis shows the percentage values.

Table 3: Classification comparison table

		Accuracy	**Precision**	**Recall**	**F-measure**
Before classification	**SVM**	90.49	90.21	90.47	90.11
	GNN	90.89	90.45	90.64	90.47
	CNN	91.23	91.01	91.11	90.94
	FCNN	91.74	91.37	91.63	91.21
After Feature selection and classification	**SVM**	90.78	90.23	90.59	90.18
	GNN	91.08	90.76	90.94	90.59
	CNN	91.52	91.32	91.48	91.31
	FCNN	91.98	91.76	91.85	91.27
	MCWRN	92.46	92.19	92.40	92.02

Table 3 compares the performance of various classification methods before and after feature selection in terms of four metrics: Which are Accuracy, Precision, Recall, F-measure. In general, there is an improvement across all methods after feature selection, especially for MCWRN which has the highest accuracy, precision, recall and f-measure values. This implies a better model performance for correctly classifying instances due to feature selection. Particularly, the FCNN model performs well, but MCWRN evaluates superior to all others in all metric evaluations after feature selection.

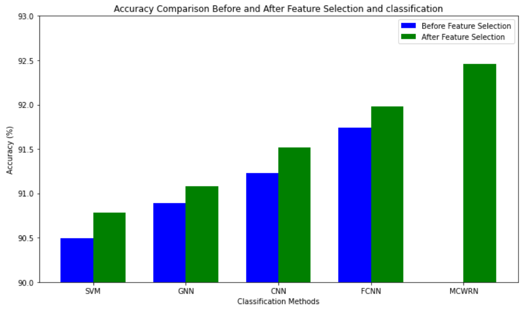

Figure 7: Accuracy comparison

Figure 7 compares the accuracy comparison of SVM, GNN, CNN, FCNN, and proposed MCWRN algorithms before and after classification. In this chart the horizontal line shows various algorithms and the vertical line shows the accuracy percentage.

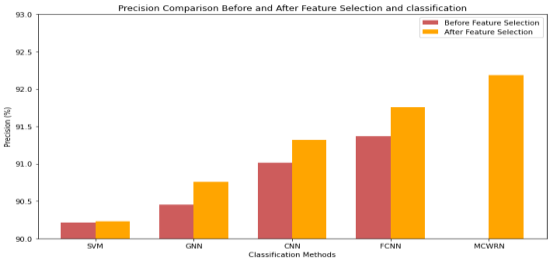

Figure 8: Precision comparison

Figure 8 compares the precision comparison of SVM, GNN, CNN, FCNN, and proposed MCWRN algorithms before and after classification. In this chart the horizontal line shows various algorithms and the vertical line shows the precision percentage.

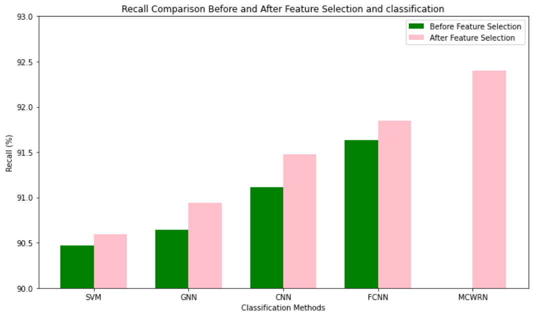

Figure 9: Recall comparison

Figure 9 compares the recall comparison of SVM, GNN, CNN, FCNN, and proposed MCWRN algorithms before and after classification. In this chart the horizontal line shows the various algorithms and the vertical line shows the recall percentage.

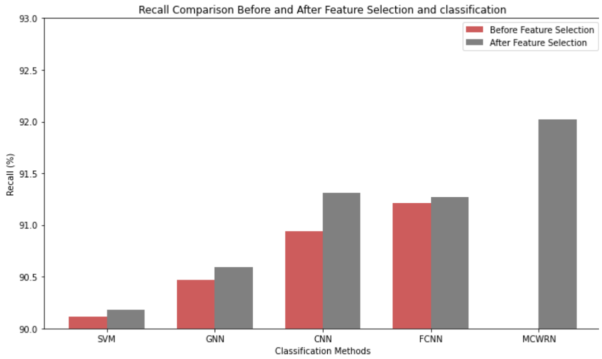

Figure 10: F-measure comparison

Figure 10 illustrates the f-measure comparison of SVM, GNN, CNN, FCNN, and proposed MCWRN algorithms before and after classification. In this chart the horizontal line shows various algorithms and the vertical line shows the f-measure percentage.

V Conclusion

In particular, a Deep Learning Based Stable Keypoint Feature Extractor is proposed to pick precise features, and Multiscale CASWide Residual Networks are proposed to perform robust classification. This method overcomes the inconsistency of keypoint detection and classification accuracy in complex forgery scenario, and shows better performance than existing methods. The system is designed to be reliable by focusing on stable keypoint extraction and its multiscale architecture allows it to capture global features present only for entire sets, as well as local features present across the dataset. To improve upon these results for future improvements, we could add attention mechanisms (or transformers) to dynamically highlight important regions in the image while selecting features. Moreover, the proposed model will also be extended to deal with the arising forgeries coming from recent GANs to cope with the threats that keep evolving. Proposed methods achieve 91.45 % accuracy in feature selection and 92.46% accuracy in classification. Other collaborative learning frameworks, e.g., federated learning, can then be used to further improve upon the model functioning by exploiting multiple distributed datasets while maintaining privacy. Finally, the system could be optimized for real time applications on edge devices, and thereby greatly expand its usability in forensic and security domains.

Reference:

[1] Guo, X., Liu, X., Ren, Z., Grosz, S., Masi, I., & Liu, X. (2023). Hierarchical fine-grained image forgery detection and localization. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 3155-3165).

[2] Shan, W., Zou, D., Wang, P., Yue, J., Liu, A., & Li, J. (2024). RIFD-Net: A Robust Image Forgery Detection Network. *IEEE Access*.

[3] Al-Hammadi, M. H., Muhammad, G., Hussain, M., & Bebis, G. (2013). Curvelet transform and local texture based image forgery detection. In *Advances in Visual Computing: 9th International Symposium, ISVC 2013, Rethymnon, Crete, Greece, July 29-31, 2013. Proceedings, Part II 9* (pp. 503-512). Springer Berlin Heidelberg.

[4] Asghar, K., Sun, X., Rosin, P. L., Saddique, M., Hussain, M., & Habib, Z. (2019). Edge–texture feature-based image forgery detection with cross-dataset evaluation. *Machine Vision and Applications*, *30*(7), 1243-1262.

[5] Rathore, N. K., Jain, N. K., Shukla, P. K., Rawat, U., & Dubey, R. (2021). Image forgery detection using singular value decomposition with some attacks. *National Academy Science Letters*, *44*(4), 331-338.

[6] Abosamra, G., & Oqaibi, H. (2021). Using residual networks and cosine distance-based K-NN algorithm to recognize on-line signatures. *IEEE Access*, *9*, 54962-54977.

[7] Ranjan, S., Garhwal, P., Bhan, A., Arora, M., & Mehra, A. (2018, May). Framework for image forgery detection and classification using machine learning. In *2018 2nd international conference on trends in electronics and informatics (ICOEI)* (pp. 1-9). IEEE.

[8] Diwan, A., Kumar, D., Mahadeva, R., Perera, H. C. S., & Alawatugoda, J. (2023). Unveiling copy-move forgeries: Enhancing detection with SuperPoint keypoint architecture. *IEEE Access*.

[9] Agarwal, R., & Verma, O. P. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. *Multimedia Tools and Applications*, *79*(11), 7355-7376.

[10] Deshpande, P., & Kanikar, P. (2012). Pixel based digital image forgery detection techniques. *International Journal of Engineering Research and Applications (IJERA)*, *2*(3), 539-543.

[11] Muhammad, G., Al-Hammadi, M. H., Hussain, M., & Bebis, G. (2014). Image forgery detection using steerable pyramid transform and local binary pattern. *Machine Vision and Applications*, *25*, 985-995.

[12] Yue, G., Duan, Q., Liu, R., Peng, W., Liao, Y., & Liu, J. (2022). SMDAF: A novel keypoint based method for copy-move forgery detection. *IET Image Processing*, *16*(13), 3589-3602.

[13] Arun Anoop, M., Karthikeyan, P., & Poonkuntran, S. (2024). Unsupervised/Supervised Feature Extraction and Feature Selection for Multimedia Data (Feature extraction with feature selection for Image Forgery Detection). *Supervised and Unsupervised Data Engineering for Multimedia Data*, 27-61.

[14] Dhivya, S., Sangeetha, J., & Sudhakar, B. J. S. C. (2020). Copy-move forgery detection using SURF feature extraction and SVM supervised learning technique. *Soft Computing*, *24*(19), 14429-14440.

[15] Khalil, A. H., Ghalwash, A. Z., Elsayed, H. A. G., Salama, G. I., & Ghalwash, H. A. (2023). Enhancing digital image forgery detection using transfer learning. *IEEE Access*, *11*, 91583-91594.

[16] Farooq, S., Yousaf, M. H., & Hussain, F. (2017). A generic passive image forgery detection scheme using local binary pattern with rich models. *Computers & Electrical Engineering*, *62*, 459-472.

[17] Jalab, H. A., Subramaniam, T., Ibrahim, R. W., Kahtan, H., & Noor, N. F. M. (2019). New texture descriptor based on modified fractional entropy for digital image splicing forgery detection. *Entropy*, *21*(4), 371.

[18] Vidyadharan, D. S., & Thampi, S. M. (2017). Digital image forgery detection using compact multi-texture representation. *Journal of Intelligent & Fuzzy Systems*, *32*(4), 3177-3188.

[19] Diwan, A., & Roy, A. K. (2024). CNN-Keypoint Based Two-Stage Hybrid Approach for Copy-Move Forgery Detection. *IEEE Access*, *12*, 43809-43826.

[20] Luo, S., Peng, A., Zeng, H., Kang, X., & Liu, L. (2019). Deep residual learning using data augmentation for median filtering forensics of digital images. *IEEE Access*, *7*, 80614-80621.

[21] Yang, P., Ni, R., Zhao, Y., & Zhao, W. (2019). Source camera identification based on content-adaptive fusion residual networks. *Pattern Recognition Letters*, *119*, 195-204.

[22] Saber, A. H., Khan, M. A., & Mejbel, B. G. (2020). A survey on image forgery detection using different forensic approaches. *Advances in Science, Technology and Engineering Systems Journal*, *5*(3), 361-370.

[23] Archana, M. R., Biradar, D. N., & Dayanand, J. (2024). Image forgery detection in forensic science using optimization based deep learning models. *Multimedia Tools and Applications*, *83*(15), 45185-45206.

[24] Kumar, D., Pandey, R. C., & Mishra, A. K. (2024). A review of image features extraction techniques and their applications in image forensic. *Multimedia Tools and Applications*, 1-102.

[25] Agarwal, S., & Chand, S. (2015). Image forgery detection using multi scale entropy filter and local phase quantization. *International journal of image, graphics and signal processing*, *7*(10), 78.

[26] Agarwal, S., & Jung, K. H. (2022). Photo forgery detection using RGB color model permutations. *The Imaging Science Journal*, *70*(2), 87-101.

[27] Ahmed, I. T., Hammad, B. T., & Jamil, N. (2021). Forgery detection algorithm based on texture features. *Indonesian Journal of Electrical Engineering and Computer Science*, *24*(1), 226-235.

[28] Chen, Z., Tondi, B., Li, X., Ni, R., Zhao, Y., & Barni, M. (2019). Secure detection of image manipulation by means of random feature selection. *IEEE Transactions on Information Forensics and Security*, *14*(9), 2454-2469.

[29] Guo, X., Liu, X., Ren, Z., Grosz, S., Masi, I., & Liu, X. (2023). Hierarchical fine-grained image forgery detection and localization. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 3155-3165).

[30] Kaushik, M. S., & Kandali, A. B. (2024). Hybrid Feature Selection for Effective Copy-Move Forgery Detection. *International Journal of Intelligent Engineering & Systems*, *17*(2).

[31] Meena, K. B., & Tyagi, V. (2019). Image forgery detection: survey and future directions. *Data, Engineering and Applications: Volume 2*, 163-194.

[32] Mittal, H., Saraswat, M., Bansal, J. C., & Nagar, A. (2020, December). Fake-face image classification using improved quantum-inspired evolutionary-based feature selection method. In *2020 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 989-995). IEEE.

[33] Saleh, S. Q., Hussain, M., Muhammad, G., & Bebis, G. (2013). Evaluation of image forgery detection using multi-scale weber local descriptors. In *Advances in Visual Computing: 9th International Symposium, ISVC 2013, Rethymnon, Crete, Greece, July 29-31, 2013. Proceedings, Part II 9* (pp. 416-424). Springer Berlin Heidelberg.

[34] Walia, S., Kumar, K., Kumar, M., & Gao, X. Z. (2021). Fusion of handcrafted and deep features for forgery detection in digital images. *IEEE Access*, *9*, 99742-99755.

[35] Balasubramanian, S. B., Prabu, P., Venkatachalam, K., & Trojovský, P. (2022). Deep fake detection using cascaded deep sparse auto-encoder for effective feature selection. *PeerJ Computer Science*, *8*, e1040.

[36] Luo, Z., Shafait, F., & Mian, A. (2015, August). Localized forgery detection in hyperspectral document images. In *2015 13th international conference on document analysis and recognition (ICDAR)* (pp. 496-500). IEEE.

[37] Qazi, E. U. H., Zia, T., & Almorjan, A. (2022). Deep learning-based digital image forgery detection system. *Applied Sciences*, *12*(6), 2851.

[38] Sudiatmika, I. B. K., Rahman, F., Trisno, T., & Suyoto, S. (2019). Image forgery detection using error level analysis and deep learning. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *17*(2), 653-659.

[39] Deep Kaur, C., & Kanwal, N. (2019). An analysis of image forgery detection techniques. *Statistics, Optimization & Information Computing*, *7*(2), 486-500.

[40] Rhee, K. H. (2021). Generation of novelty ground truth image using image classification and semantic segmentation for copy-move forgery detection. *IEEE access*, *10*, 2783-2796.

[41] Li, H., Luo, W., Qiu, X., & Huang, J. (2016). Identification of various image operations using residual-based features. *IEEE Transactions on Circuits and Systems for Video Technology*, *28*(1), 31-45.

[42] Bayar, B., & Stamm, M. C. (2016, June). A deep learning approach to universal image manipulation detection using a new convolutional layer. In *Proceedings of the 4th ACM workshop on information hiding and multimedia security* (pp. 5-10).

[43] Van der Maaten, L., & Hinton, G. (2008). Visualizing data using t-SNE. *Journal of machine learning research*, *9*(11).

[44] Wang, F., Jiang, M., Qian, C., Yang, S., Li, C., Zhang, H., ... & Tang, X. (2017). Residual attention network for image classification. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 3156-3164).

[45] Simonyan, K. (2014). Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.