PAPER – 1

|  |  |
| --- | --- |
| Title and Author | Digital Image Forgery Detection Using Pre-Trained Xception Model as Feature Extractor |
| URL | <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10080127> |
| Notes | The paper titled "Digital Image Forgery Detection Using Pre-Trained Xception Model as Feature Extractor" by Niyantha Maruthu Pandiyan presents a deep learning-based approach to identify tampered images. The primary objective is to classify images as either authentic or tampered by leveraging the capabilities of a pre-trained Xception model for feature extraction. |
| Dataset | CASIA ITDE v2 Dataset  The study utilizes the CASIA ITDE v2 dataset, a widely recognized benchmark in the field of image forgery detection. This dataset is particularly well-suited for the proposed methodology due to the following reasons:   * Diverse Image Collection: CASIA ITDE v2 comprises a substantial number of images, including 7,200 authentic and 5,123 tampered images. This variety ensures that the model is exposed to a wide range of genuine and manipulated images, enhancing its ability to generalize across different forgery techniques. * Variety in Image Sizes: The dataset includes images with resolutions ranging from 320×240 to 800×600 pixels. This variation in image sizes aids the model in learning features that are consistent across different scales, making it robust against resizing and scaling operations often involved in image tampering. * Comprehensive Forgery Types: CASIA ITDE v2 encompasses multiple types of image forgeries, including but not limited to:Copy-Move ForgerySplicingRetouchingRe-samplingMorphingThis diversity ensures that the model is trained to detect various manipulation techniques, thereby increasing its effectiveness in real-world scenarios where multiple forgery methods might be employed. * Balanced Training: Although the full dataset contains over 12,000 images, the study uses a subset of 2,400 images (1,200 authentic and 1,200 tampered) for implementation. This balanced approach between authentic and tampered images helps in mitigating class imbalance issues, ensuring that the model does not become biased towards either class. |
| Method | To effectively utilize the CASIA ITDE v2 dataset, the paper employs the following methodology:   1. Preprocessing:    * Resizing: All images are resized to 256×256 pixels to maintain consistency.    * Error Level Analysis (ELA): ELA is applied to highlight areas with different compression levels, which is indicative of tampering.    * Data Splitting: The dataset is divided into 90% training, 5% validation, and 5% testing subsets to evaluate the model's performance accurately. 2. Feature Extraction:    * The pre-trained Xception model serves as the feature extractor. By leveraging a model pre-trained on the ImageNet dataset, the approach benefits from learned features that are transferable to the task of forgery detection. 3. Classification:    * Extracted features are passed through Global Average Pooling and two Dense layers, culminating in a SoftMax activation layer that outputs the classification probabilities. |
| Key Results, Advantages & Limitations | The model achieved impressive results on the test subset of the CASIA ITDE v2 dataset:   * Accuracy: 95% * True Positive Rate (TPR): 98.2% * True Negative Rate (TNR): 98.3% * False Positive Rate (FPR): 1.6%   These metrics demonstrate the model's efficacy in accurately distinguishing between authentic and tampered images, underscoring the suitability of the CASIA ITDE v2 dataset for training robust image forgery detection systems. |
| BIB | @inproceedings{pandiyan2023digital,  title={Digital Image Forgery Detection Using Pre-Trained Xception Model as Feature Extractor},  author={Pandiyan, Niyantha Maruthu},  booktitle={2023 International Conference for Advancement in Technology (ICONAT)},  pages={1--5},  year={2023},  organization={IEEE}  } |

**PAPER – 2**

|  |  |
| --- | --- |
| Title and Author | Detectify : Image Tampering Detection using Error Level Analysis (ELA) and Convolutional Neural Network (CNN) |
| URL | <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10627878> |
| Notes | The paper titled "Detectify: Image Tampering Detection using Error Level Analysis (ELA) and Convolutional Neural Network (CNN)" explores advanced techniques for identifying manipulated digital images. The authors integrate Error Level Analysis (ELA) and Convolutional Neural Networks (CNN) to enhance the accuracy of image tampering detection. This approach is evaluated using the CASIA V2.0 dataset, a widely recognized collection of both original and tampered images.  1. Error Level Analysis (ELA)  ELA is a forensic technique used to identify inconsistencies in an image's compression levels, which may indicate manipulation. By analyzing the compression artifacts, ELA highlights areas within an image that have been altered, making it easier to detect tampered regions.  2. Convolutional Neural Networks (CNN)  CNNs are a class of deep learning models particularly effective in image recognition tasks. In this study, the CNN is trained on ELA-processed images to learn and identify subtle patterns associated with image manipulation. The architecture comprises:   * Two Convolutional Layers: Each with 32 filters and a kernel size of (5, 5). * Max-Pooling Layers: To downsample feature maps and reduce computational complexity. * Dropout Layers: Implemented to prevent overfitting by randomly deactivating neurons during training. * Fully Connected Layers: Two layers with 256 neurons each, followed by a softmax activation function for classification. |
| Dataset | CASIA V2.0 Dataset  The CASIA V2.0 dataset is central to this study. It comprises a diverse set of images, both original and tampered, which are used to train and validate the detection model. Key aspects of the dataset include:   * Diversity of Manipulations: The dataset includes various types of image tampering techniques such as copy-move forgery, splicing, deepfakes, and AI-generated images. * Data Preparation: Images undergo ELA preprocessing, are resized to 128x128 pixels, and labeled as real (1) or fake (0). The dataset is split into training and validation sets in an 80-20 ratio. * Balanced Representation: Ensures that the model is trained on a balanced number of authentic and manipulated images, enhancing its ability to generalize to unseen data. |
| Method | The proposed system operates through the following stages:   1. Preprocessing with ELA: Images are transformed using ELA to accentuate compression artifacts indicative of tampering. 2. Data Standardization: ELA-processed images are resized and flattened to maintain consistency for CNN input. 3. Model Training: The CNN is trained on the prepared dataset, utilizing binary cross-entropy loss and the Adam optimizer over 30 epochs with a batch size of 32. 4. Validation: The model's performance is evaluated using validation accuracy and loss metrics to ensure robustness and minimize overfitting. |
| Key Results, Advantages & Limitations | The integration of ELA and CNN yielded impressive results:   * Overall Accuracy: Achieved up to 99.2% accuracy in distinguishing between real and tampered images. * Confusion Matrix Insights:   + True Positives: High count indicating effective detection of manipulated images.   + False Negatives: Some instances where manipulated images were incorrectly classified as real, suggesting areas for improvement.   + True Negatives and False Positives: Demonstrated the model's precision in correctly identifying authentic images with minimal false alarms. * Performance on Manipulation Techniques:   + Copy-Move Forgery: 95% accuracy   + Splicing: 96% accuracy   + Deepfakes: 85% accuracy   + AI-Generated Images: 70% accuracy   These results highlight the system's strength in detecting various manipulation forms, particularly copy-move and splicing, while indicating challenges in more sophisticated techniques like deepfakes and AI-generated content. |
| BIB | @inproceedings{geethanjali2024detectify,  title={Detectify: Image Tampering Detection using Error Level Analysis (ELA) and Convolutional Neural Network (CNN)},  author={Geethanjali, TM and Darshan, TS and Surya, K and Rahul, HU and Sheety, Ipshika N},  booktitle={2024 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT)},  pages={1--6},  year={2024},  organization={IEEE}  } |

**PAPER - 3**

|  |  |
| --- | --- |
| Title and Author | Performance Analysis of ELA-CNN model for Image Forgery Detection |
| URL | <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10170007> |
| Notes | The paper titled "Performance Analysis of ELA-CNN model for Image Forgery Detection"explores the growing concern of digital image forgery in the age of widespread digital content sharing. With platforms like WhatsApp and Instagram facilitating the rapid dissemination of images and videos, the risk of manipulated content spreading misinformation has escalated 1. The authors address this issue by proposing a method that combines Error Level Analysis (ELA) with a Convolutional Neural Network (CNN) to effectively detect forged images. |
| Dataset | A critical aspect of the study is the utilization of three distinct datasets to evaluate the proposed method's effectiveness:   * CASIA V2.0: Comprising 7,200 pristine images and 5,123 tampered images, this dataset includes images with blurring and splicing manipulations. Image sizes range from * 320×240 * 320×240 to * 800×600 * 800×600 pixels 1. * MICC-F220: Contains 110 authentic and 110 tampered images with tampered regions covering approximately 1.2% of the entire image. The image sizes vary between * 722×240 * 722×240 and * 800×600 * 800×600 pixels 1. * MICC-F2000: This larger dataset includes 1,300 authentic and 700 tampered images, each sized at * 2048×1536 * 2048×1536 pixels. Tampered regions make up about 1.12% of each image 1.   These datasets were meticulously selected to ensure comprehensive testing across various scenarios, including different image resolutions and manipulation techniques. The diversity in image sizes and forgery types aids in validating the robustness and generalizability of the proposed ELA-CNN model. |
| Method | Preprocessing  The preprocessing stage involves several key steps to prepare images for analysis:   * Image Resizing: All input images are resized to a uniform dimension of * 224×224×3 * 224×224×3 pixels to ensure consistency. * Image Normalization: Pixel values are scaled to a fixed range, enhancing both training convergence and testing accuracy. * Color Space Conversion: Images are converted from RGB to a different color space to highlight features relevant to forgery detection. * Error Level Analysis (ELA): This technique identifies regions within an image that have different compression levels, indicating potential manipulation. * Image Augmentation: Random transformations are applied to increase the diversity of training data and mitigate overfitting.   Error Level Analysis (ELA)  ELA is pivotal in distinguishing authentic images from forged ones by analyzing compression discrepancies. When an image is saved in a lossy format like JPEG, it undergoes compression. Any subsequent editing introduces additional compression artifacts, which ELA can detect by highlighting areas with varying compression levels 1.In the context of this study, brighter regions in the ELA-processed image signify potential forgery.  Convolutional Neural Network (CNN)  The CNN architecture designed by the authors consists of five convolutional layers, each followed by a  2×2  2×2 max pooling layer. The number of feature maps increases progressively from 16 in the first layer to 256 in the fifth layer. The network employs ReLUactivation functions to introduce non-linearity and SoftMax for classification. The model is optimized using Binary Cross Entropy as the loss function and the Adam optimizer for efficient training 1.  Classification  The final classification stage utilizes a global average pooling layer followed by a fully connected layer. The SoftMax activation function categorizes the input image as either original or forged based on the extracted features from the CNN 1 |
| Key Results, Advantages & Limitations | The ELA-CNN model was trained over 100 epochs with a batch size of 32 and a learning rate of 0.0001. Comparative analyses revealed that the proposed method outperformed traditional statistical methods like DCT and LBP+DCT, as well as pretrained models such as VGG16, VGG19, and ResNet50 1. Specifically, the model achieved:   * 98.25% accuracy on CASIA V2.0 * 97.32% accuracy on MICC-F220 * 98.67% accuracy on MICC-F2000   These results demonstrate the model's high efficacy in detecting image forgery across different datasets. Notably, the method showed consistent performance, maintaining high validation accuracy and minimizing overfitting despite the variability in dataset sizes and image resolutions 1.  The study successfully demonstrates the effectiveness of combining ELA with a tailored CNN architecture for image forgery detection. By leveraging ELA's ability to highlight compression inconsistencies and CNN's prowess in feature extraction and classification, the proposed model achieves superior accuracy compared to existing methods. The comprehensive evaluation across multiple datasets underscores the model's robustness and adaptability.  For future work, the authors suggest extending the methodology to video tampering detection and enhancing dataset diversity to further validate and improve the model's performance. As digital content continues to proliferate, such advancements are crucial in maintaining the integrity and trustworthiness of shared media |
| BIB | @inproceedings{singh2023performance,  title={Performance analysis of ELA-CNN model for image forgery detection},  author={Singh, Tanishka and Goel, Yash and Yadav, Tanush and Seniaray, Sumedha},  booktitle={2023 4th International Conference for Emerging Technology (INCET)},  pages={1--6},  year={2023},  organization={IEEE}  } |
|  | PAPER – 4 |
| Title and Author | Image Forgery Detection Using Low Dimensional Texture Feature Vector |
| URL | <https://ieeexplore.ieee.org/document/10193545> |
| Notes | This paper proposes a method for detecting digital image forgeries using texture features and machine learning classification. The key components are:   1. Image preprocessing 2. Feature extraction using texture features (Tamura and LBP) 3. Classification using Gaussian Discriminant Analysis (GDA) |
| Dataset | The researchers used the CASIA V2.0 dataset, which is a popular benchmark for image forgery detection. Key details:   * Contains 7,491 authentic and 5,123 forged color images * Various image sizes and formats (JPEG, BMP, TIFF) * Includes both copy-move and splicing forgeries * Dataset was split 70% for training, 30% for testing |
| Method | 1. Preprocessing: Convert images to grayscale and resize to 384x256 pixels 2. Feature Extraction:    * Local Binary Pattern (LBP): 59-dimensional feature vector    * Tamura features: 4-dimensional feature vector (coarseness, contrast, directionality, regularity) 3. Classification: Gaussian Discriminant Analysis (GDA) classifier |
| Key Results, Advantages & Limitations | The results of the paper are as follows:   * Tamura features with GDA performed best:96% accuracy99% precision97% recall98% F1-score * Tamura features outperformed LBP features * The proposed method achieved competitive results with a very low-dimensional feature vector (4D) compared to other state-of-the-art methods   Significance  The paper demonstrates that simple texture features like Tamura, when combined with an appropriate classifier, can achieve high accuracy in image forgery detection while using a much smaller feature vector than many existing methods. This makes the approach computationally efficient and potentially more practical for real-world applications.  The research contributes to the field of digital image forensics by showing how low-dimensional texture features can be effective for forgery detection, potentially opening up new directions for future work in this area. |
| BIB | @inproceedings{mashaan2023image,  title={Image Forgery Detection Using Low Dimensional Texture Feature Vector},  author={Mashaan, Wasan Fahad and Ahmed, Ismail Taha},  booktitle={2023 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)},  pages={327--331},  year={2023},  organization={IEEE}  } |

PAPER – 5

|  |  |
| --- | --- |
| Title and Author | A Similarity-Based Positional Attention-Aided Deep Learning Model for Copy–Move Forgery Detection |
| URL | <https://ieeexplore.ieee.org/document/10478450> |
| Notes | The paper proposes a new deep learning model for detecting copy-move forgery in images. Copy-move forgery is when part of an image is copied and pasted elsewhere in the same image to create a fake or altered version. |
| Dataset | The model was tested on four datasets:   1. CoMoFoD:    * 5000 forged images (200 base images + 4800 with postprocessing)    * Various postprocessing techniques applied 2. COVERAGE:    * 100 forged images with ground truth    * Image resolutions vary from 190x334 to 551x556 pixels 3. CASIA TIDE v2.0:    * 1313 copy-move forged images (out of 5123 manipulated images)    * Total of 2626 samples including unmanipulated versions 4. MICC-F600:    * 160 manipulated images and 440 authentic images    * Resolutions range from 800x533 to 3888x2592 pixels |
| Method | 1. Modified MultiResUnet Architecture:    * Uses separable convolutional layers instead of standard ones    * Reduces parameters while maintaining performance 2. Similarity-Based Positional Attention Module (SPAM):    * Analyzes patches to identify forged regions    * Uses cosine similarity to compare patches    * Incorporates Positional Attention Module (PAM) for spatial attention |
| Key Results, Advantages & Limitations | The proposed model outperforms state-of-the-art methods on all four datasets in terms of F1-score and accuracy.   * It achieves a significant boost in performance while reducing trainable parameters by 50% compared to the base model. * The model sometimes struggles with regions of varying sizes and non-quadrilateral shapes. * There's a need for a more computationally efficient attention mechanism. * Future work could explore overlapping patches, irregular patch shapes, and patch-free approaches to improve performance.   This paper presents a novel approach to CMFD that combines efficient architecture modifications with a sophisticated attention mechanism, resulting in improved performance across multiple challenging datasets. |
| BIB | @article{roy2024similarity,  title={A Similarity-based Positional Attention aided Deep Learning Model for Copy-Move Forgery Detection},  author={Roy, Ayush and Mohiuddin, Sk and Sarkar, Ram},  journal={IEEE Transactions on Artificial Intelligence},  year={2024},  publisher={IEEE}  } |

PAPER – 6

|  |  |
| --- | --- |
| Title and Author | Detection of Manipulated Multimedia Using Machine Learning Techniques |
| URL | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10533016 |
| Notes | The paper highlights the growing concern of multimedia manipulation (images, videos, audio) in the context of misinformation and cybercrime. The proposed solution uses Convolutional Neural Networks (CNNs) to detect manipulated content. The research examines both the challenges and benefits of using deep learning for multimedia forensics and evaluates the model's robustness against adversarial attacks and deepfake variations. It emphasizes the need for ongoing advancement in deep learning models for digital forensics. |
| Dataset | The research utilized a large dataset of both real and manipulated multimedia, including images, videos, and audio files, which were pre-processed with techniques like normalization, data augmentation, and Error Level Analysis (ELA). |
| Method | The system proposed in this research employs CNNs for detecting multimedia manipulation. Key steps include:   1. **Data Pre-processing**: Image resizing, normalization, augmentation (rotations, zooms), and ELA for images. 2. **Feature Extraction**: CNN-based hierarchical feature extraction for images and videos, and MFCC feature extraction for audio. 3. **Model Architecture**: VGG16 for images and video detection; a CNN model for audio detection. 4. **Evaluation**: The model performance is evaluated using metrics such as specificity, sensitivity, accuracy, and precision, with testing on a separate dataset for validation. |
| Key Results, Advantages & Limitations | The CNN-based system achieved high accuracy in identifying manipulated multimedia, with robust performance across different types of content manipulations.     * Effective detection of various manipulation techniques. * Extensive validation and testing to ensure model robustness against adversarial attacks and deepfakes. * CNN's ability to automatically identify features from multimedia content. * Scarcity of large, high-quality datasets for training. * High false-positive rate, particularly in deepfake detection. * Difficulty in generalizing across all types of manipulation due to dataset limitations. |
| BIB | @inproceedings{anvekar2024detection,  title={Detection of Manipulated Multimedia In Digital Forensics Using Machine Learning},  author={Anvekar, Preetam and Gudnavar, Anand and Naregal, Keerti and Nagarmunoli, Sreedevi},  booktitle={2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)},  pages={33--38},  year={2024},  organization={IEEE}  } |

PAPER – 7

|  |  |
| --- | --- |
| Title and Author | Detection of Spliced Images in Social Media Application |
| URL | <https://ieeexplore.ieee.org/document/9677737> |
| Notes | In this paper, a detection system is implemented for verifying and classifying the content of social media images. The system adopted Deep Learning based on a convolutional neural network (CNN) to detect spliced images on WhatsApp. The images in dataset CASIA v2 (transformed to be appropriate for WhatsApp) are used for training and testing.   The results point to an accuracy of 99.19% of training and 87.438% of testing. |
| Dataset | * The research focuses on developing software that can detect image tampering and test its performance. * The datasets used to detect splicing images are CASIAvl and CASIAv2. * The WhatsApp application was chosen due to the very large use of this application, as the entire data set for CASIA V2 was uploaded through the WhatsApp application (30 JPEG images per upload) and then received from a second application on another device. * The total number of images that were uploaded was 9,292, divided into 7,278 original images and 2014 fake images. * This new dataset is specific for social media applications, named Wsap-CASIV2. |
| Method | This part includes four processes: Error Level Analysis (ELA), Image difference, Normalization, and Enhancement.  **1. Error Level Analysis (ELA)** - Increase the training efficiency of the CNN by identifying the areas in the image with different compression rates.  **2. Image Difference** - The differences are calculated between the original and ELA image (pixel-by-pixel) and the output is a new image.  **3. Normalize the Image** - So that CNN converges faster reaching the global minimum of loss values belonging to the validation data.  **4. Image Enhancement** - This stage enhances image brightness. After converting the image to ELA compression, sometimes the image may look blurry bright, or dark. This increases the visibility of features to increase the efficiency of CNN in detecting.  **B. Building model**   * CNN in general is a very good feature extractor. * The proposed CNN has two convolutional layers and one pooling layer as feature learning and fully connected layers with one Softmax.  1. **Convolutional layer:** The convolution layer aims to extract image features. The input of the first convolution layer is an image with 128×128 × 3 while the first and the second convolution layers have a 32 kernel filter with a 5×5 size matrix with strides 1 or 2 - pixels that move over all the pixels of the image-taking their dot product. 2. **Activation Function:** The activation function in a neural network removes unnecessary pixels, such as negative values. The Rectified Linear Unit (ReLU) function is selected. Softmax is used as the activation function for multi-class classification problems. 3. **Pooling layer:** The aim is to reduce the number of pixels in the output from the previous convolutional layer. The scale is down to 25% of the original size. |
| Key Results, Advantages & Limitations | Results:   * The proposed system's performance is evaluated using different performance metrics, such as accuracy, recall, precision sensitivity, and F1-score. * The best accuracy is obtained at the 5th epoch the validation loss after the 5th epoch starts to flat and eventually increases, which is a sign of overfitting. * The CNN uses two convolutional layers, one MaxPooling layer, one fully connected layer, and one output layer with softmax, which can achieve a maximum accuracy of 99.19% of training and 87.438% of validation using 30 epochs.   The advantages of our model are as follows: the number of training periods required to achieve convergence is significantly reduced, because the image features processed by ELA make the training more efficient, and accelerate the convergence of the CNN model. |
| BIB | @inproceedings{jabaar2021detection,  title={Detection of Spliced Images in Social Media Application},  author={Jabaar, Munera A and Alsaad, Saad N},  booktitle={2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)},  pages={63--69},  year={2021},  organization={IEEE}  } |

PAPER – 8

|  |  |
| --- | --- |
| Title and Author | Applicability of Heavily Compressed JPEG Tampered Images in Social Media and Supervised Machine Learning towards Detection of Forgery |
| URL | <https://ieeexplore.ieee.org/document/10561776> |
| Notes | This paper highlights and analyses the challenges of conventional forensic methods for forgery localization in heavily compressed tampered images.  This paper investigated the encoder-decoder-based deep learning frameworks (i.e., SegNet and U-Net) for the segmentation of the forged regions from the holistic tampered images.   Here, the forged image is studied with respect to the different quality levels (12, 8, and 1) and its corresponding compression percentages (0%, 60%, and 90%).  With a quality level maximum i.e., 12, the forged region (represented by a red bounding box) is well visualised in the generated DCT coefficients heat map.  But by reducing the quality label (8 or 1) or increasing the compression percentage, the forged region vanished as shown in Fig. 2 (a2) and (a3).  Generally, JPEG format is considered by the forensic attackers to manipulate image content thereby eliminating any forensic traces due to the compression process. |
| Dataset | **CASIA V2.0:**   CASIA ITDE V2.0 is an image-splicing dataset which is an extended version of CASIA ITDE V1.0.  There are 12,323 total images, among which 7200 are authentic and 5123 are tampered images.   There are 9 categories, which are classified as scene, animal, architecture, character, plant, article, nature, indoor, and texture in the authentic image subset and the same tool is used for V1.0.  **CMFD Dataset:**  Captured by a Canon EOS 7D camera with a resolution of 5202×3465 pixels.  From these captured images, 260 tampered images are created by Photoshop CS3 and CS5 in PNG format, each of 512×512 regions pixels and 3000×2000 pixels sized images are formed by cropping or resizing. |
| Method | **A. Data Collection and Annotation**  According to recent studies, digital image formats most widely used for the creation of passive forgery are .JPG/ JPEG, .PNG, .BMP, .TIFF, etc. JPEG format was widely used by intruders.  **CASIA V2.0:**   CASIA ITDE V2.0 is an image-splicing dataset which is an extended version of CASIA ITDE V1.0.  There are 12,323 total images, among which 7200 are authentic and 5123 are tampered images.   There are 9 categories, which are classified as scene, animal, architecture, character, plant, article, nature, indoor, and texture in the authentic image subset and the same tool is used for V1.0.  **CMFD Dataset:**  Captured by a Canon EOS 7D camera with a resolution of 5202×3465 pixels.   From these captured images, 260 tampered images are created by Photoshop CS3 and CS5 in PNG format, each of 512×512 regions pixels and 3000×2000 pixels sized images are formed by cropping or resizing.  **Own Designed Samples:** Used frames from the TUVD-CSA dataset.   To create manipulation, random 2000 sample frames are selected from the TUVD-CSA dataset comprising a resolution of 1920×1080.   After that manipulation is performed using the Adobe Photoshop tool.  **B. Forged Region Detection using Encoder-Decoder Techniques**   * In our proposed work, two widely used deep learning-based segmentation techniques including SegNet and U-Net are investigated for forgery detection. * The encoder module is used for feature extraction purposes so as to depict the local and global features to learn the forged region. * Consequently, the decoder plays an important role in maintaining the size of the feature map which helps finally to predict the result based on forged region information. * The encoder reads hierarchical features from the input image, it comprises thirteen convolution and five max-pooling layers to reduce spatial dimensions and increase channels for hierarchical feature learning. * The decoder repeatedly includes five upsampling and thirteen convolutional layers. The upsampling process is guided by the previously stored max-pooling indices, allowing the network to reconstruct spatial information lost during the encoding process. * Lastly, the softmax layer produces a probability distribution across different classes for each pixel in the input image which forms the segmentation map. * The encoder, or contracting path, comprises 16 convolutional layers, each consisting of two convolutional layers, a rectified linear unit (ReLU) activation function, and optional batch normalization. * After each convolutional block, max pooling is applied to reduce the spatial resolution and capture contextual information. * The Decoder or expansive path begins with up convolutional layers, also known as transpose convolution or deconvolution, to upsample the feature maps. These layers help in regaining the spatial resolution lost during the contracting path. * Finally, the softmax layer produces pixel-wise classification, generating the segmentation map. |
| Key Results, Advantages & Limitations | **A. Dataset Preparation and Parameter Configuration**   * To enhance the size of the dataset, we did flipping (horizontal and vertical flipping) and rotation (45°, 90°, 180°, 270 °, and 320°) on the CMFD dataset. * After applying augmentation, the CMFD dataset is increased by 2080 augmented images along with their corresponding ground truths. * From each of the considered datasets, 100 manipulated images are kept for testing purposes. * In our proposed work, each of these segmentation approaches is implemented on a GPU-based workstation with 64 GB installed memory for successful training of the encoder-decoder frameworks. * A training and validation set, each with its own collection of ground truth images is created by dividing the training set in a 4:1 ratio. * The training and validation loss/accuracy are measured using Binary cross entropy [22] and the optimizer is used as an Adam optimizer with a sigmoid activation function.   **B. Detection Performance**   * According to Table II, the CASIA-V2 dataset, SegNet + MobileNet performed well in comparison of all the backbone networks for forged region segmentation with an accuracy (0.89), recall (0.69), precision (0.48), and F1-Score (0.57).   **Conclusion:**   * This paper analyzed the challenges of conventional forensics methods for effective forged region localization in various JPEG compressed manipulated images. * The research also looks into the performance of two well-known encoder-decoder segmentation techniques. Techniques including SegNet and U-Net for forgery detection. * Moreover, the influence of the backbone networks on these segmentation techniques for more precise detection of the spliced regions is investigated. |
| BIB | @inproceedings{sarkar2024applicability,  title={Applicability of Heavily Compressed JPEG Tampered Images in Social Media and Supervised Machine Learning towards Detection of Forgery},  author={Sarkar, Saswata and Roy, Sourav Dey and Das, Santanu and Saha, Priya and Bhowmik, Mrinal Kanti},  booktitle={2024 3rd International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE)},  pages={1--6},  year={2024},  organization={IEEE}  } |