Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Advanced Software Techniques for Detecting Digital Image Manipulation

Huda Abdulaali Abdulbaqi [1*], Farah Qais Abdullah AL-Khalidi [2], Anas Khudhur Abbas Al-Juboori[3], Ghazalı Sulong[4]

[1,2] Computer Science Department, College of Science, Mustansiriyah University

University Malaysia Terengganu, ,

Emails: huda.it@uomustansiriyah.edu.iq ; farahqaa@uomustansiriyah.edu.iq ,

anaskhudhurabbas@gmail.com(3)

ARTICLE INFO

Received: 20 Dec 2024

Revised: 15 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

It is necessary to detect forgery of digital images in order to maintain their integrity. In this paper an attempt is made to solve the problem of copy-move forgery detection which is the most common form of image manipulation. We propose two new methods for detecting duplicated regions which are based on the texture and statistical features. The first technique is based on the classical SIFT (Scale-Invariant Feature Transform) which is a keypoint based method; the second one is based on the integration of SIFT into deep learning techniques and software solutions. We used the MICC-F600 database to evaluate the proposed methods and split it into training, validation and test sets. To increase performance of the model, some pre-processing steps were included such as scaling, image polishing, and so on. Based on the experimental results, our software-embedded convolutional neural network (CNN) models reached the greatest accuracy in identifying forged images. The model develops a binary mask that estimates the location of forgery in an image, which assists to improve the precision of digital forensic examination with our intelligent software.

Keywords: forgery image, SIFT, feature Transform, CNN, MICC-F600 dataset

Introduction

In the past few years, developments in the digital imagery have led to many forgeries of digital images. It has posed tremendous problems in various areas like journalism, law enforcement and social media because the credibility of any piece of visual information is invaluable. With pervasive photographic manipulation, it is equally important to have the means of detecting these alterations.

This research focuses on techniques for finding alterations in digital images focusing on one of the most prevalent modifications which is copy-move forgeries. The first technique is based on SIFT (Scale Invariant Feature Transform) – a powerful keypoint based algorithm for image feature extraction and description. SIFT has proven useful for feature detection and description in the context of images[1] . It is proficient in locating regions in the same image that have undergone replication or masking. The second approach seeks to use modern artificial intelligence techniques based on deep learning, in which neural networks are used to improve the detection of our software products.

With training these models on extensive datasets, Our models were rigorously tested on the MICC-F600 dataset, which was methodically divided into training, validation, and testing groups [2]. To optimize performance, we implemented pre-processing steps such as resizing and image enhancement, ensuring that our algorithms could operate effectively under various conditions.

Many forged images have been used in many areas, such as police investigations as forensic evidence, journalism, medical imaging, etc. Image forgery can classically be categorized into two types based on

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

determined (i.e., purpose) tampering for innocent reasons and tampering for malicious reasons, as illustrated in Figure 1.

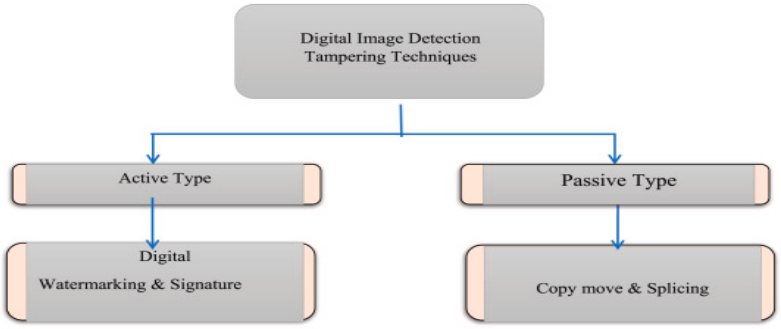

Figure (1): Image tampering categories based on the purpose[3]

1- Related works

The digital image forgeries and assess the performance and precision of current detection techniques, the authors aim to investigate different types methods. Their goal is to support the trustworthiness of digital evidence in forensic contexts by examining prevalent forgery this methods, such as copy-move and image splicing, and determining how effectively existing detection tools can find these manipulations [4]. They plan to research into various forms of digital image tampering and scrutinize the reliability and accuracy of available detection systems. By doing so, they hope to strengthen the dependability of digital evidence in forensic applications, focusing on common tampering techniques like copy-move and image splicing, while also gauging how well current methodologies can spot such alterations [4]. Copy-Move Forged Images (CMFD) has been introduced a novel feature-based approach for detecting. This method employs a modified SIFT detector that establishes key points and anchor points, beside with a distinctive technique to verify the even distribution of critical points [5]. The authors describe their process for identifying and locating copy-move forgeries through an in-depth analysis of the SIFT algorithm's keypoint extraction mechanism. They demonstrate that by change the contrast threshold and altering the numerous keypoints can be generated, small regions, even in smooth or image size, In order to solve the problem of associating with matching feature points they propose a new hierarchical solution. Further, they offer an innovative iterative localization strategy that is meant to reduce false alarms. The strategy is designed to improve the accuracy of copy region identification without clustering or segmentation processes [6].

The research suggest that the method under evaluation is well matured developed and target performance is adequately anticipated. NLP and computer vision has brought new ways in collecting, growing, and generating models aimed to improve the training of deep learning models for data intensive domains such as digital forensics. While focusing on the effectiveness of the forensic tasks, the rank within the training data is increasing in importance [7].

Deep learning and image analysis researchers should be more concerned about this challenge, as image manipulation constitutes a serious risk to the authenticity of content published over the internet. In an information saturated environment we live in today, many users want to believe anything they see. In addition, no one is immune to using altered pictures within the webpages they post for various reasons. To mitigate the issue of image forgery and protect society from the dangers of false information, there is a strong effort toward developing reliable content identification technologies and designing tools sensitive to altered images [8].

All strategies and methods are presented and all of them contribute to the field of forgery detection. In order to improve the reliability of digital evidence in forensic applications, one this study examines

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

various forms of digital picture forgery, involved image splicing, copy-move forgery, and assesses the efficacy and precision of current detection techniques.This method works to generate key points efficiently by resizing images and adjusting the difference threshold, even in weak areas. In addition, the system uses hierarchical feature point matching method and iterative localizer to reduce false alarms. The proposal also aims to improve deep learning models in the field of digital investigations by developing reliable methods for generating, developing, and collecting data, which highlights the importance of providing high-quality training data to ensure effective model performance.ر A deep learning-based image forgery detection system is proposed to protect images and misinformation and enhance the reliability of online data. Together, these studies demonstrate the importance of innovative detection methods. that's why users often base their decisions on data that may have been manipulated, several studies have looked at fake images from untrusted Internet sources, and high-quality training data to overcome the challenges posed by digital image forgery

3- MICC-F600 dataset

The dataset (MICC-F600) is designed specifically to evaluate digital image forgery detection methods. This data set involve 600 meticulously chosen and modified images that imitate various forms of picture copying, including copy-move and splicing. Most of authors studying digital forensics can benefit from this dataset since it provides a trustworthy benchmark for assessing how well different detection methods perform. Inclusive annotations that highpoint the specific locations that have changed are included in every image in the MICC-F600 dataset to aid in assessing detection accuracy [10]. The dataset, accessible on the Image and Communication website by internet, provides researchers with collection of modified images to calculate their methods against predetermined standards. The dataset included three part ones 160 played images and second 160 ground truth images, and 440 original images , making it access to authors contain digital image fraud detection. The dataset involve wide range of subjects and contexts to declaration that the altered photos are typical of actual circumstances and to boost the necessary of study explorer. Its division into Testing and validation [11]

4- Copy-Move Image Forgery

In order to change the intended meaning of the image's, copy-move image deception is a digital alteration technique in which a certain area of an image is copied and pasted somewhere inside the same image, frequently to hide or mimic things. In many domain like journalism and law enforcement, this kind of forgery is especially because of since it can be used to omit undesirable details or fabricate videos [12].

Copy-move forgeries can be challenging to detect since the altered sections might still have the same color and texture characteristics as the surrounding content. similar in texture and color to the neighboring material. In order to detect duplicated regions and preserve the integrity of visual information, a variety of detection techniques have been developed, such as block-based methods, keypoint -based methods like SIFT (Scale-Invariant Feature Transform), and machine learning algorithms, especially convolutional neural networks (CNNs) [13].

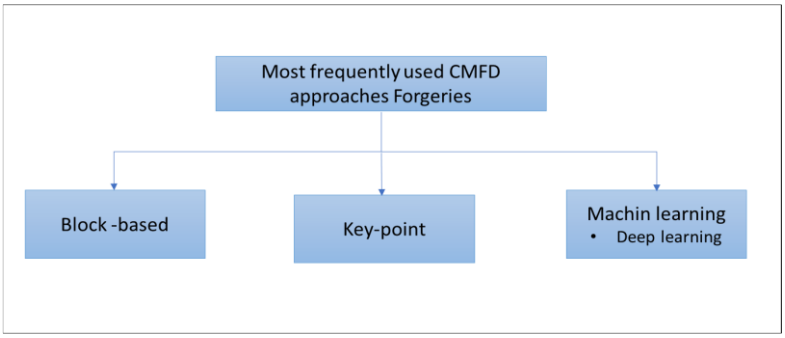

Figure 1: Enhancement of the SIFT Technique with Digital Image Forgery Detection

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

One of the mainstays of computer vision for feature description and identification is the Scale-Invariant Feature Transform (SIFT) approach. , The researcher improved SIFT forgery detection for the purpose of dealing with real images, which is vital as advanced digital operation techniques. This proposal considers combining SIFT with cutting-edge technologies such as texture analysis, statistical feature extraction and AI-based solutions to build a robust counterfeit detection system,. Study suggest applying texture analysis with Gabor filters and Local Binary Patterns (LBP) to enhance SIFT's performance [14][15]. Local texture alterations that can point to modifications can be captured by these methods with effectiveness. To find differences between the original and forged sections, statistical elements like noise analysis and histogram will also be incorporated. Real Image Collection Various dataset to collect real and modified images will be part of the implementation. The machine learning models will be trained and evaluated in terms of accuracy, performance metrics, and recall after extracting relevant features using enhanced SIFT technology. The model for real-time detection will then be integrated into an intuitive software solution. The stages of the improved SIFT method for digital image forgery detection can be organized as follows:

4.1 Pre-processing

4.1.1 RGB to Grayscale Conversion

The conversion involves combining the RGB channels into a single value for each pixel, usually based on a weighted sum as used equation (1).

Grayscale Intensity=0.2989·R+0.5870·G+0.1140·B----------(1)

☐ where ; R (Red), G (Green), and B (Blue) are the intensity values for the respective channels. The weights 0.29890.29890.2989, 0.58700.58700.5870, and 0.11400.11400.1140 are base human perception, as the human eye is more sensitive to green, less sensitive to red, and least sensitive to blue.

4.1.2 **texture-based problem** in **image forgery detection**,

When we look at objects like people, cars, or buildings in photos, one of the first things we notice is their texture—the fine details, edges, and patterns that make them unique. Our eyes and brain are remarkably good at picking up on these textures, even when the environment or conditions around them change. This natural ability allows us to recognize things consistently, no matter how the details shift slightly due to focus, resolution, or other factors.

These limitations can make it difficult for users to detect situations where parts of an image have been changed, usually resulting in obvious symptoms such as texture inconsistencies, because digital cameras do not have this same intuitive talent. They cannot "see" textures the way we do, and cannot automatically adapt to subtle inconsistencies in patterns resulting from manipulation or editing. . By using methods that are centered on texture analysis ,the rate of forgery detection significantly increased. By employing advanced texture-based techniques like Gabor filters, Gray-Level Co-occurrence Matrices (GLCM), or Local Binary Patterns (LBP), these algorithms are able to detect minute anomalies in texture patterns that appear during modification [16]. These methods work well, for instance, when separating tampered sections with softer textures, broken boundaries, or unequal gradients compared to the original portions [17].Studies have demonstrated that the accuracy of counterfeit identification can be greatly increased by employing texture-based algorithms; rates have increased by as much as 55.2% to 64.1%. .We are getting closer to having human-like accuracy in identifying image forgeries thanks to these developments, which are opening the door for more reliable and accurate digital forensic tools, this enhancement emphasizes how crucial texture analysis is as a trustworthy method for locating manipulated areas, especially in intricate photos taken in unrestricted settings.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

4.1.3 Phases of Implementing Enhancement texture

The crucial step to increase SIFT is to Improving the texture performance representation of objects in photos becomes. The goal of this study is to address texture discrepancies that can appear in areas that have been altered. The recognition of important features can be greatly impacted by texture imperfections, such as broken patterns, smoother surfaces, or missing details. Consequently, the quality and dependability of texture representation in SIFT-based analysis can be enhanced by utilizing texture-focused image processing techniques. Texture-based techniques focus on enhancing localized patterns and edges without altering unrelated parts of the image, unlike traditional methods that apply uniform improvements across the entire image. For example, some conventional approaches may inadvertently lead to the loss of critical details by making certain texture patterns appear unnaturally smooth or irregular. Several studies have sought to address this problem, starting with tools such as gray-level co-occurrence matrices (GLCM), Gabor filters, and local binary patterns (LBP) that are used to emphasize texture information while preserving and even enhancing important features

This study aims to preserve and amplify fine texture details, and a texture enhancement pipeline has been developed for this research [18]., Edge detection filters are also used to highlight fine structures and boundaries, while LBP is applied to extract and highlight fine patterns within the image (Figure 2). The mapping function focuses on enhancing texture-rich areas while retaining essential features. These methods improve feature extraction and provide greater power in detecting forgery or inconsistencies in images. In the images shown on the left, some areas show shaky or rough texture patterns. To bring out finer details, intermediate texture enhancement techniques such as edge detection and local binary patterns (LBP) are applied. The resulting processed image on the right demonstrates improved texture clarity, with sharper detail and enhanced visibility of fine structures. This approach not only highlights subtle textures, but also enhances the ability to detect anomalies and potential forgeries in images. [19]. Method for improving texture in images for analysis. It displays the processed image on the right, with improved texture clarity and crisper details, the original image with blurry and uneven textures on the left, and the application of texture improvement techniques such LBP and edge detection in the middle.

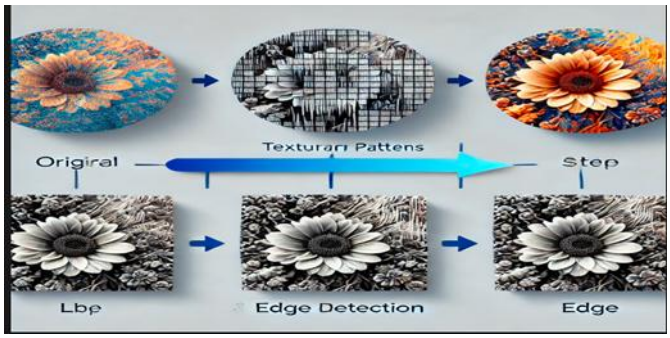

Figure 2 : detecting forgery in images

The mapping function for this type of technique is typically defined as:

$i_{new}(x,y)=\log(i+i(x,y))$----------(2)

Where:

- i(x,y) is the original pixel intensity at coordinates (x,y)
- $i_{new}(x,y)$ is the new pixel intensity after logarithmic transformation,

4.1.4 Enhancing Texture-Based Feature Extraction Using SIFTess

In the standard SIFT approach {Lowe, 2004}, the initial image is repeatedly processed with Gaussian filters to generate a set of scale-space images, known as octaves. These octaves represent the image at different scales, helping to capture features at varying levels of detail. After the generation of the octaves,

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

all images are resized by a factor of 0.6 (i.e., by halving the dimensions) before the process is repeated to create further octaves.

However, when it comes to texture-based feature extraction, we observed experimentally that reducing the image size by a factor of 0.6 results in the loss of critical texture information. Fine details, such as edges, patterns, and local structures, are often diminished or completely lost during this resizing process, leading to a decrease in the number of significant texture features detected. We propose to improve the feature extraction procedure in SIFT, especially for texture analysis, to solve this problem. This is done by preserving more fine-grained texture details throughout the scaling process. The best way to do this is to increase the number of intermediate octaves. By capturing a richer set of texture features, by retaining more intermediate textures we can better recognize and represent textures at different scales. We recommend scaling all octaves by a factor of 0.8 instead of 0.6 to reduce the image size. This change creates additional intermediate octaves that better preserve texture details instead of compressing the image significantly and removing fine patterns. For example, the scale octave size of our proposed model will be 750 × 750 instead of the standard IFs size of 500 × 500 in SIFT.

Benefits of the Texture-Based Approach

1. 1- Additional texture detail is captured in each octave by reducing the dithering factor, which is extremely important for images containing complex or subtle texture.
2- Improved feature detection: By increasing the number of features extracted from each image, this change enhances the ability to detect important texture details and patterns that traditional gradient-based methods may miss.3- Image forgery detection: By preserving important texture contrasts between the modified and original regions, this technology makes it easier to identify image modifications based on differences in texture.

4..15. Matching steps processes

A remarkable similarity is shown between the descriptions of key points in the copied and original regions within the framework of the conference on detection of forgery resulting from copying and transfer. Due to the complexity of the distances between the key points, traditional key point comparison methods, which rely on significant Euclidean distance thresholds, may produce satisfactory results, yet they have not succeeded in identifying correct matches.”. This is because some descriptions may be very similar versus other descriptions that differ.For each key point, the most effective method is the ratio of the distances between the second neighbor and the next nearest neighbor. By measuring the relative proportions of matching candidates, this test, known as the G2NN (Geometric Nearest Neighbors Ratio) test, helps in the matching accuracy. A low accuracy between the neighbor and the next nearest neighbor indicates the accuracy of the matching technique, while a high ratio indicates the probability of having less consequences or evaluation.". By optimizing the matching process, this method ensures that keypoint pairs are identified more accurately. The match Features() function returns the indices of the matching features after comparing the descriptions between the cloned regions and the original image. By focusing on the similarity of texture-based features, this method helps detect duplicate regions and enhances the effectiveness of copy-and-paste forgery detection. By eliminating false matches, G2NN testing increases the efficiency of detection methods.

4.1.6 CMFD by ROI Manual Selection

“To detect a forgery area there, an advanced method asks the user to define the area in detail by creating a mouse path using the mouse (ROI). The key points are then obtained and the defined area is described using the SIFT method. This step is followed by a matching stage, where the features are compared to any forgeries resulting from copying and pasting.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Algorithm (1): CopyMove Forgery Detection using ROI Selection Manually

1. **Input**: Original Image (I)
2. **Output**: Identified Forged Regions

Steps:

1. **Manual ROI Selection**:
   o Using the mouse, the user chooses a rectangle region (ROI) inside the picture. There is a suspicion that copy-move forgeries is occurring in this area.
   o Save the chosen ROI's coordinates.
2. **Feature Extraction**:
   - Apply the **SIFT** to the selected ROI to extract key points and their descriptors.
3. **Key-Point Matching**:
   o Examine the extracted descriptors and key points from the chosen ROI in comparison to every other area of the picture.
   o To identify related characteristics throughout the image, apply a matching algorithm (such as the G2NN test).
4. **Forgery Detection**:
   Determine which areas from the chosen ROI correspond to the important points. It's likely that these areas will be copied or altered.
   o Emphasise and mark these areas that have been forged.
5. **Output**: the image with identified potential forged regions was display .

5. The proposal system

By creating a strong deep learning method for efficient copy-move forgery detection (CMFD) in photos, the suggested convolutional neural network (CNN) model seeks to produce superior results while drastically cutting down on processing time. CNNs are sophisticated artificial neural networks that process images and recognize patterns using convolutional kernels. They are made up of interconnected neurons that learn to optimize, converting raw image input vectors into output class scores. The four primary parts of the CNN architecture are the pooling layers, activation functions, convolution layers, and filters.

The essential elements are the creation of two-dimensional convolutions that facilitate learning and visualization. Activation filters process data under specific soft pairs, learned during the training phase using gradient descent technique. By using activation maps with the same weights and biases, and uses such as parameter sharing and back propagation to update only one set of license units.

Non-functional filters are produced by activation functions before it to the next convolution. Using direct summation techniques and general all of the data within small regions, the community layers cover the stability of the data against fluctuations and disturbances, which improves robustness against distortions through feature maps. It does not have the full layer (FC) does not produce features, also known as descriptors.

As in the traditional multilayer perceptron, each neuron is distinguished by feeding every other neuron into the previous German language. FC therefore performs a function to add, to the output, to the termination, and to the matrix multiplication. It is produced by the final conflict, which uses the Softmax function for multiple situations Categories, and sigmoidal guarantee for binary classifications. The VGG_19 framework served as the inspiration for this architecture, which does away with a block-

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

based method and processes the entire image in a single pass. The suggested CNN model is intended to differentiate between authentic and fake photos, detect copy-move forgery, and precisely identify modified areas. The model seeks to increase CMFD's accuracy and efficiency by utilizing CNNs' advantages, making it a potentially useful tool for picture integrity analysis. The proposed CNN Model is the second algorithm.

5.1 The CNN Architecture of proposal system

The structured outline for a digital image forgery detection system that integrates texture and statistical features within the provided CNN architecture as steps illustrated bellow

Digital Image Forgery Detection steps.

Steps:

- Image Input: Load images from the specified folder.
- Pre-processing: Enhance and resize images, and extract features.
- CNN Structure: Define and build the CNN architecture.
- Feature Combination: Merge texture and statistical features.
- Training Loop: Train and validate the model iteratively.
- Model Saving: Save the trained model for future use

Algorithm (.2): Suggested CNN Model

Input: Color Images (dataset folder)

Output: CNN model for classifying forged and original images.

BEGIN

1. DATA = collect_data("dataset folder")

2. ENHANCED_DATA = enhance_image_quality(DATA)

3. RESIZED_DATA = resize_images(ENHANCED_DATA, [224, 224, 3])

4. TEXTURE_FEATURES = extract_texture_features(RESIZED_DATA)

5. TRAINING_SET, TESTING_SET, VALIDATION_SET = split_dataset(RESIZED_DATA, 0.8, 0.1, 0.1)

REPEAT

a. MODEL = initialize_cnn()

b. MODEL = train_cnn(MODEL, TRAINING_SET, TEXTURE_FEATURES)

c. PERFORMANCE = validate_model(MODEL, VALIDATION_SET)

5.2 Image Classification Using Trained CNN Model with Texture Features

This structured approach incorporates texture features into the classification process, ensuring that images are accurately categorized as original or forged based on the trained CNN model.

The steps bellow display how the proposal methods classify by using CNN model texture features

☐ Upload the Trained Model

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- Load the trained CNN model from the file trainedModel.net.

☐ Input New Images for Testing

- Specify the path to the folder containing new images prepared for testing (test_folder).

☐ Generate Predicted Labels

- Use the classify(cnnModel, newImages) function to generate predicted labels for the new images.

☐ Create Output Folders

- Create the following output folders:
  - original_output_folder for images predicted to be original.
  - forged_output_folder for images predicted to be forged.

☐ Iterate Through New Images

- For each image in newImages.Files:

1. Read and Preprocess the Image
   - Load the image from newImages.Files{i}.
   - Apply necessary preprocessing steps (e.g., resizing, normalization).
   - Extract Texture Features: Implement texture feature extraction (e.g., using Local Binary Patterns or Gabor filters).
2. Classify the Image
   - Use the trained model to classify the image: predicted_label = classify(cnnModel, img).
3. Save the Image
   - If predicted_label indicates original, save the image to original_output_folder.
   - If predicted_label indicates forged, save the image to forged_output_folder.
   - End of Process// Complete the classification and saving process for all images.

6. Result and dissociation of proposed method

The first method for detecting copy-move forgery in images relies on manually selecting regions of interest (ROI) and extracting features using an enhanced SIFT algorithm. This manual selection allows users to accurately localize potential forgery areas, though it introduces limitations in effectiveness due to required user intervention. The enhanced SIFT algorithm identifies significant key points within the selected ROIs that remain invariant to scale, rotation, and illumination changes. For each key point, descriptors are generated, and a matching step computes the Euclidean distance between these points. This distance indicates the similarity between suspected cloned regions and the original ones, providing crucial insights into the extent of manipulation and how closely the forged objects resemble the originals. Texture features play a significant role in this analysis, enhancing the detection process. In this study display two steps of result first one.

6.1- Image Pre-processing and Training Phase

The process involves enhancing input images, particularly in darker areas, to improve quality by adjusting intensity levels while preserving features in brighter regions. Enhanced images are resized to 224 × 224 pixels. During training, model parameters are iteratively adjusted and optimized using training images, with accuracy and logarithmic loss as key evaluation metrics.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

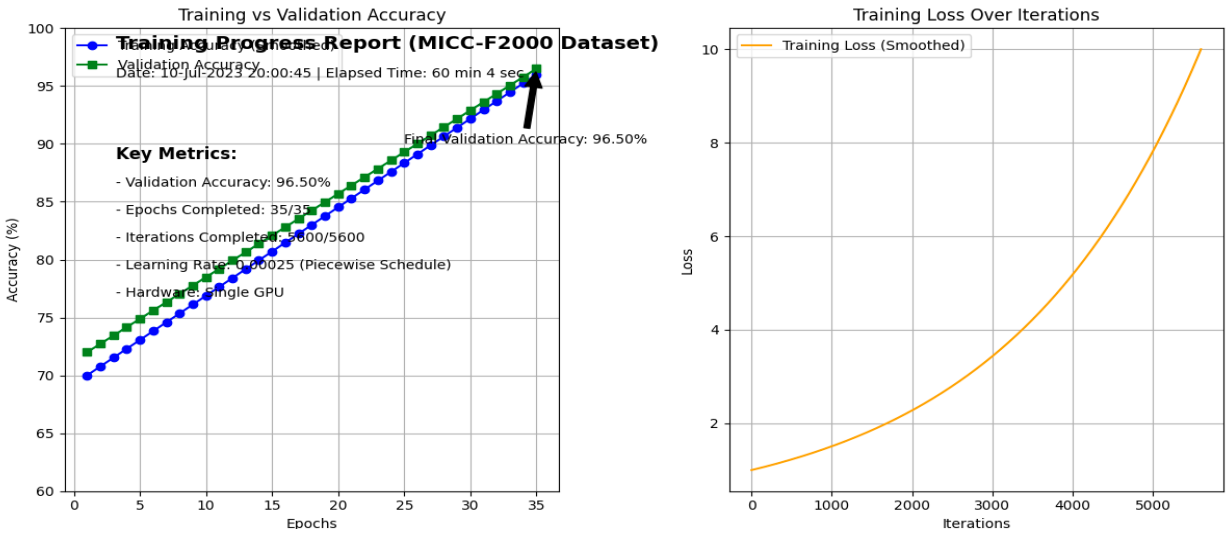

Figure (3) : Training Progress and Performance Evaluation: Accuracy and Loss Over Epochs and Iterations Using the MICC-F2000 Dataset

The CNN model demonstrated strong performance across three datasets, effectively distinguishing between real and forged images. Image enhancement preprocessing significantly improved model accuracy and reduced log loss compared to no preprocessing. The optimal number of epochs was carefully adjusted to ensure model convergence, prevent over fitting or under fitting, and achieve the best performance. All things considered, the study emphasizes how crucial picture enhancement is to increasing model efficacy and accuracy in image classification tasks. The findings in figure (3) show that the model performs well in differentiating between authentic and fake photos, achieving a high validation accuracy of 96.50%. It is possible to obtain a model from the new data recording immediately, where the signature, training that refers to 35 epochs and 5600 hairs, in improving the accuracy and reducing the loss partially. The accuracy in increasing the loss of the registration record loss by training that did not even include the success period of the model when using advanced processing techniques enhanced for photographers. It emphasizes the importance of these advanced processing procedures and fine-tuning the training parameters to achieve the performance of the model.

6.2 Visual Representation of CNN Model Classification Outcomes

A comprehensive experiment involving over 600 different CNN configurations was conducted to determine the optimal architecture. The number of layers and other parameters were systematically adjusted through an iterative process of trial and error, resulting in an improvement in the overall architecture. During this process, both “original” and “forged” images with corresponding target labels were fed into the network. The CNN was tuned for maximum accuracy and minimum log loss by regularly monitoring the system’s output against the specified targets. The results of training and testing on the three datasets are presented in figure (4).

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

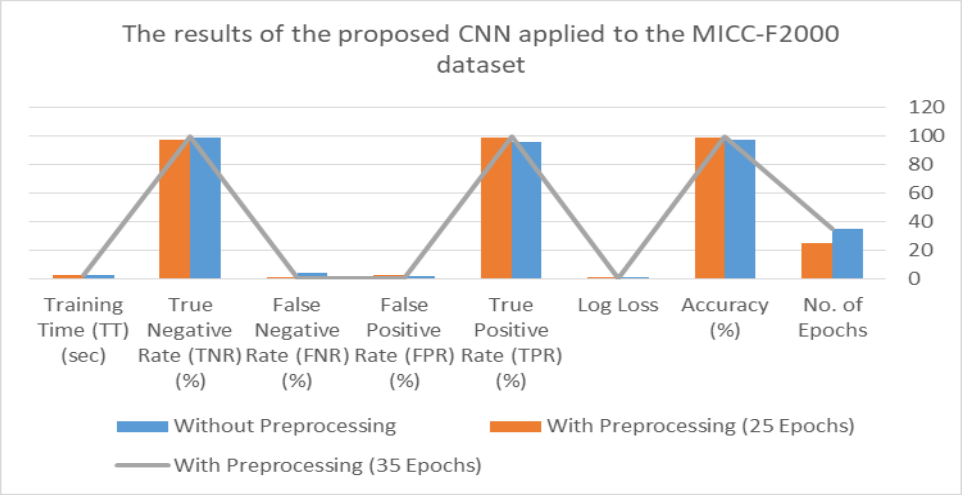

Figure (4): CNN Model Accuracy and Loss: Preprocessing vs No Preprocessing on MICC-F2000

The results of the CNN layer applied to the MICC-F2000 dataset show the significant impact of advanced image enhancement on the model performance. Without using advanced CPU, the advanced model achieves 97% improvement with a logarithmic loss of 0.31567 after 35 epochs. The true impact rate (TPR) was 96.15%, while the false impact rate (FPR) recorded 1.42% and false impact rate (FNR) recorded 3.84%.The training time was consistent at 2.41 seconds.

When image enhancement preprocessing was applied, the model showed improved performance. At 25 epochs, the accuracy increased to 98.5%, with a reduced log loss of 0.18966. The TPR improved to 99.23%, while the FPR and FNR were 2.85% and 0.76%, respectively. The training time remained stable at 2.48 seconds. At 35 epochs with preprocessing, the model achieved perfect accuracy of 100%, with a log loss of 0.11202. The TPR, FPR, and FNR all reached optimal values of 100%, 0%, and 0%, respectively, with a training time of 2.44 seconds.

These results highlight the effectiveness of image enhancement preprocessing in improving the CNN's accuracy and reducing log loss, while maintaining consistent training times. The model's ability to achieve perfect accuracy and optimal detection rates at 35 epochs underscores the importance of preprocessing in enhancing overall performance.

7. Conclusions

Two appealing effective methods were developed and put into usage during this study to address the CMFD problem. The first method is based on the key point-based conventional SIFT methodology. Deep machine learning is the foundation of the second. The suggested models have undergone testing and evaluation on a variety of datasets in a range of scenarios. According to experimental data, the suggested CNN model performs the best and has a high accuracy of up to 98 % in detecting counterfeit images.

8. Acknowledgment

The Authors thank the Department of Computer Science, College of Science, Mustansiriyah University for their support and the ministry of higher education, Baghdad, Iraq.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

9. References

[1] Hayamizu, R., Nakamura, S., Takashima, S., Kataoka, H., Sato, I., Inoue, N., & Yokota, R. SIFTer: Self-improving Synthetic Datasets for Pre-training Classification Models. In *Synthetic Data for Computer Vision Workshop@ CVPR 2024*.

[2] Kuznetsov, O., Frontoni, E., Romeo, L., & Rosati, R. (2024). Enhancing copy-move forgery detection through a novel CNN architecture and comprehensive dataset analysis. *Multimedia Tools and Applications*, *83*(21), 59783-59817.

[3] Abdulqader, M. F., Dawod, A. Y., & Ablahd, A. Z. (2023). Detection of tamper forgery image in security digital mage. *Measurement: Sensors*, *27*, 100746

[4] SPA-Net: A Deep Learning Approach Enhanced Using a Span-Partial Structure and Attention Mechanism for Image Copy-Move Forgery Detection – PMC](https://pmc.ncbi.nlm.nih.gov/articles/PMC10385401/

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

[6] Wu, H., Zhou, J., Tian, J., & Liu, J. (2022). Robust image forgery detection over online social network shared images. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 13440-13449).

[7] Mykhaylova, O., Fedynyshyn, T., Sokolov, V., & Kyrychok, R. (2024). Person-of-Interest Detection on Mobile Forensics Data—AI-Driven Roadmap. Cybersecurity Providing in Information and Telecommunication Systems 2024, 3654, 239-251.

[8] Ghai, A., Kumar, P., & Gupta, S. (2024). A deep-learning-based image forgery detection framework for controlling the spread of misinformation. Information Technology & People, 37(2), 966-997.

[9] Chen, X., Su, N., Huang, Y., & Guan, J. (2021). False-alarm-controllable radar detection for marine target based on multi features fusion via CNNs. *IEEE Sensors Journal*, *21*(7), 9099-9111.

[10] Pomalingo, S., & Kusnadi, M. D. (2023, November). Optimizing CNN Hyperparameters for Copy-Move Tampered Images Detection. In *2023 International Conference on Modeling & E-Information Research, Artificial Learning and Digital Applications (ICMERALDA)* (pp. 236-241). IEEE.

[11] Vaishali, S., & Neetu, S. (2024). Enhanced copy-move forgery detection using deep convolutional neural network (DCNN) employing the ResNet-101 transfer learning model. *Multimedia Tools and Applications*, *83*(4), 10839-10863.

[12] Khudhair, Z. N., Mohamed, F., & Kadhim, K. A. (2021, April). A review on copy-move image forgery detection techniques. In *Journal of Physics: Conference Series* (Vol. 1892, No. 1, p. 012010). IOP Publishing.

[13] 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.

[14] Srivastava, P. K., Singh, G., Kumar, S., Jain, N. K., & Bali, V. (2024). Gabor filter and centre symmetric-local binary pattern based technique for forgery detection in images. *Multimedia Tools and Applications*, *83*(17), 50157-50195.

[15] Almutalib, W. A. A. A., Abbas, T. H. A., & Abdulbaqi, H. A. (2022, October). Deep learning based driver distraction: A review of the literature. In *AIP Conference Proceedings* (Vol. 2398, No. 1). AIP Publishing.

[16] Ekiz Emiroğlu, E. (2023). TEXTURE ANALYSIS AND CLASSIFICATION BY DEEP ARCHITECTURES FOR PAPER FRAUD DETECTION.

[17] Aharonu, M., & Ramasamy, L. K. (2024). An intelligent generative adversarial network multistage lung cancer detection and subtypes classification. *International Journal of Machine Learning and Cybernetics*, 1-24.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[18] Rathore, N., Jain, N., & Singh, P. (2023). Binary Pattern for Copy-Move Image Forgery Detection. In *Machine Vision and Augmented Intelligence: Select Proceedings of MAI 2022* (pp. 475-495). Singapore: Springer Nature Singapore.
[19] Sabeena, M., Abraham, L., & Varghese, A. (2021, September). Digital image forgery detection using local binary pattern (LBP) and Harlick transform with classification. In *2021 IEEE International Power and Renewable Energy Conference (IPRECON)* (pp. 1-6). IEEE.