Comprehensive Analysis of Deep Learning Approach for detecting Forgery in Digital Images

Clifa Mascarenhas[1], Nadine Dias[2]

[1]Student, Department of Information Technology and Engineering, Goa College of Engineering, Farmagudi, Goa, India
[2]Assistant Professor, Department of Information Technology and Engineering, Goa College of Engineering, Farmagudi, Goa, India

---***---

Abstract - *Image forgery is a growing concern in today's digital age, where images can be easily manipulated and altered using various software tools. The proposed project aims to tackle the pressing issue of image forgery in the digital era by utilizing advanced deep learning techniques for detection. By curating a dataset containing both authentic and manipulated images, the project seeks to expose the model to various forgery scenarios. Through the use of lightweight deep learning architectures, strategic data preprocessing, transfer learning from pre-trained models, and rigorous training, the project endeavours to develop a reliable system for automated forgery detection. This comprehensive approach is designed to enhance image forensics and safeguard the credibility and integrity of visual content in the face of increasing threats posed by image manipulation.*

Key Words: **image forgery, lightweight deep learning architectures, transfer learning, image forensics, image manipulation**

1.INTRODUCTION

Image forgery, the manipulation of digital images, is a growing concern in today's digital age. With the increasing use of digital images in various fields such as forensic investigation, criminal investigation, intelligence systems, medical imaging, insurance claims, and journalism, the credibility and integrity of visual content are at stake. The ease of image manipulation using advanced software tools has made it challenging to distinguish between authentic and manipulated images.

To address this challenge, researchers have turned to deep learning techniques to develop automated image forgery detection systems. Deep learning models, such as convolutional neural networks (CNNs), have shown promising results in detecting image forgery with high accuracy. These models can learn complex features from large datasets of authentic and manipulated images, enabling them to distinguish between genuine and manipulated images.

This paper presents a novel approach to image forgery detection using deep learning techniques. The proposed approach involves a curated dataset of authentic and manipulated images, strategic data preprocessing, transfer learning from pre-trained models, and rigorous training. The paper emphasizes the importance of maintaining image authenticity and proposes future directions for improving detection and localization of digital forgeries.

The rest of the paper is organized as follows: Section 2 describes the Related work done in this domain. The method proposed which includes the use of transfer learning from pre-trained models and Procedure is given in Section 3. Conclusions are discussed in Section 4.

2. RELATED WORK

In the pursuit of tackling image forgery, researchers have explored various methodologies, each contributing to the evolving landscape of digital forensics. Traditional approaches often relied on handcrafted features and rule-based algorithms, but recent advancements have witnessed a paradigm shift towards data-driven techniques, particularly deep learning. Here, we delve into a brief review of related work, highlighting key developments in image forgery detection:

2.1 Traditional Methods

Traditional image forgery detection methods often focused on extracting handcrafted features such as texture, color, and shape. Techniques like error level analysis (ELA), wavelet transforms, and statistical measures were commonly employed. While these methods showcased effectiveness, they struggled to adapt to the complexities of modern forgery techniques.

Traditional image forgery detection methods have historically relied on extracting handcrafted features from images, including texture, color, and shape, to identify potential anomalies indicative of tampering. These methods aimed to leverage intrinsic characteristics of digital images to distinguish between authentic and manipulated content. Techniques such as error level analysis (ELA), wavelet transforms, and statistical measures were commonly employed in this regard.

Error Level Analysis (ELA):

ELA is a widely used technique in traditional image forensics, based on the observation that different compression levels are applied to regions of an image during multiple save operations. By resaving an image with a known compression level and then comparing it to the original, regions with inconsistent compression artifacts can be identified, potentially indicating areas that have been digitally altered. ELA exploits these discrepancies to detect forgeries, although its effectiveness can be limited in cases of sophisticated manipulation or when the image undergoes additional processing.

Wavelet Transforms:

Wavelet transforms have been extensively utilized in image processing and forensics due to their ability to decompose images into different frequency bands. In forgery detection, wavelet transforms are employed to analyze variations in frequency content across different regions of an image. Alterations such as copy-move, splicing, or retouching often introduce irregularities in the frequency domain, which can be detected through careful analysis of wavelet coefficients. However, the efficacy of wavelet-based methods may diminish in the presence of noise or when dealing with high-resolution images with subtle manipulations.

Statistical Measures:

Traditional forgery detection methods also relied on statistical measures to identify anomalies within images. These measures encompassed a range of statistical properties, including pixel intensity distributions, spatial correlations, and higher-order statistics. By quantifying deviations from expected statistical distributions, these methods aimed to flag regions of an image that exhibited irregular behavior indicative of tampering. However, their performance could be influenced by factors such as lighting conditions, image content, and the specific characteristics of the forgery.

Challenges and Limitations:

While traditional image forgery detection methods demonstrated effectiveness in certain scenarios, they faced significant challenges in adapting to the complexities of modern forgery techniques. With the proliferation of advanced image editing tools and sophisticated manipulation algorithms, traditional methods often struggled to reliably detect subtle alterations or forgeries designed to evade detection. Moreover, the increasing prevalence of high-resolution images and the rapid evolution of digital media presented new challenges for traditional techniques, which may have been designed with older, lower-resolution imagery in mind.

2.2 ELA and Forensic Tools

Error Level Analysis (ELA) has emerged as a popular post-processing technique in digital image forensics, offering valuable insights into the compression history of an image. By analyzing the discrepancies in compression artifacts across different regions of an image, ELA can help identify areas that have undergone multiple save operations or digital alterations. This technique has been widely adopted by forensic analysts and researchers alike for detecting various forms of image manipulation, including copy-move, splicing, and retouching.

ELA operates on the principle that different compression levels are applied to regions of an image during successive save operations. By resaving an image with a known compression level and comparing it to the original, ELA highlights areas with inconsistencies in compression artifacts, indicating potential tampering. This process allows forensic examiners to pinpoint suspicious regions for further analysis, guiding subsequent investigations into the authenticity of the image.

In addition to ELA, forensic tools such as Adobe Photoshop's Content-Aware Fill have played a significant role in tampering detection. Content-Aware Fill is a powerful feature that enables users to seamlessly remove or replace objects within an image by intelligently filling in the surrounding areas based on the image content. While Content-Aware Fill can be a valuable tool for digital editing and retouching, it has also been leveraged by forensic analysts to detect tampered regions.

However, despite the utility of ELA and forensic tools like Content-Aware Fill, they often lack the automation and scalability offered by deep learning techniques. ELA requires manual inspection and interpretation of compression artifacts, making it labor-intensive and time-consuming, especially when dealing with large datasets or high-resolution images. Similarly, while Content-Aware Fill can identify potential tampering, it may not always provide definitive evidence or detect subtle manipulations that evade visual inspection.

The advent of deep learning has revolutionized the field of digital image forensics by enabling automated and scalable approaches to tampering detection. Deep learning models, particularly convolutional neural networks (CNNs), have demonstrated remarkable performance in identifying forged or manipulated images, leveraging large datasets and powerful computational resources to learn complex patterns and features indicative of tampering. By training on diverse sets of authentic and manipulated images, deep learning models can generalize well to detect a wide range of forgery techniques with high accuracy and efficiency.

2.3 Deep Learning Approaches

The integration of deep learning, particularly convolutional neural networks (CNNs), has catalyzed a significant leap in the field of image forgery detection. Unlike traditional methods that rely on handcrafted features and heuristic approaches, deep learning models have demonstrated unparalleled capabilities in learning intricate patterns and features directly from raw image data.

Various deep learning architectures, such as MobileNet, VGG16, and ResNet, have been successfully applied to the task of image forgery detection. These architectures are characterized by their deep, hierarchical structures composed of multiple layers of convolutional and pooling operations, which enable them to learn increasingly abstract representations of image content.

MobileNet, for instance, is renowned for its efficiency and lightweight design, making it suitable for resource-constrained environments or real-time applications. Despite its compact size, MobileNet retains impressive performance in detecting forged or manipulated images, thanks to its depthwise separable convolutions and parameter-efficient design.

On the other hand, VGG16, with its deeper architecture comprising multiple convolutional layers followed by fully connected layers, excels in capturing fine-grained details and subtle features indicative of tampering. VGG16's ability to learn rich representations of image content has made it a popular choice for image classification, object detection, and forgery detection tasks.

One of the key advancements facilitated by deep learning is transfer learning, a technique that leverages pre-trained models on large datasets to expedite training and enhance model generalization. By initializing a deep learning model with weights learned from a large-scale dataset, such as ImageNet, and fine-tuning it on a smaller, domain-specific dataset of manipulated images, transfer learning enables the model to quickly adapt to the nuances of forgery detection.

Transfer learning not only accelerates the training process but also improves the robustness and performance of deep learning models by leveraging the rich representations learned from diverse visual concepts in the pre-trained network. This approach has been instrumental in democratizing deep learning for forgery detection, enabling researchers and practitioners with limited resources to achieve state-of-the-art results with minimal effort.

[1] Francesco Marra, Diego Gragnaniello, Luisa Verdoliva, Giovanni Poggi proposed a CNN-based image forgery detection framework designed to make decisions using full-resolution information gathered from the entire image. To overcome limited memory resources and rely on weak (image-level) supervision, the framework incorporates gradient checkpointing, enabling end-to-end training.

The architecture consists of three independent blocks: patch-level feature extraction, feature aggregation, and decision. Each block is trained separately. Xception, a deep learning model known for its performance in image-related tasks, is utilized in the framework.

The research reports an average AUC (Area Under the Curve) of 0.824, suggesting promising performance in the detection of forged images.

[2] A-Rom Gu; Ju-Hyeon Nam; Sang-Chul Lee proposed a forgery localization approach using a Discrete Cosine Transformation (DCT)-based multi-task learning network called FBI-Net.

The network is designed for forgery detection and includes an encoder-decoder model capable of end-to-end learning. DCT filtering is employed to extract frequency information from the input images, and a technique called DFSAM (DCT Filtering and Spatial Attention Module) is used to combine these features, emphasizing the traces of the forged region. Additionally, a pre-trained segmentation model is integrated to guide the location of specific forged objects during the decoding process.

The proposed FBI-Net achieves a promising F1-score of 76.98%, indicating effective forgery localization and detection performance.

[3] Ali, S.S.; Ganapathi, I.I.; Vu, N.-S.; Ali, S.D.; Saxena, N.; Werghi, N. proposed a robust deep learning-based system tailored for identifying image forgeries in the context of double image compression. The proposed system features a lightweight CNN model with minimal parameters, comprising three convolutional layers and a dense fully connected layer.

Despite its simplicity, the model achieves a commendable accuracy of 92.23%, highlighting its effectiveness in accurately detecting forged images subject to double compression. The emphasis on robustness and efficiency makes this system a potentially valuable tool in the field of digital forensics, particularly for scenarios involving manipulated images with multiple compression stages.

[4] A. H. Khalil, A. Z. Ghalwash, H. A. -G. Elsayed, G. I. Salama and H. A. Ghalwash proposed technique which focuses on identifying forged areas in digital images by leveraging the differences in compressed quality between the manipulated region and the rest of the image.

A deep learning-based model is employed to detect forgery by calculating the dissimilarity between the original image and its compressed counterpart. The process involves generating a featured image, which serves as input to a pre-trained model for training. Subsequently, the model's classifier is removed, and a new classifier is fine-tuned.

The technique is tested against various frameworks, with three of the best performers being VGG19, MobileNet, and ResNet50, achieving detection accuracy rates of 94.77%, 94.69%, and 94.6%, respectively. MobileNet is highlighted for its optimal balance between high detection accuracy and minimal computational costs and training time. This approach demonstrates promise in effectively detecting image forgeries, particularly in scenarios where compressed quality discrepancies reveal manipulated regions.

[5] Sudiatmika, Ida & Rahman, Fathur & Trisno, Trisno & Suyoto, Suyoto employed Deep Learning techniques VGG16 to discern manipulations in images. The dataset consists of both manipulated images and authentic ones, and Error Level Analysis (ELA) is applied to each image, accompanied by supporting parameters for error rate analysis. The experimental outcomes reveal compelling results, showcasing a noteworthy accuracy of 92.2% during training and 88.46% in validation after 100 epochs. This signifies the effectiveness of their approach in accurately identifying manipulated images, demonstrating the potential of combining Deep Learning and ELA for image forgery detection.

2.4 Datasets for Training

The availability of diverse datasets, such as CASIA and ImageNet, has played a pivotal role in training deep learning models. These datasets encompass a wide range of forgery scenarios, aiding models in learning features that generalize well to different types of image manipulation.

2.5 Challenges and Future Directions

Despite the advancements, challenges persist, including the detection of adversarial attacks and unseen manipulation techniques. Future directions involve exploring more robust architectures, incorporating domain-specific knowledge, and addressing ethical considerations in image forensics.

The evolution of image forgery detection reflects a transition from rule-based methods to data-driven approaches, with deep learning at the forefront. The exploration of diverse datasets and the continuous refinement of model architectures underscore the dynamic nature of research in this domain.

3. PROPOSED METHOD

In the realm of digital content, image forgery has become a pressing issue due to the widespread availability of sophisticated editing tools. Originally intended for image enhancement, these tools are now frequently misused to manipulate images, raising concerns about misinformation, deception, and malicious intent. Image forgery manifests in various forms, including common techniques like copy-move forgery and splicing, where parts of an image are duplicated or combined to create deceptive visuals.

To address these challenges, the integration of deep learning techniques, particularly convolutional neural networks (CNNs), has shown great promise in the field of image forensics. Deep learning models excel in pattern recognition and feature extraction, enabling them to detect subtle alterations within images effectively. The fundamental concept is to equip machines with the capability to autonomously distinguish between authentic and manipulated images.

By utilizing a diverse dataset representing real-world scenarios, deep learning models like VGG, Resnet, MobileNet can learn complex patterns indicative of forgery. During training, the model is exposed to both genuine and manipulated images, enabling it to identify features that traditional methods might overlook.

Deep learning architectures play a pivotal role in image forgery detection, offering diverse trade-offs between model complexity, computational requirements, and detection performance. Among the prominent architectures, VGG, ResNet, and MobileNet stand out for their distinct characteristics and applicability in forensic applications.

VGG (Visual Geometry Group):

VGG is renowned for its depth and simplicity, comprising multiple layers of convolutional and pooling operations stacked sequentially. While VGG achieves impressive performance in capturing fine-grained details and complex patterns in images, its architectural complexity comes at a cost in terms of computational requirements and memory footprint. The sheer number of parameters in VGG models, particularly VGG16 and VGG19, necessitates substantial computational resources for training and inference. Additionally, the computational overhead associated with processing high-resolution images or large datasets can further exacerbate the computational burden of VGG models, limiting their scalability and real-time applicability.

ResNet (Residual Neural Network):

ResNet introduced a groundbreaking architectural innovation with the concept of residual connections, which alleviate the vanishing gradient problem and facilitate the training of extremely deep networks. Despite its remarkable performance in achieving state-of-the-art results on various computer vision tasks, ResNet's depth and parameter count render it computationally intensive, especially for training from scratch on large datasets. The deep stacking of residual blocks in ResNet architectures, such as ResNet50 and ResNet101, requires significant memory resources and computational power, making them less practical for resource-constrained environments or applications with stringent latency requirements.

MobileNet:

In contrast to VGG and ResNet, MobileNet offers a lightweight and efficient alternative tailored for deployment on resource-constrained devices or scenarios where computational efficiency is paramount. MobileNet achieves its efficiency through depthwise separable convolutions, which factorize standard convolutions into depthwise and pointwise convolutions, significantly reducing the number of parameters and computational cost while preserving representational capacity. This design choice not only minimizes the memory footprint and computational overhead of MobileNet models but also accelerates inference speed, making them well-suited for real-time applications, edge computing, and mobile platforms.

The efficiency and scalability of MobileNet models make them particularly attractive for image forgery detection tasks, where rapid processing of large volumes of image data is essential. Compared to VGG and ResNet, MobileNet models offer a compelling balance between detection performance and computational efficiency, enabling forensic analysts to deploy sophisticated forgery detection systems on diverse hardware platforms with minimal computational overhead. Moreover, the lightweight nature of MobileNet models facilitates their integration into embedded systems, IoT devices, and cloud-based services, democratizing access to state-of-the-art forgery detection capabilities across various domains.

In conclusion, the choice of deep learning architecture for image forgery detection depends on a careful consideration of factors such as computational requirements, detection performance, and deployment constraints. While VGG and ResNet offer exceptional accuracy and representational capacity, their computational demands may limit their applicability in resource-constrained environments. On the other hand, MobileNet's lightweight design and computational efficiency make it an attractive option for real-time forgery detection, enabling scalable and cost-effective solutions that can be deployed across a wide range of platforms and scenarios.

MobileNetV3, the latest iteration of the MobileNet architecture, is optimized for efficient deployment on mobile and edge devices with computational constraints. Introduced to enhance performance over MobileNetV1 and MobileNetV2, MobileNetV3 incorporates novel architectural elements to strike a balance between model accuracy and efficiency. Introduced in the paper "Searching for MobileNetV3" by Andrew Howard et al. [6], MobileNetV3 employs neural architecture search to produce variants like "Large" and "Small" models. It features efficient inverted residual blocks, innovative activation functions like Swish, and Squeeze-and-Excitation blocks for improved feature extraction. MobileNetV3 achieves enhanced accuracy while maintaining computational efficiency, making it ideal for real-time applications such as object detection and image segmentation. Its versatility is evident in the range of variants tailored to different deployment scenarios.

The application of deep learning in image forgery detection reflects the evolving landscape of artificial intelligence and its potential to bolster digital security. As these techniques progress, they offer robust solutions to combat the increasing sophistication of image manipulation tools, promising a more secure digital environment.

In the proposed method for image forgery detection, we harness the power of transfer learning from deep learning models alongside the integration of forensic tools such as Error Level Analysis (ELA). Transfer learning offers a potent strategy for leveraging the knowledge gained from large-scale datasets by pre-trained deep learning models. These models, such as MobileNet, VGG16, or ResNet, have been extensively trained on diverse image datasets like ImageNet, enabling them to extract intricate features from images. By employing transfer learning, we can capitalize on the learned representations encoded in these models and adapt them to the forgery detection task. This involves fine-tuning the top layers of the pre-trained network while preserving the lower layers, which serve as feature extractors. Through this process, the model learns to discern subtle patterns indicative of image forgeries, enhancing its detection capabilities.

Alongside transfer learning, we integrate forensic tools like Error Level Analysis (ELA) into the forgery detection pipeline. ELA serves as a valuable forensic technique for highlighting potential regions of tampering or manipulation within digital images. By analyzing the discrepancies in compression levels across different regions of an image, ELA can reveal artifacts introduced during image manipulation processes. These artifacts, often imperceptible to the human eye, provide valuable cues for identifying forged regions within an image. By incorporating ELA-enhanced features alongside deep learning-based representations, we aim to enrich the feature set used for forgery detection. This fusion of deep learning and forensic analysis techniques enables a holistic approach to image forgery detection, leveraging the strengths of both methodologies to enhance the model's accuracy and robustness. Through this synergistic integration, our proposed method aims to advance the state-of-the-art in digital forensics, enabling more effective detection and mitigation of image forgeries across various applications and domains.

3.1Proposed Algorithm

Input: Curated dataset with authentic and manipulated images.

Initialization: Choose a suitable deep learning architecture (e.g., MobileNetv3). Prepare a balanced dataset for training and evaluation.

Data Preprocessing: Standardize image dimensions (e.g., resize to 224x224 pixels). Augment dataset using zooming, shifting, and shearing for diversity. Applying ELA on the images.

Transfer Learning: Utilize a pretrained MobileNetv3 on a large-scale dataset. Fine-tune the model for forgery detection using the curated dataset.

Training: Split dataset into training and test sets. Train the model with optimization techniques (e.g., gradient clipping, batch normalization). Use binary cross-entropy as the loss function.

Evaluation: Assess model using accuracy, precision, recall, and F1-score metrics. Ensure robustness across various forgery scenarios.

Result Analysis: Analyse accuracy on the test dataset. Identify areas for potential improvement.

Further Optimization: Explore techniques to enhance accuracy, addressing false positives and false negatives. Iterate on the algorithm based on analysis and feedback.

Output: Reliable forgery detection and localization algorithm.

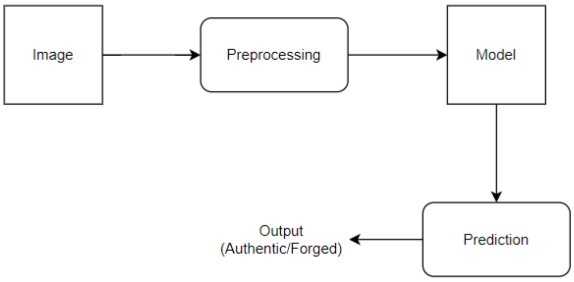

Fig 1 Flow of the proposed model

4. Conclusion

The proposed algorithm addresses the challenge of image forgery detection by leveraging the capabilities of deep learning, specifically employing the MobileNetv3 architecture. Through a meticulous data preprocessing phase, including resizing and augmentation, a curated dataset is prepared, ensuring the model's exposure to diverse forgery scenarios. Transfer learning is applied, utilizing a pretrained MobileNetv3 model to expedite training and capture intricate features relevant to forgery detection.

In conclusion, this survey paper highlights the synergistic potential of integrating transfer learning from deep learning models and forensic tools like Error Level Analysis (ELA) for image forgery detection. Through an extensive review of existing research and methodologies in the field, we have observed that both transfer learning and forensic analysis techniques offer unique advantages and capabilities in identifying image forgeries.

Transfer learning enables the adaptation of knowledge learned from pre-trained deep learning models to new tasks, significantly enhancing the efficiency and effectiveness of forgery detection algorithms. By leveraging the rich feature representations learned by these models on large-scale datasets, transfer learning empowers forgery detection systems to capture subtle patterns and anomalies indicative of image manipulations.

On the other hand, forensic tools like ELA provide valuable insights into the compression history of digital images, revealing potential regions of tampering or manipulation. ELA operates on the principle of analyzing differences in compression levels within an image, allowing forensic analysts to identify suspicious areas that may require further investigation.

By combining the strengths of transfer learning and forensic tools like ELA, we believe that forgery detection systems can achieve unprecedented levels of accuracy, robustness, and adaptability. The integration of deep learning-based feature extraction with forensic analysis techniques offers a holistic approach to image forensics, enabling the detection of a wide range of forgery types and manipulation methods.

In summary, our survey paper underscores the significance of collaborative efforts between transfer learning and forensic tools in advancing the field of image forgery detection. We advocate for further research and development in this interdisciplinary domain, with the aim of creating more sophisticated and reliable forgery detection systems capable of addressing the evolving challenges posed by digital manipulation techniques.

REFERENCES

[1] F. Marra, D. Gragnaniello, L. Verdoliva and G. Poggi, "A Full-Image Full-Resolution End-to-End-Trainable CNN Framework for Image Forgery Detection," in IEEE Access, vol. 8, pp. 133488-133502, 2020.

[2] A. -R. Gu, J. -H. Nam and S. -C. Lee, "FBI-Net: Frequency-Based Image Forgery Localization via Multitask Learning With Self-Attention," in IEEE Access, vol. 10, pp. 62751-62762, 2022.

[3] Ali, S.S.; Ganapathi, I.I.; Vu, N.-S.; Ali, S.D.; Saxena, N.; Werghi, N. Image Forgery Detection Using Deep

Learning by Recompressing Images. Electronics 2022, 11, 403.

[4] A. H. Khalil, A. Z. Ghalwash, H. A. -G. Elsayed, G. I. Salama and H. A. Ghalwash, "Enhancing Digital Image Forgery Detection Using Transfer Learning," in IEEE Access, vol. 11, pp. 91583-91594, 2023.

[5] Sudiatmika, Ida & Rahman, Fathur & Trisno, Trisno & Suyoto, Suyoto. (2018). "Image forgery detection using error level analysis and deep learning". TELKOMNIKA (Telecommunication Computing Electronics and Control).

[6] A. Howard et al., "Searching for MobileNetV3," 2019 IEEE/CVF International Conference on Computer Vision (ICCV), Seoul, Korea (South), 2019, pp. 1314-1324, doi: 10.1109/ICCV.2019.00140.

[7] Dertat, A. Review: MobileNetV2—Light Weight Model (Image Classification).. Available online: https://towardsdatascience.com/review-mobilenetv2-light-weight-model-image-classification-8febb490e61c (accessed on 19 May 2019) .

[8] Elsayed Abd Elaziz, Mohamed & Al-qaness, Mohammed A. A. & Dahou, Abdelghani & Alsamhi, Saeed & Abualigah, Laith & Ibrahim, Rehab & Ewees, Ahmed. (2023). "Evolution toward intelligent communications: Impact of deep learning applications on the future of 6G technology." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 14. 10.1002/widm.1521.

[9] Cheuque, César & Querales, Marvin & León, Roberto & Salas, Rodrigo & Torres, Romina. (2022). "An Efficient Multi-Level Convolutional Neural Network Approach for White Blood Cells Classification." Diagnostics. 12. 248. 10.3390/diagnostics12020248.

[10] Ayoub Kirouane 2022, LinkedIn, accessed 2 February 2024, <https://www.linkedin.com/pulse/squeeze-and-excitation-networks-senet-ayoub-kirouane/>

[11] Kaur, Amanpreet and Richa Sharma. "Optimization of Copy-Move Forgery Detection Technique." Computer Engineering and Applications 2 (2013): n. pag.

[12] Islam, M.M.; Karmakar, G.; Kamruzzaman, J.; Murshed, M. A Robust Forgery Detection Method for Copy–Move and Splicing Attacks in Images. Electronics 2020, 9, 1500. https://doi.org/10.3390/electronics9091500