Enhancing Digital Image Forensics with Error Level Analysis (ELA)

Robert Idlbek *, Mirko Pešić **, Krešimir Šolić ***
* J. J. Strossmayer University of Osijek, Faculty of Tourism and Rural Development, Croatia, Pozega,
** J. J. Strossmayer University of Osijek, Faculty of Medicine, Osijek, Croatia
*** J. J. Strossmayer University of Osijek, Faculty of Medicine, Osijek, Croatia
ridlbek@ftrr.hr; kresimir@mefos.hr; mpesic@mefos.hr

Abstract — **Today, visual content's integrity is increasingly important. This paper focuses on Error Level Analysis (ELA), a pivotal technique in digital image forensics for detecting digital alterations in images. ELA analyzes variations in compression levels to identify inconsistencies that suggest manipulation. This paper outlines the fundamentals of ELA and its application in detecting forgeries. Also, it explores its integration with artificial intelligence (AI) and machine learning (ML) technologies to enhance forensic accuracy. The paper discusses the evolution of image manipulation techniques and the corresponding advancements in ELA that address these challenges.**

Also, the paper highlights recent innovations in ELA that improve its effectiveness and adaptability in the forensic investigation of digital images. In the end, it concludes with the prospective enhancements in forensic methods, emphasizing the necessity of ELA in maintaining digital authenticity in an era increasingly dominated by sophisticated image manipulation techniques.

Keywords - Error Level Analysis, Digital Forensic, Picture Analysis, Image Manipulation Techniques

I. Introduction

Digital and visual content accuracy has never been more important in a world where digital images are everywhere, and many different Image Forgery Detection Techniques are used (Fig.1.). In this this article, we will explore Error Level Analysis (ELA), a crucial technique in verifying digital images. ELA serves as a tool for detecting image changes, thus ensuring digital integrity and responsibility.

This paper starts with an introduction to ELA, explaining its principles and its significant role in forensics. After that, it breaks down how ELA works, showcasing its usefulness and limitations through examples and comparisons with forensic methods. As techniques for manipulating content become increasingly advanced, it is important to examine how ELA combines cutting-edge technologies like Artificial Intelligence (AI) and Machine Learning (ML). This fusion not only showcases what ELA can currently achieve but also predicts its development in strengthening the trustworthiness of digital media.

This paper considers the implications and urgent need for rigorous forensic techniques in today's digitally driven society. This introduction offers an overview of ELA in both today's and future contexts of digital image forensics, laying the foundation for a thorough exploration of how the technique is used, its challenges, and potential improvements in subsequent sections.

A. Related Work

The chosen literature references emphasize the growth and significance of ELA in image investigation while also focusing on its fusion with AI and ML. The literature selection process concentrates on relevant and recent academic papers that showcase the development of image alteration methods and the progress in forensic technologies to combat these alterations. They cover theories, recent technological advancements and practical studies that showcase the effectiveness of ELA and related technologies in different scenarios. This selection aims to establish a foundation for discussing ELAs current capabilities and future possibilities, ensuring that the document remains relevant for researchers and professionals in the digital forensics field.

For a beginning, it is crucial to define ELA. We can say that Error Level Analysis is a "forensic method to identify portions of an image with a different level of compression" [21]. ELA is a well-recognized algorithm in image processing, with numerous research papers underscoring its significance across various fields. The rise in digital image tampering has encouraged more studies in image forensics. In today's world, where pictures and videos are primary information carriers, the surge in forensic methods for image source identification and tamper detection is unsurprising. Initially, it is important to understand the process of acquiring digital images, so Fig. 2 presents a schematic view of a standard digital image acquisition pipeline.

According to Redi et al. [3], the leading fraud techniques include a) identification through artefacts produced during acquisition, b) identification through sensor imperfections, and c) source identification using properties of the imaging device. Many active and passive detection techniques are used to detect tampered images [2], and there is extensive literature on both broad and specific applications.

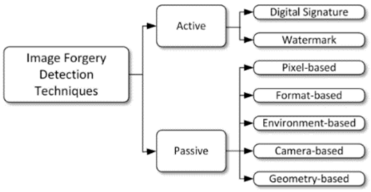


Figure 1. Image Forgery Detection Techniques [2]

As the use of temper detection techniques in image forensics increases, counter-forensic methods consistently rise. Some counter-forensic methods tend to include additions of digital noise to the manipulated photos since several temper detection techniques often rely on fluctuations in digital noise among the sections of a given image [3].

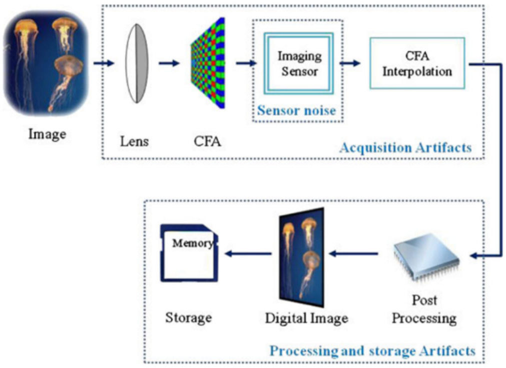


Figure 2. Schematic view of a standard Digital Image Acquisition Pipeline [4]

The most widespread format for digital pictures is JPEG. Therefore, the researchers wish to implement image forensics tools primarily for the JPEG algorithm. Bakiah Abd Warif [5] has assessed ELA against various tampering types such as JPEG compression, image splicing, copy-move, and retouching of images. Experiments involving JPEG compression, image splicing, and image retouching forgery have shown that ELA is reliable. This detection technique is intensively studied in digital image forensics because of its detection effectiveness in different types of tampering.

Jeronimo [6] improved ELA by filtering out its noisy parts using automatic wavelet soft thresholding, which is shown to be an effective method for detecting image forgery. This additional filter enhanced the detection of photo-edited pictures. In another important paper, Gunawan [2] developed a photo forensics algorithm that demonstrated excellent results in detecting photo manipulation using ELA and Artificial Intelligence. Furthermore, Morra [8] introduced a method that uses ELA as input for an AI-trained model to identify potential slicing frauds in pictures such as car license plates. These studies highlight the potential of ELA in digital image forensics, particularly in aiding the detection of various forms of image tampering and their possibility to be used with AI.

Although ELA has existed for years, it alone cannot expose fraud, and new researchers continue to improve the technique with its additions to other concepts. For instance, Azhan [9] studied a way to recognize the distinct signature of JPEG 8 × 8 blocks using ELA and tried to identify the efficiency of this approach in detecting characteristics of JPEG 8 × 8 blocks and its applicability for the analysis of fragmented JPEG files in digital forensics.

Quantization tables (QT) are essential for understanding JPEG compression, and quantization table–gradation can be seen in Fig. 3. They give a picture of using the JPEG compression rate in various parts of an image. As illustrated in [10], JPEG quantization affects the rate-distortion tradeoff by incorporating details on chroma downsampling, DCT and inverse DCT, and quantization and dequantization processes. QT is optimizable for several different scenarios, as indicated by manufacturers like Nikon and Olympus fine-tuning QTs for their photo sensors. Fine-tuning involves comparing default and optimized tables based on their effect on image quality metrics such as Peak signal-to-noise ratio (PSNR) and bits-per-pixel [12].

Artificial Intelligence (AI), its subset Machine Learning (ML) and Deep Learning (DL) have become embedded in various aspects of life. AI is now commonly used for image editing, applying real-time filters, and even producing photorealistic images through tools like Midjurney and Stable Diffusion. However, using open-source generative models for image generation carries risks, as these unregulated models might inadvertently train on banned content such as child pornography. However, the application of AI in digital image forensics demonstrates significant potential. Rafique [11] emphasizes the need for systems that can distinguish true from false content on social media, especially in the era of deep fakes. Utilizing DL and ML, this approach achieved an 89.5% accuracy rate in deep fake image classification using a Residual Network and K-nearest neighbour. That illustrates the technique's effectiveness in combating the spread of fake news and unwanted AI-generated content.

Several open and accessible databases, like RAISE and CASIA V1/V2, are available for studying image tampering and training DL algorithms. In digital image forensics, critical open-source databases like NIST offer extensive collections of images for testing integrity and authenticity [16]. The Dresden Image Database provides valuable data for camera-based forensic analysis [17]. At the same time, the RAISE dataset contributes a large number of high-quality raw images for forensic studies [14]. The DVMM Columbia Image Splicing Detection Evaluation Dataset, developed by Columbia University, marks progress in image splicing detection [15]. These resources, along with others, are fundamental in advancing the detection of image manipulation and verifying the authenticity of digital images in digital forensics.

These databases contain diverse images and are crucial in advancing forensic tools and refining AI-based models.

B. *Understanding Image Compression*

Image compression is an essential technique in digital image processing, especially for efficiently storing and transmitting images. The main goal is to reduce data redundancy, enabling better or more effective storage or transmission. There are two basic categories of image compression: lossless and lossy.

Lossless Compression ensures the perfect reconstruction of the original image from compressed data. That is vital in medical imaging or technical illustrations where preserving detail is crucial. Key algorithms include Run-Length Encoding (RLE), Huffman Coding, and Lempel-Ziv-Welch (LZW).

On the other hand, Lossy Compression reduces image sizes by irreversibly removing specific data, usually unnoticeable to the human eye. It is widely used in web graphics, video streaming, and digital cameras. Techniques include JPEG and Wavelet Compression. JPEG (Joint Photographic Experts Group) is the most common compression method that transforms images into a frequency domain through Discrete Cosine Transform (DCT), then quantizes frequency components to reduce precision before encoding efficiently.

Both lossless and lossy compressions often involve steps like colour space transformation (e.g., RGB to YCbCr), subsampling (reducing chrominance resolution), and entropy coding (data expression based on statistical properties).

The quality association in JPEG compressed files (e.g., 75%, 80%, 95%) is crucial in digital image forensics. JPEG compression processes each 8x8 pixel block with a Discrete Cosine Transform (DCT) variant—alterations in an image result in varying noise levels in different sections. Extracting and displaying this noise as a separate image makes it obvious where and how it has been modified.

Since 2017, advancements in artificial intelligence (AI) have led to the development of innovative algorithms for image compression, referenced in [19][20]. These state-of-the-art AI-based compression techniques utilize machine learning algorithms to enhance the efficiency of reducing image file sizes, surpassing traditional methods such as JPEG or PNG. In its training phase, the AI system is exposed to many images, enabling it to discern and preserve essential features during compression. This approach results in substantially smaller file sizes while retaining high image quality. Notably, the AI's capacity to adapt to specific types of images significantly augments its utility in specialized domains, including medical imaging. This advancement marks a considerable progression in managing digital image data, providing a balance between quality preservation and storage efficiency.

New research [18] in AI and image forensics discusses the impact of AI-based compression on JPEG-related image forensic detectors. So, AI-based compression can act as a counter-attack against these detectors.

II. Method

The present study was an analysis of 43 screen captures of PDF documents oriented towards data like payment confirmations and bookings involving technical and business resolutions. Since original and digitally signed PDFs were unavailable, the analysis aimed to determine whether these JPG screenshots recovered from analyzed disks were original or altered. The analysis of JPG file originality and image analysis for metadata was facilitated by the open-source tool Ghyro, which provides automated capabilities such as static analysis and metadata extraction. Additionally, an online forensic tool (https://29a.ch/photo-forensics) was referenced for Clone Detection, ELA, Noise Analysis, Level Sweep, and Luminance Gradient. Each photograph underwent ELA analysis to assess the likelihood of digital alteration. Four categories were established, each indicating a 25% probability of digital modification. The summary results are presented in Table I, categorizing each image into a range based on subjective assessment.

TABLE I. Image fraud candidate number

Analysis type	Image count			
	0≤P(A)<0.25	0.25≤P(A)<0.50	0.50≤P(A)<0.75	0.75≤P(A)≤1
ELA	22	15	4	2
Clone Detection	22	6	9	6
Noise Analysis	21	13	9	0
Level Sweep	24	12	8	0
Luminance Gradient	43	0	0	0
Principal Component Analysis	43	0	0	0

A. JPEG Compression Analysis

Next, a JPEG analysis was performed, followed by the Quantisation tables (QT) computation for all images. All analyzed images had the same QT0 and QT1. as seen in Fig. 4. That indicates that quality levels range from 99% to 100%, indicating minimal or no compression applied to the images. It is important to note that different tools calculate JPG compression levels differently. For instance, Adobe Photoshop generally shows higher compression levels compared to other tools, such as GIMP.

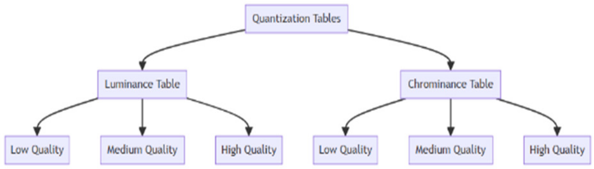
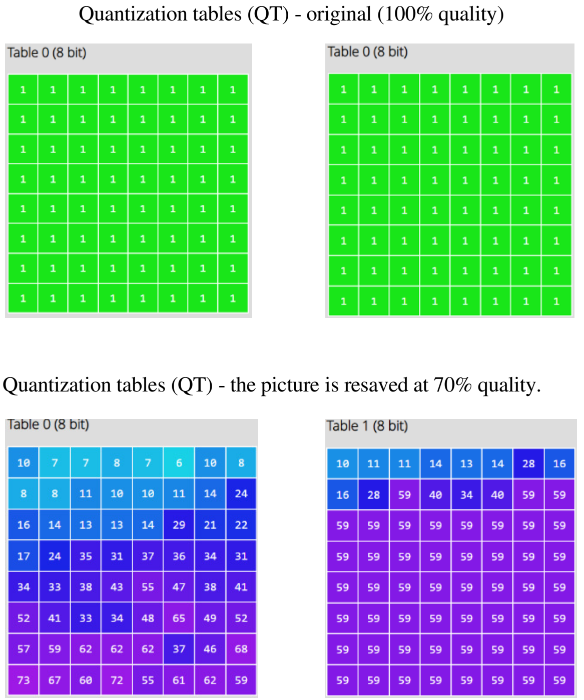


Figure 3. Quantization table – gradation



Quantization tables (QT) - original (100% quality)

Table 0 (8 bit)

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Table 0 (8 bit)

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

Quantization tables (QT) - the picture is resaved at 70% quality.

Table 0 (8 bit)

10	7	7	8	7	6	10	8
8	8	11	10	10	11	14	24
16	14	13	13	14	29	21	22
17	24	35	31	37	36	34	31
34	33	38	43	55	47	38	41
52	41	33	34	48	65	49	52
57	59	62	62	62	37	46	68
73	67	60	72	55	61	62	59

Table 1 (8 bit)

10	11	11	14	13	14	28	16
16	28	59	40	34	40	59	59
59	59	59	59	59	59	59	59
59	59	59	59	59	59	59	59
59	59	59	59	59	59	59	59
59	59	59	59	59	59	59	59
59	59	59	59	59	59	59	59
59	59	59	59	59	59	59	59

Figure 4. Quantization tables for detecting image quality

QT 1 and QT0 in JPEG quantization refer to Standard Quantisation Tables used in image compression. Typically, the JPEG format employs two basic types of quantization tables. These tables are distinct for luminance (light) and chrominance (colour) components. That allows the quality to be varied over those two components. QT1 represents the chromatic (colour) components, permitting more compression for colours since the human eye is less sensitive to changes in colour. All elements of these tables indicate the number 1, signifying no compression (Q=100%), which is atypical for image processing tools where the typical value is Q=70%-85%. The analyzed image, resaved with higher compression (Q=75%), shows different Quantization Tables, as seen in Fig. 4.

B. Digital Noise Analisys

Using the Noise Analysis tool (settings: Noise Amplitude: 10, Equalize Histogram (true), Magnifier Enhancement: Histogram Equalization, Opacity=0.95), noticeable noise levels were detected, as evident in Fig. 5. These include digital noise pixels typical of chromatic noise, which are varied.

There are three types of digital noise [18][13]: (1) chromatic noise, (2) luminance noise, and (3) colour-specific noise. Chromatic noise is often seen as random coloured pixels (red, green, blue). Chromatic noise usually arises due to sensor errors or signal processing, which is more visible in darker parts of a photo. That affects the perception of colours and the overall visual quality of the image. Adding such noise in post-production (after image tempering) by hand can reduce the accuracy of ELA and other forensic-analytical methods.

Fig. 5 shows Chromatic Digital noise in one of the analyzed documents, and Fig. 6 shows ELA analysis for that same document.

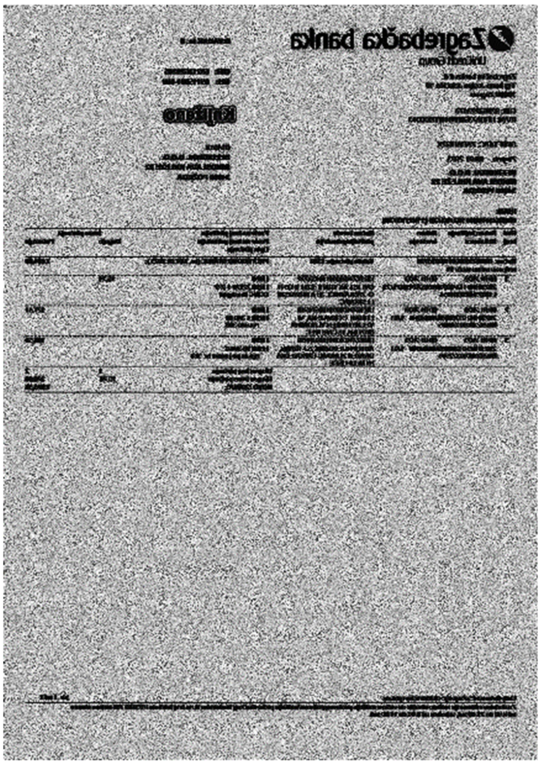


Figure 5. Chromatic Digital Noise in Document Screenshot

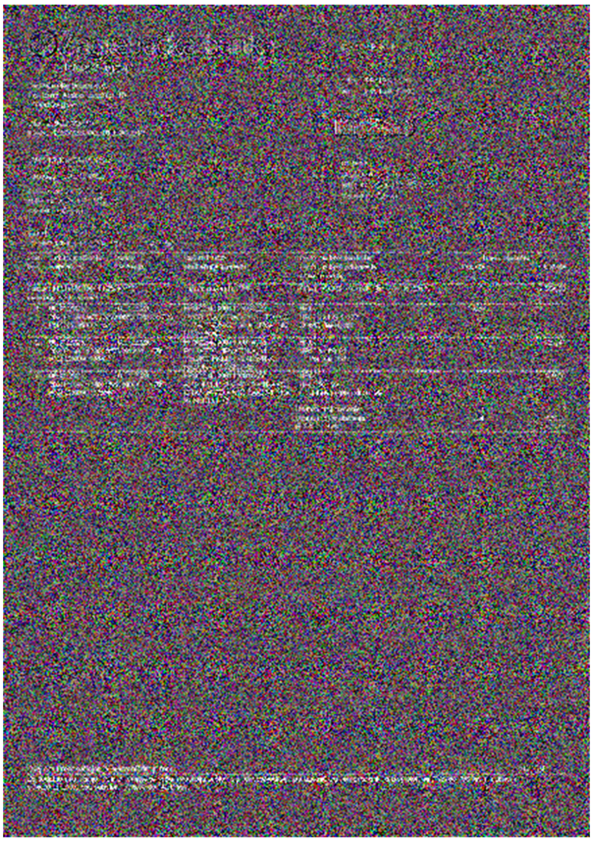


Figure 6. ELA Analysis in Document Screenshot

III. Results

No analysis performed above could provide a conclusive result as to whether these images were altered or not. Each analysis offered a different perspective on the documents, but none had sufficient information for a definitive conclusion about alterations. The ELA analysis, which should not be used in isolation but instead complemented with other analytical methods, showed no signs of changes in the business document images.

However, the noise level analysis did not raise questions about the authenticity of these documents, and the analysis method did not attribute to quantization tables. It is illogical that a screenshot from an existing document would have 1) a high noise level and 2) a JPEG quality level equal to 100%.

A. JPEG Compression Analysis

It is unusual for a JPEG file to be saved at 100% quality. The quality or compression percentage is typically 70-85% in most applications, representing the best quality and file size balance. A file saved at 100% quality is likely intended for professional use, such as large-format printing.

Utilizing a JPEG format with a 100% quality setting, equating to zero compression is atypical due to the disproportionate increase in file size without a corresponding perceptible enhancement in image quality. The JPEG algorithm is specifically designed for efficient storage and transfer, and its use at full quality negates this advantage, resulting in unnecessarily large files. Moreover, most software defaults to some compression, reflecting common usage scenarios. For scenarios requiring lossless storage, formats like PNG or TIFF are preferred, as they preserve image data without the artefacts associated with JPEG compression. Consequently, employing 100% quality JPEGs is not standard practice. It is often avoided in favour of more size-efficient and visually comparable compression levels or alternative lossless formats.

In conclusion, the person who altered the image likely inadvertently chose to save the document at 100% quality.

B. *Digital Noise Analysis*

Analyzing and removing digital noise is essential for maintaining digital image quality. Noise is a pretty common issue in digital photography. It can be caused by many things, like high ISO settings, long exposures, shooting in low light, the size and quality of the camera sensor, and even how the image is processed afterwards. Sometimes, increasing the sharpness or exposure in editing can worsen any existing noise.

It is interesting to note that when it comes to photos taken with a camera, some sensors have a unique digital footprint that can be identified. However, it is a different story when discussing a screenshot from a PDF document. Screenshots do not involve a digital sensor, so any noise in them would likely come from how they were processed after being taken.

Now, when it comes to tools like ELA, they can usually detect changes in the noise levels in different parts of an image, significantly if it has been altered in several layers. However, if digital noise is artificially added, it can make these forensic tools less useful. That means that noise in a screenshot from a PDF, like in the 43 analyzed pictures, has been added in post-production.

IV. Discussion

The need to conduct forensic analyses of digital photographs and deepfake videos will become increasingly prevalent. Unfortunately, today's forensic tools, although advanced, actually represent a collection of methods (analyses) that can be applied, but much manual work is required to perform the analysis. That often includes using analytical software from various vendors or open-source tools.

Analytical methods such as ELA should not be used as the sole analytical method, nor is it perfect, as it can be deceived in various ways and ultimately depends on the subjective assessment of the person conducting the analysis. One of its partial limitations is its application only to lossy compressed content.

The application of AI, particularly Deep Learning and Neural Networks (especially Convolutional Neural Networks, CNNs), has proven to be an efficient method for image analysis. Models trained on large datasets (images) such as CASIA can detect complex patterns and anomalies indicative of manipulation. The combination of neural networks, various additional analysis tools, and the ELA method seems like a good foundation for further developing applied artificial intelligence for digital forensics needs. For example, Zhang et al. [20] showed that combining ELA with Convolutional Neural Network (CNN) can significantly improve the accuracy of image fraud detection. That means that the characteristics identified in images by the Error Level Analysis (ELA) method are adequate for determining whether an image is authentic.

It should be borne in mind that these methods are very new. However, even the current AI and ELA method application models dramatically accelerate the training speed of CNN models. It is important to note that the achieved acceleration does not reduce the accuracy of recognition while at the same time significantly reducing the need for CPU power (up to 90% less need for floating-point computing power).

There is an explosion of new AI tools for manipulating images, audio, and video. Artificial Intelligence is creating entirely new illustrations and photorealistic images (Midjourney, DaLL-E, Stable Diffusion), enhancing existing images (Remini AI, Fotor), voice generators (Lovo.Ai, Speechify), and creating deepfake videos (DeepFakeLab, Reface). Additional uncertainty is introduced by the increasingly present AI-based tools that allow training neural network models on local computers using powerful graphics cards (GPUs), even without the need for an internet connection. Therefore, it can be expected that it will be necessary to digitally verify many information sources for authenticity, as mentioned in the Introduction part of this work.

Introducing new AI models for forgery detection could be integral to future operating systems. For example, the minimal requirements for Windows 12 could be set to 40 TOPS (tera operations per second) precisely because of locally executable AI operations [7]. In the future, the operating system could alert users to potential deepfake videos or retouched digital photographs.

Integrating these technologies could lead to more user-friendly tools for image verification, accessible not only to experts but also to journalists, law enforcement, and the general public.

V. Conclusion

After reviewing the discussions in this paper, it is evident that Error Level Analysis (ELA) plays a vital role in image forensics. It remains a tool for identifying inconsistencies in JPEG compression levels indicating alterations. However, it is recommended that ELA need to be used alongside other methods for more comprehensive results. Furthermore, integrating artificial intelligence (AI) and machine learning (ML) technologies shows potential for enhancing analyses by detecting subtle image details that human analysts might miss. This combination of technologies with ELA could lead to the development of practical tools to combat digital manipulation effectively.

The future of image forensics is heading towards developing intelligent tools that can learn and improve by analyzing new data and forgery techniques. By integrating AI, repetitive tasks can be automated, and detailed analysis of image alterations can be done more efficiently, leading to quicker and more precise evaluations. Standardized open-source tools and databases will make forensic practices more accessible and consistent across regions.

One of the challenges faced by forensic methods, such as ELA, is keeping up with the ever-changing landscape of image manipulation techniques. To overcome this challenge, ongoing research should focus on enhancing the adaptability and learning capabilities of AI-driven tools. Moreover, establishing frameworks to govern the use of AI in forensics is essential to ensure that privacy rights are protected and to prevent wrongful accusations.

Additionally, analysts' training programs must include AI and machine learning modules to prepare professionals to utilize these technologies.

In conclusion, ELA continues to play a role in image forensics. However, the future seems to involve more effort with AI and ML. By adopting these technologies, forensic science can match the progress made in image manipulation. This forward-thinking approach will be essential in safeguarding the authenticity of content amid the evolving digital environment.

References

[1] Farid, H. “Digital image forensics.” Scientific American 298 6 (2008): 66-71.

[2] Gunawan, Teddy Surya et al. “Development of photo forensics algorithm by detecting Photoshop manipulation using error level analysis.” Indonesian Journal of Electrical Engineering and Computer Science 7 (2017): 131-137.

[3] Stamm, Matthew C. and K.J.R. Liu. “Anti-forensics of digital image compression.” IEEE Transactions on Information Forensics and Security 6 (2011): 1050-1065.

[4] Redi, Judith et al. “Digital image forensics: a booklet for beginners.” Multimedia Tools and Applications 51 (2010): 133-162.

[5] N. B. A. Warif, M. Y. I. Idris, A. W. A. Wahab and R. Salleh, “An evaluation of Error Level Analysis in image forensics,” 2015 5th IEEE International Conference on System Engineering and Technology (ICSET), Shah Alam, Malaysia, 2015, pp. 23-28, doi: 10.1109/ICSEngT.2015.7412439.

[6] Jeronymo, Daniel Cavalcanti, Yuri Campbell and Leandro dos Santos Coelho. “Image forgery detection by semi-automatic wavelet soft-Thresholding with error level analysis.” Expert Syst. Appl. 85 (2017): 348-356.

[7] Vrbanus, S. "Windows 12: veći zahtjevi za resursima zbog uvođenja Copilota", Accessed: Jan. 22, 2024 [Online]. Available: https://www.bug.hr/operacijski-sustavi/windows-12-veci-zahtjevi-za-resursima-zbog-uvodjenja-copilota-37717

[8] Morra, E., et al., “A method for image forgery detection based on Error Level Analysis (ELA),” in Knowledge Innovation Through Intelligent Software Methodologies, Tools and Techniques: Proceedings of the 19th International Conference on New Trends in Intelligent Software Methodologies, Tools and Techniques (SoMeT_20), vol. 327, IOS Press, 2020.

[9] Azhan, Nor Amira Nor, et al. “Error Level Analysis technique for identifying JPEG block unique signature for figital forensic Analysis.” Electronics 11.9 (2022): 1468.

[10] “The rate-distortion-accuracy tradeoff: JPEG case study,” ar5iv.org, 2020. [Online]. Available: https://ar5iv.org/abs/2008.00605. [Accessed: Jan. 24, 2024].

[11] Rafique, R., Gantassi, R., Amin, R. et al. “Deep fake detection and classification using error-level analysis and deep learning”. Sci Rep 13, 7422 (2023). https://doi.org/10.1038/s41598-023-34629-3

[12] S. Annam i A. Singla, “Correlative analysis of denoising methods in spectral images embedded with different noises,” u 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, str. 318-323. doi: 10.1109/PDGC50313.2020.9315749.

[13] Farace and B. Staver, Better available light digital photography: how to make the most of your night and low-light shots, CRC Press, 2008.

[14] D. T. Dang-Nguyen, C. Pasquini, V. Conotter, and G. Boato, “Raise: A raw images dataset for digital image forensics,” in Proc. of the 6th ACM Multimedia Systems Conference, Mar. 2015, pp. 219-224.

[15] Z. Moghaddasi, “Image splicing detection approach based on low dimensional SVD features and kernel PCA,” Ph.D. dissertation, Univ. of Malaya, Malaysia, 2017.

[16] T.-T. Ng, J. Hsu, and S.-F. Chang, “Columbia image splicing detection evaluation dataset,” DVMM Lab, Columbia Univ., New York, NY, USA, Report, 2009.

[17] T. Gloe and R. Böhme, “The ‘Dresden Image Database’ for benchmarking digital image forensics,” in Proc. of the 2010 ACM Symposium on Applied Computing, 2010, pp. 1584-1590.

[18] Ballé, Johannes, et al. "Variational image compression with a scale hyperprior." *arXiv preprint arXiv:1802.01436* (2018).

[19] Li, Mu, et al. “Learning convolutional networks for content-weighted image compression.” *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2018.

[20] W. Zhang, C. Zhao, and Y. Li, “A novel counterfeit feature extraction technique for exposing face-swap images based on deep learning and error level analysis,” Entropy, vol. 22, no. 2, p. 249, 2020.

[21] Paganini, P. “Photo forensics: Detect photoshop manipulation with error level analysis,” Infosec Institute, Oct. 25, 2013. [Online]. Available: https://www.infosecinstitute.com/resources/digital-forensics/error-level-analysis-detect-image-manipulation/. [Accessed: Apr. 3, 2024].