Error Level Analysis (ELA)

DEJAN N. RAKOVIĆ, University of Belgrade
School of Electrical Engineering, Belgrade

Review paper
UDC: 004.932.342
779.026.342:343.98
DOI: 10.5937/tehnika2304445R

ELA (Error Level Analysis) is a digital image analysis technique that has gained popularity in recent years in the field of modern forensics. It is a powerful method that can help experts determine if an image has been altered or manipulated in any way. ELA works by analyzing the levels of compression within an image and identifying areas that have been edited or manipulated at a different level than the rest of the image. This information can be crucial in criminal investigations, where the authenticity of an image can be key to solving a case. In this article, we will explore the use of ELA in modern forensics, its benefits, and limitations, as well as its potential impact on the future of forensic investigation.

Key Words: *Digital, Forensics, ELA, Error, Level, Analysis*

1. INTRODUCTION

Error Level Analysis (ELA) is a powerful digital forensics technique that helps in identifying image tampering or manipulation. ELA works by comparing the level of error introduced into an image during its compression process. During the compression of an image, the JPEG algorithm divides the image into blocks, and each block is compressed with varying degrees of error. ELA detects these differences in error levels and highlights the parts of the image that have been altered, revealing any potential tampering. ELA calculates the difference between the original image and a re-saved version of the image. The re-saved version is compressed with a similar amount of compression as the original image. The difference between the original image and the re-saved image shows the amount of error introduced by the compression process. In areas of the image that are unchanged, the error level is low, while in areas that have been manipulated, the error level is high. ELA uses a threshold value to determine the areas of the image that have been manipulated. Typically, the threshold value is set at a percentage of the maximum error level. Any areas of the image that exceed this threshold value are highlighted as potentially tampered with. ELA also uses a color mapping technique to highlight the areas of the image that have been manipulated. Typically, unchanged areas of the image are highlighted in blue, while areas with higher error levels are highlighted in red. This color map makes it easy for a forensic investigator to quickly identify the areas of the image that have been tampered with. ELA algorithms work by analyzing the compression levels of the image. By comparing the compression levels of different parts of the image, ELA can identify the areas that have been tampered with. The algorithms used by ELA are based on the principle that the error introduced during compression is proportional to the difference between the original and re-saved image. Figure 1 will display the unaltered photograph prior to undergoing photo manipulation, with the addition of the vessel depicted in Figure 2.

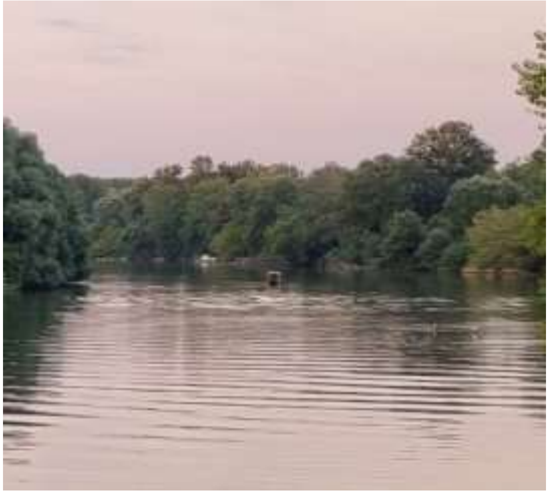

Figure 1 – Original image

Author's address: Dejan Raković, University of Belgrade, School of Electrical Engineering, Belgrade, Bulevar kralja Aleksandra 73

e-mail: rakovicdejan@outlook.com

Paper received: 28.03.2023.

Paper accepted: 23.06.2023.

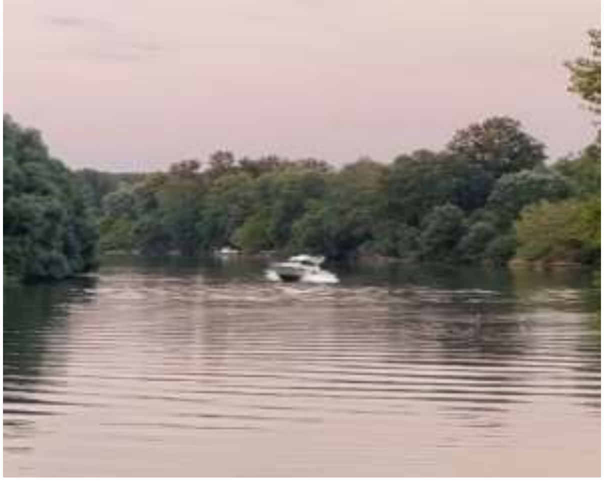

Figure 2 – Altered version

2. MANUAL METHOD

To ensure the reliable application of the Error Level Analysis (ELA) method through manual means, it is essential to follow a strict procedural guideline. A trained forensic expert is required to execute the following steps: Identify the image file to be analyzed and make a copy of the original file. This step is necessary to avoid any accidental alterations to the original file. Open the image file in a photo editing software, such as Adobe Photoshop, and save a copy of the image in a lossless format, such as TIFF or PNG. This process preserves the original quality of the image and ensures that no data is lost during analysis. Open the saved copy of the image and resave it as a compressed format, such as JPEG, with a compression level of 80-90%. This step simulates the natural compression that occurs when an image is edited or saved in a different format. Open both the original lossless copy and the resaved compressed copy in software that can perform ELA analysis. For the manual method, Adobe Photoshop is commonly used. Use the software to generate an ELA map by subtracting the compressed copy from the original copy. This process highlights any areas of the image that have been altered or manipulated. It is crucial to note that the manual method is the only acceptable method for court expertise usage. This is because it ensures that the expertise is credible, reliable, and admissible. However, ELA technique can only detect image tampering and may not always determine the type or extent of manipulation that has been done. Therefore, it is essential to interpret the results of the ELA analysis within the context of other available evidence. The photograph used as an example in this article was captured to demonstrate various photo manipulation techniques, including ELA. The image was taken by the author in the popular fishing area located in the small strait behind Cakljanac island, near the Danube River and the town of Slanci in Belgrade. Figure 3 shows the manual implementation of Error Level Analysis on the original photograph, while Figure 4 demonstrates the manual implementation of Error Level Analysis on the manipulated photograph. These figures illustrate how ELA can be used to identify areas of an image that have been altered or manipulated. In conclusion, the application of ELA through manual means is crucial to ensure that the results are accurate and reliable.

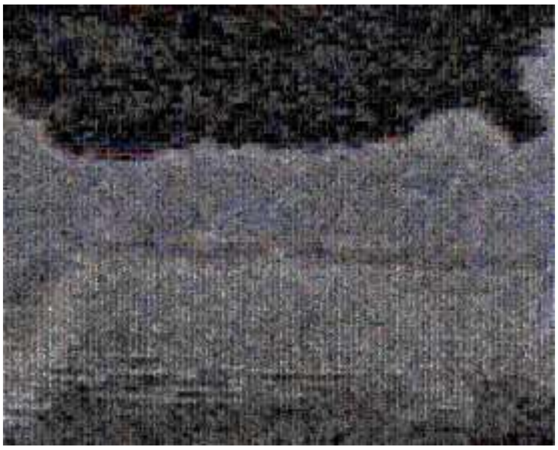

Figure 3 – ELA implementation (Original image)

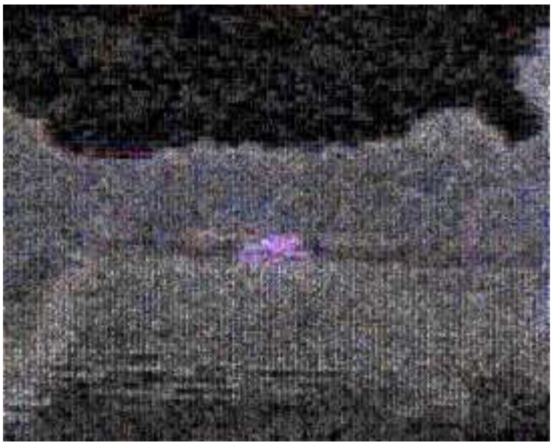

Figure 4 – ELA implementation (Altered version)

3. ALGORITHMIC APPROACH

ELA algorithms use the following steps to identify tampering: Divide the image into blocks. Compress each block with the JPEG algorithm. Calculate the difference between the original image and the re-saved image. Calculate the error level for each block. Set a threshold value to identify areas of high error level. Highlight the areas of the image that exceed the threshold value. ELA algorithmic approach to identifying image tampering is based on statistical analysis. The method is efficient in detecting image tampering by comparing the error levels between the original image and the re-saved image. The algorithm analyzes the level of compression applied to the image and highlights the areas that display inconsistent error levels. ELA algorithms can be applied to various types of images, including digital photographs, scanned images, and screen captures. This method has been used in several high-profile cases, including the Iranian missile test image, which was subjected to ELA analysis after it was revealed that the image was manipulated. The analysis showed clear signs of manipulation, leading to the Iranian government admitting to altering the image. Moreover, ELA algorithms have been applied in forensic investigations, including identifying tampering in evidence presented in court proceedings. ELA analysis is widely accepted as a reliable and objective method of image authentication in legal cases. Overall, ELA algorithmic approach offers a unique perspective in identifying tampered images, making it an indispensable tool in detecting image manipulation. As technology continues to advance, the need for reliable image authentication techniques will become increasingly important, and ELA algorithmic approach will remain a valuable tool in the field of image forensics.

4. COMBINING ELA AND METADATA ANALYSIS

ELA and metadata can be used together to provide evidence of photo manipulation. ELA can identify areas of the image that exhibit a different level of compression, which could indicate possible editing or manipulation. Metadata, on the other hand, contains information about the image, such as the date and time it was taken, the device that captured it, and the software used to edit it. By examining both ELA and metadata, forensic experts can gather evidence that supports their findings of photo manipulation. For example, if the metadata indicates that an image was captured on a certain date, but the ELA analysis shows that certain areas of the image were manipulated after that date, it suggests that the image may have been altered. Similarly, if the metadata shows that an image was captured with a particular device and edited with a certain software, but the ELA analysis suggests that the image was manipulated using a different method, it raises questions about the image's authenticity. By combining ELA and metadata analysis, forensic experts can build a stronger case for photo manipulation and provide more convincing evidence in court.

5. HISTOGRAM ANALYSIS

A histogram is a graphical representation of the distribution of pixel values in an image. It plots the frequency of each tone or shade of color present in the image. Histograms are particularly useful in detecting photo manipulation because they can reveal inconsistencies in the tonal range of an image. When a photo is manipulated, the tonal range of the image can be affected, causing the histogram to look different from that of an unaltered image. For example, if a portion of an image is cloned or copied from another part of the image, the histogram will show a spike in the tonal values that were copied. This can be seen as a sharp peak or a sudden change in the curve of the histogram. Another common manipulation is altering the exposure or brightness of an image. This can be done to make an image appear brighter or darker than it originally was. Such manipulation will also be reflected in the histogram. For instance, if an image has been overexposed, the histogram will show a peak at the far right end, indicating that there are too many bright pixels in the image. Similarly, if an image has been underexposed, the histogram will show a peak at the far left end, indicating that there are too many dark pixels in the image. Histograms can also reveal if an image has been cropped or resized. Cropping or resizing an image changes its tonal range and affects the overall distribution of pixel values. If an image has been cropped or resized, the histogram will show a change in the curve shape. One of the advantages of using histograms to detect photo manipulation is that they are not subjective. They provide objective evidence that can be used to support or refute claims of photo manipulation. However, interpreting histograms requires some knowledge and experience, and it is not always easy to tell whether an image has been manipulated just by looking at its histogram. In conclusion, histograms are a valuable tool in photo analysis and can be used to detect photo manipulation. They provide objective evidence that can be used to support or refute claims of photo manipulation. Understanding how to read and interpret histograms can help forensic analysts identify inconsistencies in the tonal range of an image and determine whether it has been manipulated or not. Figure 5 displays the Histogram analysis of the original image subjected to ELA analysis, while Figure 6 depicts the Histogram of the altered version. The charts in Figure 6 evidently depict changes, indicating manipulation. The use of Error Level Analysis (ELA) and histogram analysis together can provide a more robust analysis of image manipulation.

Histogram analysis is used to analyze the tonal distribution of an image, whereas ELA identifies areas of the image that have undergone compression or manipulation. By combining these two methods, the analyst can get a more complete picture of the image's authenticity. Histogram analysis is used to examine the pixel values of an image and create a graph that shows the distribution of tones. By examining the graph, the analyst can determine if there are any unusual patterns or if the image has undergone any modifications. For example, if the graph shows a high spike in the shadows, it could indicate that the image has been heavily manipulated. ELA analysis works by comparing the error levels between the original and re-saved image blocks. This method can highlight areas of the image that have undergone significant compression or manipulation. These areas may indicate the presence of an object that has been added or removed from the image. Combining histogram and ELA analysis allows for a more comprehensive analysis of the image. By examining the tonal distribution and identifying areas of compression or manipulation, the analyst can get a better understanding of the image's authenticity. For example, if the histogram shows no unusual patterns, but the ELA analysis highlights significant areas of manipulation, the analyst can conclude that the image has been manipulated, despite a lack of visual evidence in the tonal distribution. In conclusion, combining the use of histogram and ELA analysis can provide a more thorough analysis of image manipulation.

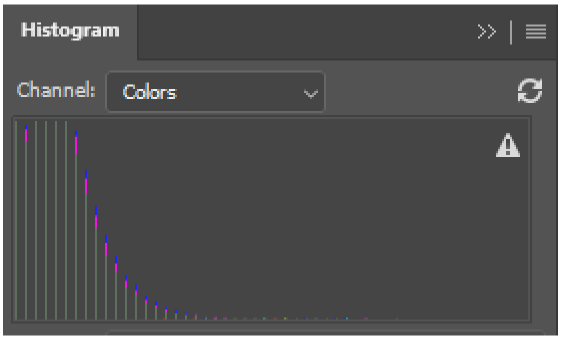

Figure 5 – Histogram (Original image)

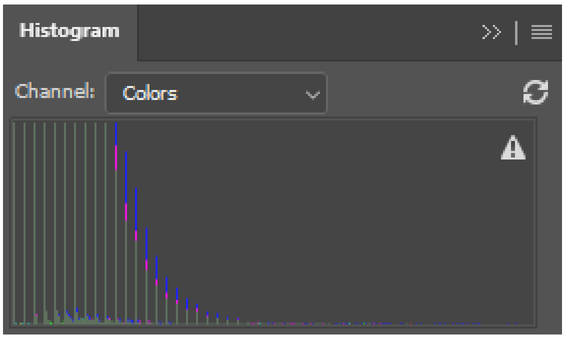

Figure 6 – Histogram (Altered version)

6. CLONE DETECTION METHOD

One method that forensic experts use to analyze image manipulation is the "Clone Detection" method. This method involves analyzing an image for signs of cloned regions or areas that have been copied and pasted from other parts of the image. When an image is manipulated, such as when someone adds or removes an object or person from the image, it often creates a "clone" of another part of the image. This clone can be detected using specialized software. The detecting clone method can be used in conjunction with other methods, such as Error Level Analysis (ELA) and histogram analysis, to provide a more complete picture of image manipulation. ELA and histogram analysis can detect changes in compression and brightness levels, respectively, while detecting clones can help identify areas of the image that have been altered. To use the detecting clone method, forensic experts first select a portion of the image to analyze. This can be done manually or using specialized software. Next, they search the selected portion for identical or nearly identical regions. If any are found, the expert can compare these regions to other areas of the image to determine if they are clones. If clones are found, it is a strong indication that the image has been manipulated. The detecting clone method has been used in a variety of high-profile cases, including the analysis of photographs related to the assassination of President John F. Kennedy and the identification of manipulated images in news reports. While this method is not foolproof, it has proven to be a valuable tool in forensic analysis and has helped to expose many instances of image manipulation. In conclusion, the detecting clone method is a powerful tool in analyzing image manipulation. By detecting cloned regions in an image, forensic experts can identify areas that have been altered and help to determine the authenticity of an image. As image manipulation continues to be a concern in various fields, including journalism, law enforcement, and politics, it is likely that the detecting clone method will become even more important in the future. The forthcoming images are presented to showcase the practice of cloning in digital photo manipulation and its detection through the clone detection method.

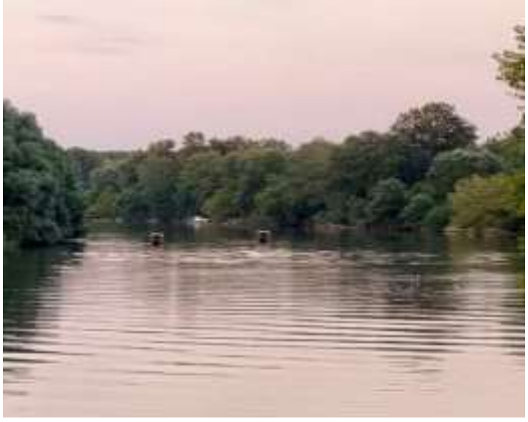

Figure 7 – Image with clone vessel added

Figure 7 exhibits an altered image that has undergone cloning, while Figure 8 showcases the same image analyzed with the clone detection method, allowing for the detection of the clone areas. It's important to note that the cloning method involves copying a selected portion of the image and duplicating it to replace or cover an unwanted section of the photo.

The Clone Detection Method operates by identifying similarities in the image, specifically looking for identical pixel patterns in different areas of the photograph. When these patterns are found, it suggests that the image has undergone manipulation, as such patterns are unlikely to occur naturally. The following examples of clone detection were carried out using the algorithm provided by the 29.ch website.

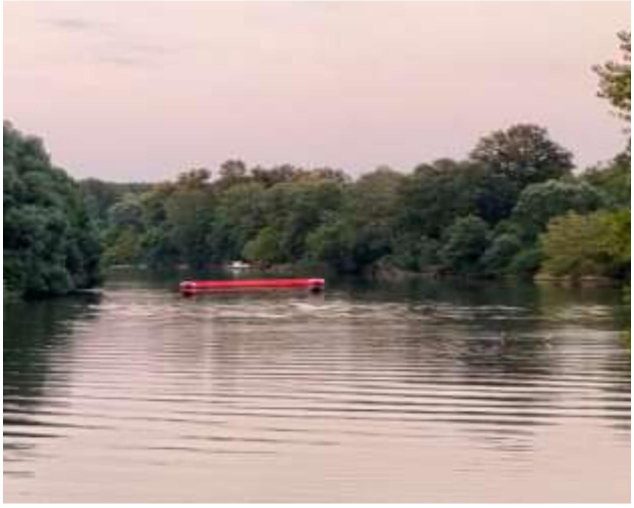

Figure 8 – Image analyzed with Clone Detection algorithm

7. HIGH-PROFILE CASES INVOLVING ELA ANALYSIS

- The „Burma soldier“ case: In 2007, a photograph was released by a news agency that appeared to show a Burmese soldier shooting at unarmed civilians during a protest. The photograph was later found to be manipulated using ELA analysis. The original photograph showed the soldier firing in the air, and the protesters had been added to the image.
- The „Obama handshake“ case: In 2012, a photograph was released that showed President Barack Obama shaking hands with Iranian President Hassan Rouhani. The image was claimed to be historic, as the two nations had not held official talks since 1979. However, ELA analysis showed that the image had been doctored. The hands of the two presidents had been merged from two separate images, and the background had been added later. The photographer was subsequently fired by the news agency that published the image.
- The „Jenna Talackova“ case: In 2012, a photograph was released of Jenna Talackova, a transgender woman, competing in the Miss Universe Canada pageant. The photograph was manipulated to remove Talackova's Adam's apple. ELA analysis showed that the image had been doctored, and the original image was subsequently released.
- The Johnny Depp and Amber Heard case: During their highly publicized legal battle, both Johnny Depp and Amber Heard presented manipulated images as evidence. The authenticity and manipulation of several images, including photographs of injuries and text messages, were analyzed by forensic experts from both sides using various techniques, including ELA. The experts presented conflicting opinions on the authenticity and manipulation of the images, and the judge considered their opinions as part of the evidence. Digital forensics involves the examination and analysis of digital media to recover evidence for use in a legal investigation. One critical area of digital forensics is the analysis of images, including those created with Photoshop. Adobe Photoshop is a powerful software program used to manipulate digital images.
- Osama Bin Laden case: The demise of Osama Bin Laden in 2011. sparked controversy when the US government released images of his body. Skeptical groups accused the government of tampering with the images. However, to alleviate the concerns, ELA analysis was employed to determine if the images were indeed doctored. The results of the analysis proved that the images were authentic and had not been manipulated in any way. This afirmated ELA as an example as it really stands for a reliable and objective method.

8. HISTORY OF ELA

ELA was first introduced by Dr. Neal Krawetz in 2006/7, a computer forensic analyst and the founder of the Hacker Factor blog. In 2007, he published a paper titled „Detecting Photo Manipulation Using Statistical Analysis of JPEG Compression“ in which he introduced the concept of ELA. He developed a software called „FotoForensics“ which used ELA to detect digital image manipulation. One of the most well-known cases in which ELA was used is the Zimmerman case. In 2012, George Zimmerman was charged with second-degree murder for the death of Trayvon Martin. During the trial, the defense team introduced an image of Zimmerman's head with a large wound. The prosecution team used ELA to analyze the image and found that it had been heavily manipulated, indicating that it was not an accurate representation of Zimmerman's injuries. This helped to cast doubt on the credibility of the defense team's evidence.

9. ACKNOWLEDGMENT

Substantial part of this study was a result of authors certain professional association with Security Information Agency (BIA) of the Republic of Serbia.

REFERENCES

[1] Battiat S. & Farinella, G. M. Image forensics based on statistical features in the DCT domain, 2003.

[2] Farid, H. (2006). Detecting digital forgeries using sensor pattern noise. *Proceedings of the IEEE International Conference on Computer Vision and Pattern Recognition*, 2006.

[3] Farid, H. Digital Image Forensics. *IEEE Signal Processing Magazine*, vol. 26, no. 2, pp. 16-25, 2009.

[4] Fridrich J, Soukal D, & Lukas J. Detection of copy-move forgery in digital images. *Proceedings of the Digital Forensic Research Workshop* (DFRWS), Cleveland, OH, USA, 55-60, 2003.

[5] Best practices for digital forensic evidence. National Institute of Justice. Retrieved from https://nij.-ojp.gov/topics/articles/best-practices-digital-forensic-evidence, 2016.

[6] Korus P. & Huang J. Detecting digital image forgeries using sensor pattern noise and a support vector machine. *Digital Investigation*, 12, 58-66, 2015.

[7] Krawetz, N. Detecting Photo Manipulation Using Statistical Analysis of JPEG Compression. Retrieved from https://www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf, 2007.

[8] Krawetz, N. Forensic image analysis: A low-level approach to identifying computer-generated graphics. Proceedings of the *12th international conference on computer forensics and investigations*, pp. 131-138, 2011.

[9] Lowe D. U.S. releases bin Laden images. CNN. Retrieved from https://www.cnn.com/2011/WORLD/-asiapcf/05/04/bin.laden.photos/index.html, 2011.

[10] Pevny T. & Bas P. Exposing digital forgeries by detecting inconsistencies in lighting. *IEEE Transactions on Information Forensics and Security*, 6(2), 461-470, 2011.

[11] Shi Y. Q. & Sun Q. A survey on image forgery detection. *Signal Processing: Image Communication*, 29(8), 918-935, 2014.

[12] Souto N, Nascimento J. & Botelho S, Digital image forensics using error level analysis and source camera identification. *Journal of Real-Time Image Processing*, 7(2), 97-107, 2012.

[13] High-profile cases where digital forensics played a role. Digital Forensics Corp. Retrieved from https://-www.digitalforensics.com/high-profile-cases-where-digital-forensics-played-a-role/, 2019.

[14] Chierchia G, Cozzolino D, Poggi G. & Verdoliva L. Deep learning for image forgery detection: A comprehensive review. *ACM Computing Surveys*, 54(5), 1-37, 2021.

[15] Fridrich J, Kodovsky J. & Holub V. Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, 7(3), 868-882, 2012.

[16] Goljan M. & Fridrich J. Steganalysis of JPEG images using rich models. *IEEE Transactions on Information Forensics and Security*, 9(3), 496-505, 2014.

[17] Kirchner M. & Fridrich J. (2018). Breaking the wall of JPEG steganography. *IEEE Transactions on Information Forensics and Security*, 13(8), 1989-2004, 2018.

[18] Korus P. & Huang J. Robust detection of image alternations using statistical moments of color channels *IEEE Transactions on Information Forensics and Security*, 8(9), 1512-1525, 2013.

[19] Korus P. & Huang J. Blind detection of image clones using color moment invariants. *IEEE Transactions on Information Forensics and Security*, 9(4), 554-567, 2014.

[20] Li B. & Lyu S. Nonintrusive component forensics of visual sensors using output images. *IEEE Transactions on Information Forensics and Security*, 5(4), 734-746, 2010.

[21] Li Y, Yang X. & Sun J. Copy-move forgery detection based on saliency map and feature points. *Signal Processing: Image Communication*, 64, 1-10, 2018.

[22] Qiao Y, Luo W. & Liu Z. A novel copy-move forgery detection method based on gradient field and extreme point information. *Signal Processing: Image Commmunication*, 87, 115991, 2020.

[23] Wang C, Zhang Y, Liu X. & Wu Z. Automatic face manipulation detection through feature-based histogram analysis. *Journal of Electronic Imaging*, 29(3), 033010, 2020.

[24] Wu X, Lu H, Niu Y. & Wu Y. Clone detection for digital video forensic analysis. *Journal of Electronic Imaging*, 28(5), 053019, 2019.

[25] Zhang C, Su X, Liu S. & Xie H. ELA-based tampered image detection method for online rumors, 2020.

REZIME

ANALIZA NIVOA GREŠKE (ANG)

ANG (Analiza Nivoa Greške) je tehnika analize digitalne slike koja je stekla popularnost poslednjih godina u oblasti savremene forenzike. ANG važi za moćnu metodu koja može pomoći ekspertima da utvrde da li je slika izmenjena odnosno izmanipulisana na bilo koji način. ANG radi tako što analizira nivoe kompresije slike i identifikuje oblasti koje su izmenjene ili izmanipulisane na različitom nivou od ostatka slike. Ove informacije mogu biti krucijalne u krivičnim istragama, gde autentičnost slike može biti ključna za rešavanje slučaja. U ovom radu istražujemo upotrebu ANG u modernoj forenzici, njene prednosti i ograničenja, kao i njen potencijalni uticaj na budućnost forenzičke istrage.

Ključne reči: *digitalna, forenzika, ELA, analiza, nivo, greške*