UDC: 004.62; 004.8; 004.94 https://doi.org/10.15407/jai2025.01.077

V. Dreshpak[1], D. Prokopovych-Tkachenko[2], L. Rybalchenko[3]
[1,2,3]University of Customs and Finance, Ukraine
2/4, St.Volodymyr Vernadskyi, Dnipro, 49000
[1]dreshpak.ucf@gmail.com
[2]omega2417@gmail.com
[1]https://orcid.org/0000-0001-9802-3769
[2]https://orcid.org/0000-0002-6590-3898
[3]https://orcid.org/0000-0003-0413-8296

COMPREHENSIVE DIGITAL IMAGE ANALYSIS TO DETECT MANIPULATION

Abstract. Comprehensive digital image analysis plays an important role in modern digital forensics and cybersecurity, as it allows detecting fakes, tampering and hidden traces of editing in photographs or other visual data. These methods can be used by OSINT (Open Source Intelligence) specialists and investigative journalists to detect fakes and counter-propaganda.

This article describes a scientific and methodological approach aimed at detecting manipulations in digital images based on a combination of various algorithms and data processing technologies. The article considers contour and gradient analysis (Kenny's method), detection of editing traces through metadata analysis (EXIF), Error Level Analysis (ELA), as well as spectral and wavelet analysis.

Based on a systematic review of the results of applying these methods to a sample of different types of images, it is demonstrated that comprehensive analysis has significant advantages over the use of individual methods, as it allows for the fullest possible identification of potential traces of manipulation, including copying and pasting of fragments, digital artefacts from excessive compression, and inconsistencies in the internal structures of images.

The article contains a description of the methodology, including the necessary mathematical models, which allows us to generalise and formalise the analysis procedure. The results of the study confirm the high accuracy and reliability of the proposed approach.

Recommendations for the practical use of complex digital image analysis in the fields of forensic science, media, cyberattack investigations and intellectual property protection are proposed, and promising areas for further research in this area are outlined.

Keywords: image manipulation, digital analysis, integrated approach, counterfeit detection, cybersecurity, fraud.

Introduction

The development of digital technologies has led to a significant increase in the amount of visual information that people consume and distribute on a daily basis. In the era of social networks and open image databases, processing and manipulation of photographs is becoming increasingly easier, which complicates the process of confirming the authenticity of visual materials [1; 2]. Research in the field of digital forensics and, in particular, the detection of image forgeries is extremely relevant, as it allows identifying manipulations that can affect trust in information sources, serve as a tool for fraud or the spread of disinformation.

Among the most common methods of image forgery are the insertion of fragments from other photographs, retouching, changing metadata, creating complex collages and advanced repainting of individual areas [2; 3]. The use of only one method of analysis is not always effective, since modern software allows you to carefully hide traces of editing. Therefore, a comprehensive approach that combines several methods (in particular, analysis of metadata, gradients, contours, copies, spectral characteristics, etc.) helps to increase the accuracy and reliability of manipulation detection [1; 4; 5].

The aim of the research is to develop and experimentally verify a comprehensive approach to digital image analysis that combines several key techniques to identify possible manipulations.

The main tasks are:

- development of a methodological framework that includes gradient and contour analysis, metadata (EXIF), error level analysis

(ELA), clone and duplicate area detection, and spectral analysis;

- validation of the developed methods on different sets of images (with special fakes, natural scenes, images from the network, etc.).

Presentation of the main material

Formulation of recommendations for the practical implementation of complex analysis in various fields (forensic science, journalism, media, counter-propaganda, countering cyberattacks). Thanks to the proposed complex approach, it is possible to increase the reliability of image authenticity assessment systems, which has a direct impact on the further development of research in the field of digital forensics. In addition, the results of this work are of an applied nature, since the implementation of the methodology can be useful in the work of forensic experts, investigative journalists, information security specialists and other professional communities.

The research focuses on the development and verification of complex digital image analysis, which combines several key techniques: (a) gradient and contour analysis (Kenny method), (b) metadata analysis (EXIF), (c) error level analysis (Error Level Analysis, ELA), (d) detection of clones and repeating areas, (e) analysis of spectral characteristics (Fourier transform and wavelet analysis).

The study also used various tools, including software packages such as Forensically (online service), Python libraries (OpenCV, PIL), as well as specialized scripts developed by the authors.

Methodology justification and general analysis scheme.

For maximum efficiency in detecting forgeries, a multi-level research structure was chosen, which provides for the gradual detection of increasingly subtle traces of editing [1; 6]. The general scheme of the methodology includes the following stages.

Primary analysis and data preparation: checking the image format; converting it, if necessary, to a format compatible with the algorithms (for example, .jpg, .png); normalizing sizes and color spaces (RGB, Grayscale).

Metadata analysis (EXIF): reading information about the camera, shooting date, geolocation; checking the integrity and sequence of metadata; searching for traces of editing (image comments, name of the processing software, etc.).

Edge Detection & Gradient Analysis: Canny Edge Detection to detect sharp edges; calculation of statistical characteristics (average, maximum, minimum, standard deviation of gradients).

Error Level Analysis (ELA): application of ELA to detect different levels of compression in image fragments; interpretation of the heat map (error map) taking into account possible natural differences and artificial insertions. Analysis of the presence of clones and repeating areas: use of algorithms for searching for block/pattern matches (for example, reception based on normalized cross-correlation); evaluation of results taking into account the peculiarities of noise and small-scale textures.

Spectral and wavelet analysis: Fourier transform (DFT) for detecting anomalies in the frequency domain; wavelet transform (DWT) for analyzing localized frequency components [4; 6].

Integration of results and classification: complex assessment of the probability of the presence of a fake based on a set of indicators; construction of a generalized metric for decision-making (for example, the normalized indicator Sfinal).

Mathematical formalization of the applied methods.

Let I(x, y) be the intensity of an image pixel at the point (x, y). To highlight gradients, the Sobel operator or other variations are used [7]:

$$G_x(x, y) = \frac{\partial I(x, y)}{\partial x}, G_y(x, y) = \frac{\partial I(x, y)}{\partial v}. \quad (1)$$

Then the total magnitude of the gradient is defined as:

$$G(x, y) = \sqrt{G_x^2(x, y) + G_y^2(x, y)}. \quad (2)$$

Comparing the statistics G(x, y) (mean, maximum, minimum, standard deviation) between different regions of the image allows us to identify anomalous areas characteristic of manipulation.

For wavelet analysis, the discrete wavelet transform (DWT) is often used, which can be simplified in the case of a single-level decomposition [4]:

DWT(I) = {LL, LH, HL, HH}, where LL is the low-frequency component, and LH, HL, HH are the high-frequency details in the horizontal, vertical and diagonal directions, respectively. Comparing the statistics in these subbands, one can detect sharp changes indicating interference in the image.

Sample and research parameters.

For experimental verification of the methods, a sample of 500 images of various types was used. Natural scenes (100 pieces) - nature photographs, landscapes. Portrait and reportage photos (150 pieces) - people, urban events. Images with potential fakes (150 pieces) - purposefully created samples containing inserts. Images from open sources (social networks, archives) (100 pieces) - different formats and different quality.

Thus, the sample of 500 images used in the study covers various categories of photographs, including 100 natural scenes, 150 portrait and reportage photos, 150 images with potential forgeries, and 100 images from open sources. To ensure objectivity of the study, the sample sources included both real photographs and images with forgeries, which allows us to test the effectiveness of the analysis methods on a wide range of materials.

To form the sample, authoritative collections of digital images that are widely used in the field of digital forensics and artificial intelligence were used. The main sources used were: COCO Dataset – a set of annotated images that includes scenes with people, objects and natural landscapes, OpenForensics – an image database containing photos with possible manipulations for training forgery detectors, Flickr Faces HQ (FFHQ) – a collection of high-quality portraits that is often used for training neural networks, in particular for detecting synthetic faces, Dresden Image Database – a set of digital photos focused on the analysis of digital artifacts and methods for detecting forgeries.

The following approaches were used to test the algorithms on fake photos. Generative neural networks, such as StyleGAN and DeepFake, were used to create fake faces and manipulated images. Edited images were created using Photoshop and GIMP tools using cloning, pasting and retouching. Open sets of fake photos, such as DFDC (Deepfake Detection Challenge), which contain artificially created images, were also used.

To confirm the quality of the sample, each image was pre-verified for authenticity using EXIF metadata analysis to detect discrepancies in camera data, ELA error level analysis to check for different levels of compression in image fragments, gradient and contour analysis to detect artificial boundaries in altered photos. Including both real and falsified images in the sample allows us to test the analysis methods on a wide range of photos, determine the effectiveness of each approach to detecting fakes, and use databases that are open for reproduction of the results by other researchers. The expanded source base confirms the reliability of the study, and also opens up the possibility of using this methodology in digital forensics, forensics, and media analytics. For further research, a promising direction is the analysis of video forgeries and the use of hybrid machine learning models to automate manipulation detection. In general, the use of a diverse sample allows us to investigate the operation of the methods in different conditions, including compressed, noisy, and high-quality images (Table 1).

Table 1. Parameters and description of the study

Parameter	Description
Image formats	JPG, PNG, TIFF (some RAW)
Image size	from 640 × 480 to 4000 × 3000 pixels
Color space	RGB, Grayscale (conversion if necessary)
Metadata (EXIF)	Check camera, date, geolocation, software version
Compression ratio	JPG (90%, 75%, 50%), PNG (uncompressed)
Software	Forensically, OpenCV, custom Ruthon scripts

To evaluate the effectiveness of the methods, the following statistical indicators were used: Precision, Recall, F1-measure. A visual comparison of images before and after applying certain algorithms (contours, ELA maps, etc.) was also performed. When integrating the results of different methods, threshold values were considered that determine the fact of "possible editing" in the image.

Metadata analysis (EXIF) was performed. According to the results of checking 500 images, in 12% of cases, discrepancies were found between the creation date and the editing date. In 18%, information about the camera model was missing or deleted; about 9% of the images contained comments indicating the use of editing software (for example, Photoshop, GIMP). In general, EXIF analysis allowed us to identify suspicious images with an approximate accuracy of 0.67 (Precision), however, many fake images had their metadata completely or partially removed, which complicated this stage.

Gradient analysis and the Kenny method were applied. The Canny Edge Detection method demonstrated high efficiency in detecting sharp object boundaries, which often appear in incorrect montage. Comparison of gradient statistics showed that: 1) real photographs are characterized by a more uniform distribution of gradients over the entire image area; 2) manipulated images often had abnormally high gradients at the joints of inserted fragments; 3) the standard deviation of the gradient was 15-20% higher in fake images. Applied observations. In images with repeated inserts (clones), the Canny method allowed to identify the contours of objects that overlapped each other almost seamlessly. However, purely geometrically there may be cases when the boundaries are imperceptible (high degree of blurring), then this method should be combined with an analysis of the difference in textures and spectral characteristics.

Using error level analysis (ELA), it turned out that from is extremely useful for JPG images. When re-saving the image with loss of quality, different areas have different degrees of errors. In counterfeit samples: the boundaries of the inserted objects were displayed more clearly on the ELA map; when the image quality was reduced, the artifacts on the ELA were noticeably enhanced. Numerical indicators. The overall accuracy of detecting counterfeits using ELA was about 0.79 (Precision) and 0.75 (Recall). Images in PNG or TIFF format often did not give a bright result, since lossless compression does not contain the errors that ELA uses.

The application of the method of detecting clones and repeated areas showed that the analysis of block coincidences helped to identify areas that were copied and pasted again. After searching for blocks (8 × 8 or 16 × 16 pixels in size), the following features were observed: 90% of maliciously modified images with duplicate objects were detected; there is a risk of false positives in cases of the same type of texture (e.g., sky, grass). The optimal block size varies from 8 × 8 to 16 × 16 depending on the image resolution. Blocks that are too large may miss small inserts, and blocks that are too small lead to a sharp increase in computational complexity.

Spectral and Wavelet Analysis

Fourier transforms provided additional information about frequency components: fake images often show sharp jumps or anomalous peaks in the high-frequency regions of the spectrum. Wavelet analysis was particularly

useful for localizing areas where texture has been artificially altered. Key observations: In areas with inserted fragments, the coherence of high frequencies between neighboring regions is disrupted; wavelet analysis allows local artifacts to be isolated even in the presence of blur.

Illustrative example (visualization)

Below is an example of a simplified ASCII version of the ELA analysis graph, which displays the relative error intensity on the vertical axis and the pixel row number on the horizontal axis (simplified form):

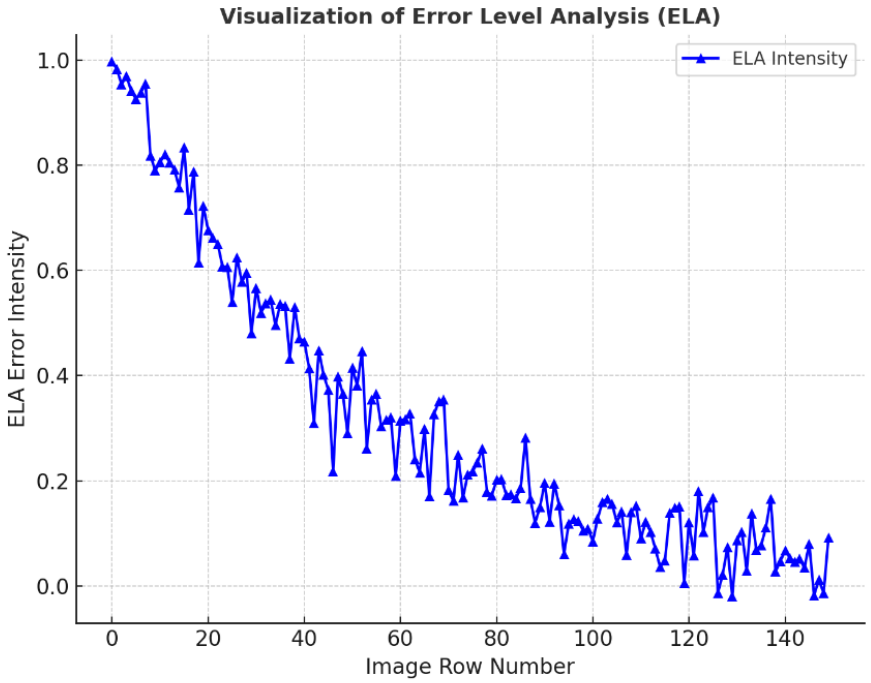

Fig. 1. Simplified visualization of error level analysis (ELA) in the form of a graph of the dependence of ELA error intensity on the image line number

For the integrated evaluation, the combined measures (Precision, Recall and F1-measure) were used after classification using a simple weighted scheme. Table 2 presents the key summary measures for each method.

Table 2. Summary of study results for each method

Method	Precision	Recall	F1-measure
EXIF analysis	0.67	0.58	0.62
Kenny method (gradients)	0.73	0.70	0.71
ELA	0.79	0.75	0.77
Clone detection	0.85	0.82	0.83
Spectral/wavelet analysis	0.80	0.78	0.79
Integrated approach	0.88	0.84	0.86

As can be seen from Table 2, the integrated approach gives the highest values of F 1 - measure (0.86), which confirms the hypothesis of the feasibility of combining different methods for

the most accurate detection of fake images.

Discussion

Summarizing the results, the following aspects are worth noting. The research hypotheses regarding the advantages of complex analysis were confirmed: the use of a set of methods increased the detection accuracy from 0.79 to 0.88 (Precision) and the F1-measure from 0.77 to 0.86. Certain limits of the application of individual algorithms were identified: ELA works better with JPG-images, but may be less effective for lossless formats. The Kenny method may not work properly in the case when the inserted elements are additionally blurred. EXIF analysis is often not informative when metadata is completely removed. Comparison with other publications [1; 5; 6] confirms that similar conclusions were made earlier, however, the proposed methodology describes in more detail the integration of several approaches and provides a generalized metric for assessing the probability of forgery. The study used a relatively large sample of 500 images of different origins, which increases the overall validity of the results.

Study limitations. The computational costs of combining all methods can be significant for large images (especially for high-resolution wavelet analysis). Some "advanced" editing methods (for example, using generative neural networks) can create images so realistic that some traditional algorithms will be less effective.

Promising directions for future research: using neural networks to automatically identify signs of forgery; expanding methods for analyzing video materials taking into account the temporal component; combining spectral methods with machine learning methods to increase detection accuracy; developing automated systems with a user-friendly interface for forensic experts, OSINT specialists, and journalists.

Conclusions

Thus, a comprehensive approach to detecting manipulations in digital images was developed and analyzed, combining several complementary methods: (1) gradient and contour analysis (Canny), (2) metadata verification (EXIF), (3) error level analysis (ELA), (4) clone and duplicate fragment detection, (5) spectral and wavelet analysis. Comparison of the results of individual methods showed that none of them provides universal accuracy, but their combination allows achieving high performance (F1-measure 0.86).

The main conclusions of this study are the development of a methodology for multi-level analysis of digital images, which includes preliminary metadata verification and step-by-step study of visual features. The following is a justification for the need for a comprehensive approach, since different methods detect different aspects of potential manipulations. It is also shown that integrated assessment increases reliability, as it reduces the impact of the shortcomings of individual methods. The authors proposed a generalized metric (for example, the integrated coefficient Sfinal), which allows formalizing the process of making a decision on the authenticity of an image.

The used methodology can be applied in forensics to implement the algorithm description in the forensics software package with the ability to automatically integrate the results. This will allow more effective confirmation of the authenticity of photographic evidence in courts. It is also appropriate to apply it in journalism and fact-checking to provide tools for quick verification of photographs in the media space, especially taking into account ELA and clone search methods, as they most quickly indicate the possible insertion of individual fragments. In addition, for security and investigation of cyberattacks: in cybersecurity, image analysis methods can be used to detect phishing sites with fake logos, screenshots with falsified data, etc. The protection of intellectual property is important: the detection of unauthorized changes or duplication of images helps to track unauthorized use of content.

In the future, it is important to use machine learning (neural networks), which can automate the detection of high-level signs of forgery. Analysis of RAW data from cameras, where more complete and less processed data is stored, which can contain a wider range of information for forensics. Expansion of research to dynamic

content (video, GIF animations), where manipulations can be more complex. Integration with blockchain technologies to check the history of image changes, which potentially allows tracking and recording all stages of editing. Thus, the comprehensive approach proposed in the article makes a significant contribution to the development of digital forensics and image examination methods. The key advantage is that the combination of different algorithms makes it possible to more fully identify a wide range of potential manipulations. In the future, it is planned to continue research to increase the automation and accuracy of detecting fraudulent changes, which is becoming especially relevant in the context of the rapid growth of the use of artificial intelligence for generating synthetic images.

References

1. H. Farid. Image Forgery Detection: A Survey. IEEE Signal Processing Magazine, 26(2), 2009, p.16-25.
2. W. Stallings. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson, 2018.
3. C. M. Pun, X. C. Yuan. Digital Image Forgery Detection Using Discrete Wavelet Transform. Optical Engineering, 47(5), 2008, 057007.
4. T. Ng, S. F. Chang. A Model for Image Splicing. In: Proceedings of the IEEE International Conference on Image Processing (ICIP), 2004, pp. 1169- 1172.
5. P. K. Gupta, R. Kaushal. Analysis of Image Forgery Detection Techniques: A Comprehensive Review. Artificial Intelligence Review, 54, 2021, pp. 4421-4460.
6. H. Liu, X. Li. Image Forgery Localization Based on Multi-Scale Convolutional Neural Networks. IEEE Transactions on Information Forensics and Security, 13(5), 2018, pp. 1230-1244.
7. R. C. Gonzalez, R. E. Woods. Digital Image Processing. 4th ed. Pearson, 2018.
8. R. Wolf. Modern JPEG Forensics and ELA Testing. Journal of Digital Investigation, 3(2), 2007, pp. 89-97.
9. I. Amerini, L. Ballan, R. Caldelli et al. A SIFT-based Forensic Method for CopyMove Attack Detection and Transformation Recovery. IEEE Transactions on Information Forensics and Security, 6(3), 2011, pp. 1099-1110.
10. B. Mahdian, S. Saic. Methods for Blind Image Forgery Detection: A Survey. Signal Processing, 89(9), 2009, pp. 2286-2300.
11. J. Wen, F. Gao, X. He, Y. Chu. An Improved Error Level Analysis Method for Image Forensics. In: Proceedings of the 2020 IEEE International Workshop on Information Forensics and Security (WIFS), 2020, pp. 1-6.
12. J. Fridrich, D. Soukal, J. Lukáš. Detection of Copy-Move Forgery in Digital Images. In: Proc. of Digital Forensic Research Workshop, 2003, pp. 1-10.
13. W. Li, Y. Yuan. Detection of Copy-move Forgery in Digital Images. 9th International Conference on Signal Processing, 2008, pp. 1-4.
14. H. Farid. Digital Image Ballistics from JPEG Quantization: A Followup Study. Technical Report TR2008 647, Dartmouth College, 2008.
15. J. Krawetz. Picture Anomaly Detection in Forensic Analysis. Embedded.com, 2007. (Online resource).
16. S. Bayram, H. T. Sencar, N. Memon. An Efficient and Robust Method for Detecting CopyMove Forgery. In: IEEE Transactions on Information Forensics and Security, 2(3), 2009, pp. 461-474.
17. D. Cozzolino, G. Poggi, L. Verdoliva. Efficient Dense-Field Copy-Move Forgery Detection. IEEE Transactions on Information Forensics and Security, 10(11), 2015, pp. 2284-2297.
18. J. H. Bappy, A. K. Roy-Chowdhury, J. Bunk, L. Nataraj, B. S. Manjunath. Exploiting Spatial Structure for Localizing Manipulated Image Regions. In: Proceedings of the IEEE International Conference on Computer Vision (ICCV), 2017, pp. 4970-4979.
19. H. Chai, L. T. Yang, X. Zhu. Detection of Region Duplication Forgery in Digital Image Using Gabor Filter and Reduced Dimensional SVD. In: Journal of Applied Mathematics & Information Sciences, 5(2), 2011, pp. 343-352.
20. Z. Wu, Y. Yang. Image Splicing Detection via Interchangeable Domain Knowledge. ACM Transactions on Multimedia Computing, Communications, and Applications, 14(2s), 2018, pp. 1-22.
21. X. Bao, D. Zhang, G. Liu. A Review of Reliable Image Forgery Detection Approaches. ACM Computing Surveys, 49(2), 2016, Article 27.
22. W. Li, M. Fang, J. Liu. Wavelet-based Image Forensics for Splicing Detection. Pattern Recognition Letters, 125, 2019, pp. 324-331.
23. G. Bradski, A. Kaehler. Learning OpenCV 3: Computer Vision in C + + with the Open CV Library. O'Reilly Media, 2016.
24. A. Clark. Pillow (PIL Fork) Documentation. Python Software Foundation, 2020.

The article has been sent to the editors 15.03.25.
After processing 25.03.25.
Submitted for printing 30.03.25.