JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

PixelTrace: A Forensic Investigation Tool

Yash Nagare[1] Devendra Mishra[2] Darshan Ghevade[3] Pranali Pawar[4] Dr. Nilakshi Jain[5]
Engineering Student[1] Engineering Student[2] Engineering Student[3] Co-Guide[4] Head of Department[5]
Department of Cyber Security[1,2,3,4,5]
Shah & Anchor Kutchhi Engineering College, Mumbai, India[1,2,3,4,5]

Abstract: Cyberspace has evolved significantly in the last few decades and has brought it rise in consumption of digital media. The widespread use of digital media has led to increased numbers of image tampering incidents. Image tampering refers to the process of manipulating images to mislead people. To combat this issue, few image tampering detection have been deployed, but none being able to detect sophisticated image tampering. In our research paper we propose an image tampering tool that uses ELA (Error Level Analysis) to determine image tampering. ELA is a technique that compares the original image to a compressed version of the same image to identify possible tampering. The proposed tool uses image trained library and machine learning to detect regions of tampering. This proposed tool can be used in various fields of forensics, journalism, and social media platforms to ensure the authenticity of digital images.

IndexTerms **- Error Level Analysis (ELA), Image tampering, Image manipulation, Forensics, Authenticity.**

I. INTRODUCTION

As technology progresses in both the realm of equipment and programs with each passing day, it brings certain benefits along with notable drawbacks. With progress in the development of computer bought its drawback of morphing data and exploiting it for personal gains. Image Tampering and Morphing is such a threat which can lead to spread of misinformation, illegal document forging, personal data, and security risk with many more. Considering this threat, a Tool which can detect morphing and tampering done to an image file is much needed in the field of Digital Forensics.

Various factors like machine learning, image trained datasets combined with ELA make up a strong Image Tampering Detection Tool which can provide more accurate details. This new approach to solving Digital Forensics Cases can produce fairer outcomes which can be crucial. While we cannot be perfectly accurate in tampering detection this Tool can be a much-needed help which was needed in the field of Digital Forensics.

II. LITERATURE SURVEY AND TECHNOLOGY STACK

A. Literature Survey

In the literature review for this project, we compared over 15 research papers on the topic of Photo morphing and Image Tampering. Most of the papers were based on a single approach to detection and their result on accuracy and time complexity. Some papers were based on Digital forensics and tools for the same. With this review we were able to expand our knowledge in the field of digital forensics and Cybercrimes.

These are the points that we have identified, through our review of various papers, which distinguish our project from pre-existing ones:

- Our project is not only a Research Paper or a terminal-based tool but an Open-Source Project which anyone can access.
- The image feed is checked for authenticity.

[1] Focuses on the field of digital forensics. In this paper, many images forensic techniques and tools, as well as their applications in real-world cases are mentioned. It also mentions the importance of ensuring the authenticity and integrity of digital images in various fields, including law enforcement, journalism, and medical research.

[2] Discusses the challenges associated with the forensics of images in the context of smart devices and media. The article proposes a forensic analysis framework for images shared on social networks and captured using smart devices. It also discusses the use of various imaging techniques, such as watermarking and steganography, for forensic purposes.

[3] A summary of digital forensics tools used in criminal investigations to detect forgery/fraud and other cases involving picture morphing is given. It also covers several forensic instruments and their capabilities. It also emphasizes the necessity of digital forensics in criminal investigations, as well as the necessity for advanced digital forensic technologies.

[4] Discusses various image authentication methods for verifying the legitimacy and integrity of digital images. They examine several picture authentication approaches, such as digital signatures, hash functions, and watermarking, and present a critical analysis of their strengths and weaknesses. They also highlight the significance of picture authentication in a wide range of fields such as law enforcement and medical research.

[5] In this paper, Error Level Analysis efficiency is evaluated. It is a technique which detects difference in compression level to identify possible morphs and tampers.

[6] This paper proposes a new and unique way to identify unique signature in JPEG files for detection of Morphing using ELA. With aim to improve the effectiveness of ELA in determining digital image manipulation.
[7] In this paper, how ELA can be integrated with Deep Learning is introduced. With this new fusion the accuracy of Tampering Detection has been increased.
[8] This paper proposes a new technique how ELA and Laplacian-edge detection plugin on GIMP software can effectively detect image splicing in images with high accuracy.
[9] Proposed a novel technique in which ELA is combined with CNN (Convolutional Neural Network) and is trained and evaluated on datasets and is compared with other methods of image forgery detection. The proposed method is effective against copy move forgery, splicing.
[10] The paper proposes deployment of a tool that can detect common image manipulation such as splicing, cloning, and retouching. The tool is designed to process images shared over social media, it also includes potential future implementations and improvements to enhance the tool's accuracy and usability.
[11] This research provides a unique approach for identifying face-swap photos using deep learning and error level analysis (ELA). They provide a new feature extraction approach that combines ELA with a deep neural network to detect picture manipulation. The results of the experiment suggest that the proposed method is successful in detecting face-swap photos and beats current approaches.
[12] An overview of image authentication techniques based on watermarking is presented in this paper. The paper also discusses visible watermarking and invisible watermarking, as well as the applications they can be applied to digital images. The paper also highlights the challenges and future directions in this field.
[13] Several types of image authentication schemes are discussed in this research paper, including watermarking, digital signatures, and hashing. Comparison of advantages and disadvantages of the techniques are and future direction for image authentication are mentioned in the paper.
[14] This research provides a review of multiple methods used in digital picture watermarking for image authentication and visual cryptography. They examine many techniques to picture authentication and security, including fragile watermarking, semi-fragile watermarking, and robust watermarking. The study also discusses the field's difficulties and potential directions.
[15] This work provides a strong and adaptable photo authentication technique that is both effective and safe. They propose a novel notion of "modulation code," which mixes secret sharing with modulation to ensure durability and security against many forms of attacks. The research also includes experimental data that show the efficacy of the suggested strategy.

B. Technology Stack

- Python
- Python Imaging Library
- Pillow
- NumPy
- Matplotlib
- OS (Operating System Module)

III. METHODOLOGY AND IMPLMENTATION

This study presents a technique for detecting image manipulation through Error Level Analysis (ELA), a process of identifying differences in compression levels between parts of an image. The technique is based on the assumption that areas of an image that have been manipulated will have different compression levels than areas that have not.

To implement ELA, the study used a Python script that makes use of the Pillow library. Pillow is a library for handling and manipulating images in Python. The script utilized the ImageChops module of Pillow to calculate the difference between an original image and a copy of the image that has been saved with a lower quality setting.

Once the script calculated the difference between the two images, it marked the pixels that had a difference above a specified threshold with a color that indicates the intensity of the difference. The script also created a heatmap of the difference values to provide a visual representation of the differences between the two images.

In addition to detecting image tampering, the study also implemented a feature that checks for the authenticity of the image. To do this, the script marks any pixels with a difference above a certain threshold with a red color in a new image. It then scans this new image object to confirm the authenticity of the image. If any differences were found, it concludes that the image is not authentic, otherwise, it concludes that the image is authentic.

The time and space complexity of the ELA script are also important factors to consider. The time complexity of the script is

O(W * H), where W is the width and H is the height of the image. This is because the script needs to calculate the difference between each pixel in the original image and the compressed copy of the image. The space complexity of the script is O(n^2), where n is the size of the image. This is because the script needs to store the difference values for each pixel in a new image object, which can be as large as the original image. Understanding the time and space complexity of the script is important for optimizing its performance and for ensuring that it can handle large images efficiently.

The study then conducted several experiments to evaluate the effectiveness of ELA for detecting image tampering. The experiments used a variety of test images that were either unmodified or manipulated. The manipulated images had added or removed objects, altered colors or brightness, or resized images.

In addition to evaluating the performance of the ELA script, the study also investigated the impact of different parameters on its performance. Specifically, the study tested different values for the difference threshold, the scaling factor for marking pixels, and the color of the marking. The performance of the script with these different parameter settings was evaluated, and the results were compared to identify the optimal settings for each parameter.

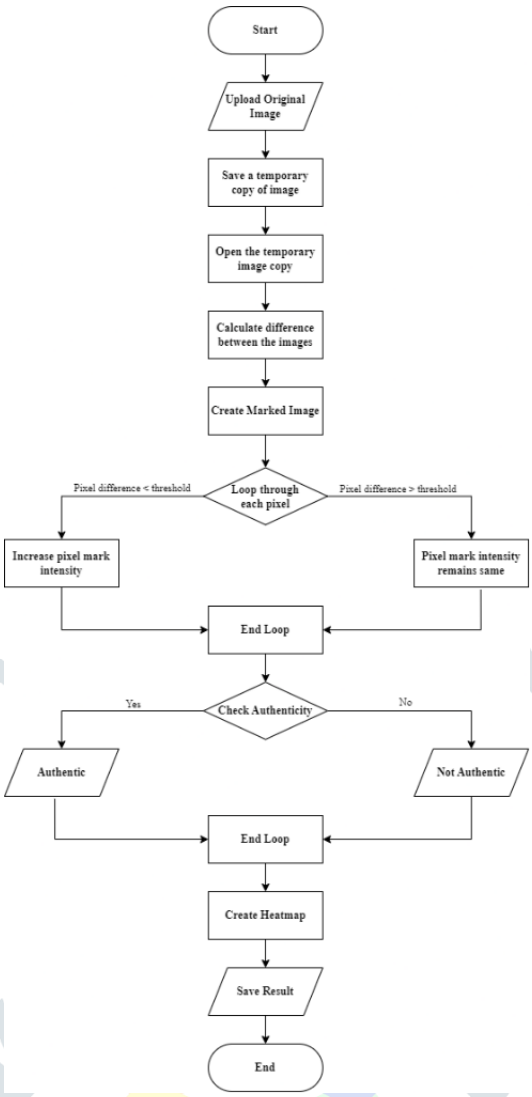

Fig. 1. Block Diagram of ELA

Fig. 1 represents the block diagram of working of PixelTrace. The goal of the study is to provide a comprehensive evaluation of the effectiveness of Error Level Analysis for detecting image tampering and to identify the optimal parameter settings for the technique. By providing a detailed analysis of the performance of the ELA script, the study hopes to contribute to the development of effective and reliable methods for detecting image tampering.

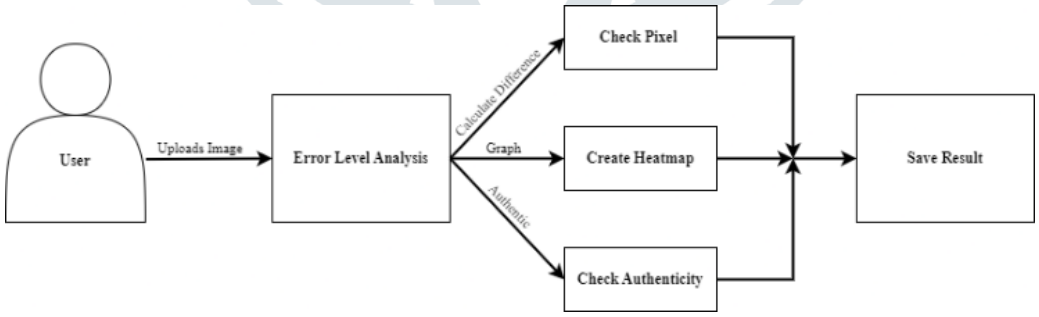

Fig. 2. Use Case diagram of ELA

Fig. 2 represents the user interaction with PixelTrace.

IV. RESULT

Fig. 3. Working of PixelTrace

Fig. 3 represents Command Line interface of PixelTrace.

Fig. 4. Original Tampered Image

Fig. 4 represents an AI generated image which was tampered for testing purpose. As seen in the figure the sign board has been placed with the help of photo manipulation tool.

Fig. 5. Temporary Compressed Image

Fig. 5 original image was resaved as temporary image with reduction in quality for further processing.

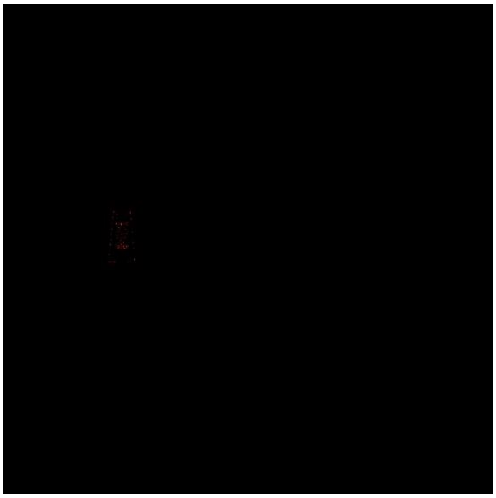

Fig. 6. Output Image

Fig. 6 represents the output of ELA with the manipulated region highlighted with red mark.

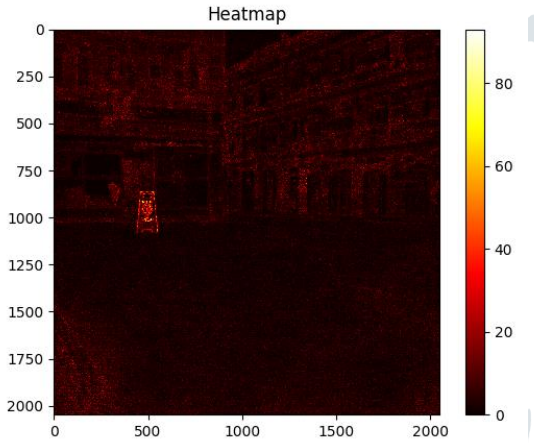

Fig. 7. Heatmap Graph

Fig. 7 represents the Heatmap graph plotted with the help of Matplotlib library using python. The tampered area is depicted with a high intensity that is different from the image's overall intensity.

V. CONCLUSION

In conclusion, this study introduced Error Level Analysis (ELA) as an effective technique for detecting image manipulation and verifying image authenticity. By implementing ELA using a Python script and the Pillow library, the study achieved an efficient comparison of compression levels between an original image and a compressed copy. The script accurately marked areas with significant compression differences, providing a visual representation of potential tampering.

Through extensive experiments involving various types of image manipulation, such as object alterations, color changes, and resizing, the study demonstrated the robustness of ELA in detecting image tampering. Additionally, the study examined the impact of different parameters on the performance of the ELA script, aiming to identify optimal settings. This analysis contributes to the refinement of ELA, enhancing its accuracy and efficiency in detecting image tampering.

The novelty of this study lies in its comprehensive evaluation of ELA, which encompasses diverse manipulation scenarios and parameter settings. By leveraging error level analysis, the study offers a practical solution for image forensics, making significant contributions to the development of reliable methods for detecting image tampering.

Overall, the findings establish error level analysis as a promising technique for image tampering detection and image authenticity verification. The insights gained from this study provide valuable guidance for optimizing ELA's performance, enabling its effective application in the field of image forensics.

REFERENCES

[1] R. S. Khalaf and A. Varol, "Digital Forensics: Focusing on Image Forensics," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-5, doi 10.1109/ICCSEA49143.2020.9132965.

[2] S. Li, Q. Sun and X. Xu, "Forensic Analysis of Digital Images over Smart Devices and Online Social Networks," 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2018, pp. 1015-1021, doi: 10.1109/HPCC/SmartCity/DSS.2018.00168.

[3] G. U. Reddy, M. Madhu Bala and B. Padmaja, "An Overview on Digital Forensics Tools used in Crime Investigation for Forgery Detection," 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), 2020, pp. 1-5, doi: 10.1109/ICCSEA49143.2020.9132965.

[4] Marakumbi Prakash R, Jayashree V. Khanapuri "A Study on Image Authentication Methods" International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 12 | Dec 2018 www.irjet.net

[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), 2015, pp. 23-28, doi: 10.1109/ICSEngT.2015.7412439.

[6] Azhan, Amira & Adeyemi, Ikuesan & Razak, Shukor & Kebande, Victor. (2022). Error Level Analysis Technique for Identifying JPEG Block Unique Signature for Digital Forensic Analysis. Electronics. 11. 1468. 10.3390/electronics11091468.

[7] 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). 17. 653. 10.12928/telkomnika. v17i2.8976.

[8] Budiman, M. A., Suksmono, A. B., & Wibowo, A. (2019). Photo splicing detection using error level analysis and Laplacian-edge detection plugin on GIMP. Journal of Physics: Conference Series, 1193(1), 012014. doi:10.1088/1742-6596/1193/1/012014

[9] Sari, W. P., & Fahmi, H. (2021). The Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 6(3). https://doi.org/10.22219/kinetik.v6i3.1272

[10] Kumar, S., Singh, R., Singh, S., & Singh, G. (2019). Development of the Error Level Analysis forensic tool for images shared over messaging and social networking applications. In Proceedings of the 4th International Conference on Computing Sciences (ICCS 2019) (pp. 254-259). doi:10.1145/3344542.3344565

[11] N. Wang, L. Zhang, X. Wu, and Y. Yang, "A Novel Counterfeit Feature Extraction Technique for Exposing Face-Swap Images Based on Deep Learning and Error Level Analysis," in IEEE Access, vol. 8, pp. 163233-163245, 2020, doi: 10.1109/ACCESS.2020.3028602.

[12] Hasan, Basna & Ameen, Siddeeq & Hassan, Omer. (2021). Image Authentication Based on Watermarking Approach: Review. Asian Journal of Computer Science and Information Technology. 9. 34-51. 10.9734/AJRCOS/2021/v9i330224.

[13] Shinde, Anushri and Salunkhe, Prital and Mane, Prajakta and Nichal, Arjun, A Review Paper on Image Authentication Scheme (February 6, 2019). International Journal of Advanced Research in Engineering and Technology, 10(1), 2019, pp 11-19., Available at SSRN: https://ssrn.com/abstract=3532951

[14] C. Vyas and M. Lunagaria, "A review on methods for image authentication and visual cryptography in digital image watermarking," 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, India, 2014, pp. 1-6, doi: 10.1109/ICCIC.2014.7238504.

[15] Chen, H., Huang, X., Wu, W. et al. Efficient and secure image authentication with robustness and versatility. Sci. China Inf. Sci. 63, 222301 (2020). https://doi.org/10.1007/s11432-020-3007-5