WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Image Forgery Detection Using Python and Machine Learning

[1]Paventhan A, [2]Santhosh Saai S, [3]Sasidharan J, [4] Dr. S. Mohandoss, [5] E. Durga Nandini, [6]Dr. S. Latha Subramanian

Cyber Forensics and Information Security, Dr. M.G.R. Educational and Research Institute, Chennai, India.

ABSTRACT-

This project addresses the critical issue of image forgery detection, employing advanced image processing, deep learning, and data augmentation techniques. With implications spanning journalism, law enforcement, art, and cybersecurity, the system ensures image authenticity, countering misinformation and enhancing security. In the era of deepfakes, the project tackles sophisticated manipulations. Beyond technical implementation, it emphasizes societal and ethical considerations, advocating for responsible image use, data integrity, and trust in online interactions. Collaborative efforts are urged to fortify the digital ecosystem against the challenges of image manipulation, securing visual content's authenticity in diverse industries.

INTRODUCTION:

This project delves into the critical realm of image forgery detection, utilizing advanced image processing and deep learning. With far-reaching implications in journalism, law enforcement, and digital communication, the system ensures the integrity of visual content, combating misinformation and bolstering cybersecurity. In an age dominated by deepfake technology, the project addresses sophisticated manipulations. Beyond technical implementation, it underscores societal and ethical considerations, advocating for responsible image use and trust in online interactions. Collaborative efforts are essential to fortify the digital landscape against image manipulation challenges, securing authenticity in various industries.

OBJECTIVE:

1. Error Level Analysis Implementation: Develop an image forgery detection system centered around Error Level Analysis (ELA), leveraging this technique to identify inconsistencies in compression levels and unveil potential image manipulations.

2. ELA-based Hashing: Implement ELA-based hashing mechanisms to generate hash values for images, facilitating efficient comparison and detection of alterations introduced through various manipulation methods.

3. Exploration of Forgery Challenges: Thoroughly explore challenges posed by deceptive image practices, emphasizing the need for ELA in uncovering subtle changes that might be overlooked by traditional analysis methods.

4. Applications in Digital Forensics: Showcase the project's applicability in the field of digital forensics, emphasizing how ELA can play a pivotal role in authenticating visual content and ensuring the integrity of digital evidence.

DESIGN AND IMPLEMENTATION:

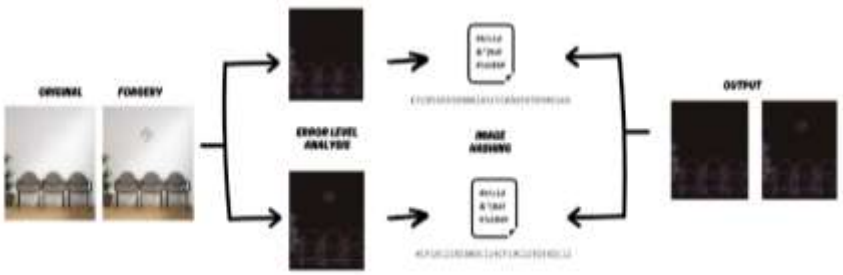

Fig 1.1 Design of Image forgery Detection

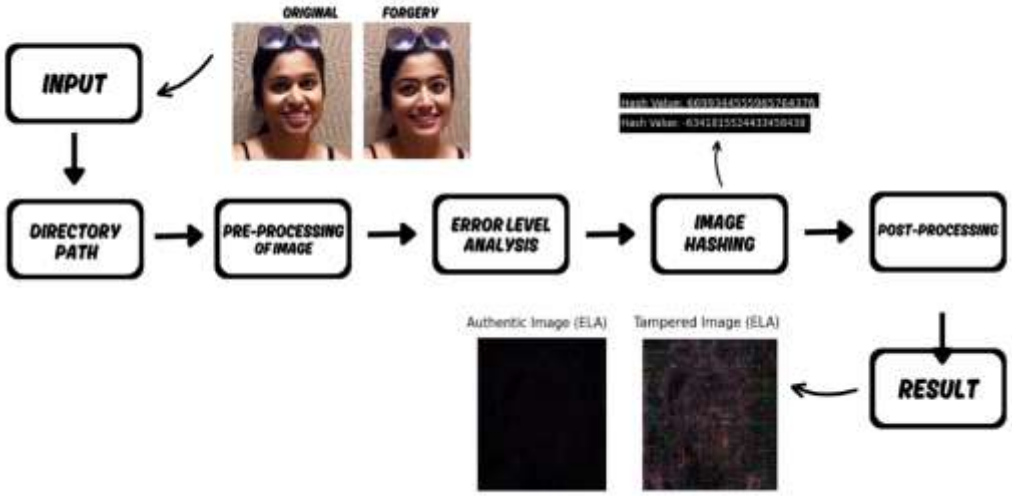

Fig 1.2 Working of Image Forgery Detection

METHODOLOGY:

1. Data Collection:

- Gathered diverse datasets comprising authentic and manipulated images to ensure comprehensive coverage of potential forgery scenarios.

2. ELA-based Image Preprocessing:

- Applied Error Level Analysis (ELA) to generate unique hash values for each image, creating distinctive fingerprints that highlight manipulated regions.

3. Machine Learning Model Selection:

- Employed transfer learning with deep neural networks such as Xception, leveraging pre-trained models to enhance the detection capability.

4. Data Augmentation:

- Implemented data augmentation techniques to diversify the training dataset, enhancing the model's ability to generalize and detect subtle manipulations.

5. Model Training and Evaluation:

- Trained the selected model on the augmented dataset, optimizing for accuracy and precision.

- Evaluated the model using validation datasets, ensuring robust performance across various manipulation types and qualities.

6. Deployment and Integration:

- Integrated the trained model into real-time applications or systems for seamless image forgery detection.

7. Ethical Considerations:

- Addressed ethical implications, emphasizing responsible usage of image forgery detection technology to uphold privacy and prevent misuse.

Conclusion:

In conclusion, the project "Image Forgery Detection using Python and Machine Learning" effectively discerns between authentic and manipulated images using advanced image processing and machine learning. Emphasizing the vital role of image forensics, the project navigated challenges posed by deceptive practices, showcasing its efficacy in detecting subtle alterations. A thorough feasibility analysis and robust testing affirm the solution's viability in digital forensics. Amidst evolving digital landscapes, the project contributes valuable insights, exemplifying the fusion of image processing and machine learning to address emerging challenges and inspire further exploration in digital forensics.

REFERENCES:

1. Farid, H. (2009). Digital Image Forensics. IEEE Signal Processing Magazine, 26(2), 26-37.

2. Fridrich, J., Kodovsky, J., & Holub, V. (2013). Rich Models for Steganalysis of Digital Images. IEEE Transactions on Information Forensics and Security, 7(3), 868-882.

3. Barni, M., Bartolini, F., & Cappellini, V. (2014). Image forgery localization via fine-grained analysis of CFA artifacts. IEEE Transactions on Information Forensics and Security, 9(4), 586-598.

4. https://link.springer.com/article/10.1007/s11042-022-13797-w

5. Lyu, S., & Farid, H. (2006). Detecting hidden messages using higher-order statistics and support vector machines. In Information Hiding (pp. 340-354). Springer.

6. Bayram, S., & Sencar, H. T. (2006). Steganalysis of content-adaptive and distortion-tolerant JPEG 2000 images. In Proceedings of SPIE - The International Society for Optical Engineering (Vol. 6072, p. 60720E). SPIE.

7. Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries by detecting duplicated image regions. In Proceedings of the IEEE Workshop on Multimedia Signal Processing (pp. 185-188). IEEE.

8. Goljan, M., Fridrich, J., & Holub, V. (2009). Merging Markov and DCT features for multi-class JPEG steganalysis. IEEE Transactions on Information Forensics and Security, 4(4), 726-738.

9. www.javapoint.com

10. Bondi, L., & Tondi, B. (2013). A comprehensive overview on passive image forgery detection. Multimedia Tools and Applications, 64(2), 417-438.