INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 930-934

FAKE IMAGE DETECTION USING MACHINE LEARNING

Mrs. Harshita D. Jain[1], Ms. Sakshi Meshram[2], Mr. Preet Sathe[3], Ms. Yamini Hatwar[4], Ms. Divya Bhilawe[5], Mr. Piyush Zade[6]

[1]Assistant Professor of Information Technology Kavikulguru Institute of Technology and Science, Nagpur, India

[2,3,4,5,6]Department of Information Technology Kavikulguru Institute of Technology and Science, Nagpur, India.

ABSTRACT

In this technological era a huge number of people have become victims of image forgery. A lot of people use technology to manipulate images and use it as evidences to mislead the court. So to put an end to this, all the images that are shared through social media should be categorized as real or fake accurately. Social media is a great platform to socialize , share and spread knowledge but if caution is not exercised, it can mislead people and even cause havoc due to unintentional false propaganda. Especially in the political arena, manipulated images can make or break a politician's credibility. Current forensic techniques require an expert to analyze the credibility of an image. We implemented a system that can determine whether an image is fake or not with the help of machine learning and thereby making it available for the common public.

Keyword: Image forgery, photoshoped Deep learning. Social media. pixelization

1. INTRODUCTION

Since the inception of photography, there has been a persistent pursuit by individuals and organizations to manipulate images, aiming to deceive viewers. Initially, this task demanded considerable expertise and hours of work from professional technicians.

However, with the advent of digital photography, the ease of image modification has become accessible to virtually anyone, yielding results that mimic professionalism effortlessly. Consequently, this widespread accessibility has given rise to social issues, ranging from the reliability of images presented by the media to the alteration of photographs of models to enhance their appearance or body image.

The extensive array of methods available for image manipulation has led to a growing interest in image forgery detection, both in academic research and the professional domain. While numerous detection methods exist, determining the most efficient and practical ones to implement and execute proves challenging. An algorithm with a high detection rate may concurrently exhibit a substantial rate of false positives. Additionally, while runtime significantly influences an algorithm's efficiency and usability, it is often discussed academically rather than in practical, real-world terms.

Benefits of a image forgery detection:

Image forgery detection, also known as image forensics, is a crucial field with several benefits:

1. Authenticity Verification: Image forgery detection helps in verifying the authenticity of images, ensuring that the images have not been manipulated or tampered with. This is particularly important in legal and forensic investigations, journalism, and digital evidence authentication.
2. Maintaining Trust: In the age of digital media and social networking, maintaining trust in the authenticity of images is paramount. Detecting image forgeries helps in preserving trust among users, especially in platforms where images play a significant role, such as news websites and social media.
3. Preventing Misinformation: With the proliferation of digital manipulation tools, images can be easily altered to spread misinformation or propaganda. By detecting image forgeries, the spread of false information can be mitigated, contributing to a more informed society.
4. Protecting Intellectual Property: Image forgery detection helps in protecting the intellectual property rights of photographers, artists, and content creators. By identifying instances of unauthorized alterations or use of their work, creators can take appropriate legal action to safeguard their rights.

Challenges of a image forgery detection:

Detecting image forgeries comes with several challenges due to the increasing sophistication of digital manipulation techniques. Some of the key challenges include:

1. Advanced Manipulation Techniques: As digital editing tools become more sophisticated, perpetrators can employ advanced techniques to manipulate images subtly, making it difficult for traditional forgery detection

methods to detect alterations.

2. Variety of Manipulations: Images can be forged in various ways, including copy- move forgery, splicing, retouching, and manipulation of metadata. Detecting these different types of forgeries requires a diverse set of techniques and algorithms, each tailored to specificmanipulation methods.
3. Scale and Complexity: With the vast amount of digital images uploaded online every day, detecting forgeries at scale poses a significant challenge. Additionally, the complexity of images, such as high-resolution images or those with intricate details, can further complicate the detection process.

Opportunities for Society Communities:

1. Advancing Justice and Legal Proceedings: In legal proceedings, the authenticity of photographic evidence is crucial for delivering justice. Image forgery detection techniques can assist forensic investigators and legal professionals in verifying the authenticity of images presented as evidence, thereby ensuring fair trials and accurate verdicts.
2. Empowering Digital Creatives: Image forgery detection tools can empower digital creatives, such as photographers, artists, and designers, by providing mechanisms to protect their intellectual property rights. By detecting unauthorized alterations or use of their work, creatives can take appropriate actions tosafeguard their creations and livelihoods.
3. Enhancing Cybersecurity Awareness: Increased awareness of image forgery techniques can also contribute to enhancing cybersecurity awareness among the general public. By understanding how images can be manipulated, individuals can become more vigilant and critical consumers of visualcontent, thereby reducing the likelihood of falling victim to online scams or phishing attempts.

2. REQUIRNMENTS SPECIFICATION

2.1 Functional Requirements

Functional requirements for digital image forgerydetection using machine learning might include:

1. Input Image Compatibility: The system should be able to process various image formats (e.g., JPEG, PNG) and sizes.
2. Preprocessing: Preprocessing steps such as resizing, noise reduction, and color normalization may be necessary to enhance the input images.
3. Feature Extraction: Extract relevant features from images such as texture, color distribution, and geometric patterns to create a feature vector.
4. Training Data: Acquire a diverse dataset of authentic and forged images for training themachine learning model.
5. Model Training: Develop and train machine learning models (e.g., convolutional neural networks) using the extracted features and labelled training data.
6. Validation: Validate the trained model's performance using separate validation datasets to ensure generalization.
7. Testing: Test the model on unseen data toevaluate its accuracy, precision, recall, and F1score.
8. Real-time Detection: Implement real-time detection capabilities for identifying forged images quickly.
9. User Interface: Develop a user-friendly interface for uploading images, displaying results, and interacting with the system.
10. Integration: Ensure compatibility and integration with existing image processing software or platforms.
11. Accuracy and Robustness: Ensure the modelis accurate and robust against various types of forgery techniques such as copy-move, splicing, and retouching.
12. Scalability: Design the system to handle a large volume of image data efficiently.
13. Customization: Allow users to customizedetection parameters or choose specific forgery detection techniques based on theirrequirements.
14. Reporting: Provide detailed reports on detected forgeries including the type of manipulation, confidence scores, and regions of interest.
15. Security: Implement security measures to protect the integrity of the detection process and prevent unauthorized access to sensitive data.
16. Maintenance and Updates: Establish procedures for maintaining and updating the system to adapt to emerging forgery techniques and improve performance over time.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 930-934

3. RESEARCH METHODOLOGY

Detecting image forgery is a complex task that often requires a multidisciplinary approach involving image processing, computer vision, and machine learning techniques. Here's a basic research methodology for image forgery detection:

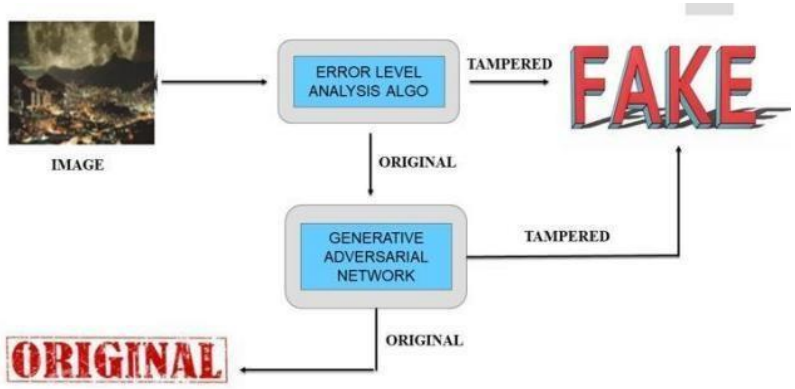

Fig 1. Images of image forgery detection

Problem Definition:

- Clearly define the scope of image forgery detection. Determine the types of forgery to be detected, such as copy-move, splicing, or retouching.
- Specify the characteristics of authentic andforged images to identify potential features fordetection.

4. LITERATURE REVIEW

- Review existing literature on image forgery detection techniques. Understand the state-of- the-art methods, their strengths, and limitations.
- Identify commonly used features, algorithms, and datasets in the field.
- Dataset Acquisition and Preparation:
- Gather a diverse dataset containing both authentic and forged images. Ensure the dataset covers various types of forgeries and includes ground truth annotations.
- Preprocess the dataset by standardizing image sizes, formats, and resolutions.
- Feature Extraction:
- Extract relevant features from images that can distinguish between authentic and forged regions.
- Common features include statistical moments, texture descriptors, gradient information, and frequency domain representations.
- Algorithm Selection:
- Choose appropriate algorithms or models for detecting image forgeries based on the extracted features.
- Consider techniques such as machine learning classifiers (e.g., Support Vector Machines, Random Forests, Convolutional Neural Networks), digital forensic algorithms, or a combination of both.
- Training Phase:
- If using machine learning approaches, divide the dataset into training, validation, and testing sets.
- Train the chosen model(s) using the training data and optimize hyperparameters using the validation set.
- Evaluate the model(s) using appropriate metrics such as accuracy, precision, recall, and F1-score.

Testing and Evaluation:

- Evaluate the trained model(s) using the testing dataset to assess its generalization performance.
- Analyze the detection performance in terms of false positives, false negatives, and overall accuracy.
- Compare the results with existing methods or benchmarks to validate the effectiveness of the proposed approach.
- Fine-tuning and Optimization:
- Refine the detection algorithm based on the evaluation results.
- Fine-tune parameters, explore different feature combinations, or experiment with alternative algorithms to improve performance

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 930-934

- Validation and Verification:
- Validate the effectiveness of the proposed method on additional datasets, preferably with different characteristics and complexities.
- Verify the robustness of the detection algorithm against common countermeasures used by forgers, such as noise addition or compression.

Documentation and Reporting:

- Document the methodology, experimental setup, results, and conclusions in a research paper or technical report.
- Discuss the implications of the findings and suggest potential directions for future research in image forgery detection.
- Open Source and Reproducibility:
- If possible, make the code, datasets, and trained models publicly available to facilitate reproducibility and further research in the field.

5. SYSTEM ANALYSIS

System analysis theory for fake image detection using the Error Level Analysis (ELA) algorithm involves understanding the principles behind ELA, its strengths, limitations, and how it fits within the broader context of fake image detection systems. Here's a breakdown:

Understanding ELA Algorithm:

Explain the ELA algorithm: Error Level Analysis is a technique used to detect differences in the compression levels within an image. When an image is edited and saved repeatedly, the compression levels of different parts of the image may vary, resulting in noticeable discrepancies.

Strengths of ELA:

Sensitivity to manipulation: ELA is particularly effective at detecting certain types of manipulations, such as copy-pasting or areas that have been digitally altered and saved at different compression levels.

Limitations of ELA:

Sensitivity to compression artifacts: ELA may produce false positives or miss manipulations in images with complex compression artifacts, such asJPEG compression.

Integration into Fake Image Detection Systems:

Explain how ELA fits within a broader fake image detection system: ELA can serve as one component of a multi-layered approach to fake image detection, complementing other techniques such as deep learning algorithms or metadata analysis.

Evaluation and Validation:

Discuss methodologies for evaluating the effectiveness of ELA and fake image detection systems incorporating ELA, including benchmark datasets, performance metrics, and validation techniques.

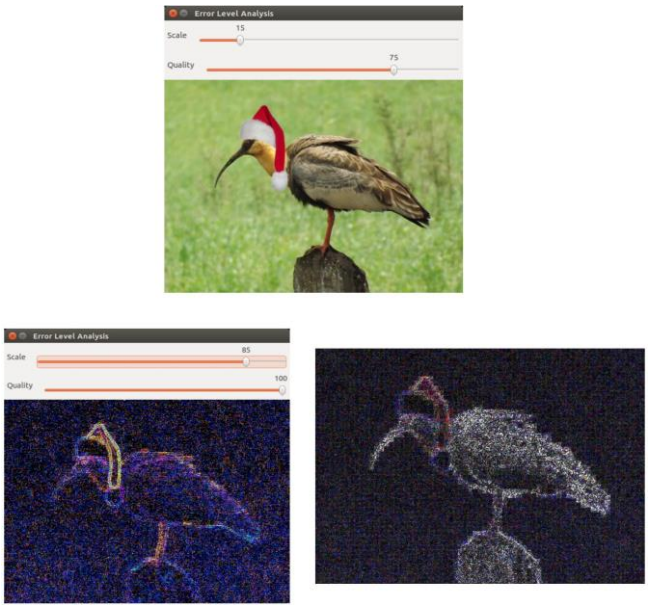

Fig 2. Fake Image Detection

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 03, March 2024, pp: 930-934

6. SYSTEM ARCHITECTURE

The system architecture gives an overview of theworking of the system.

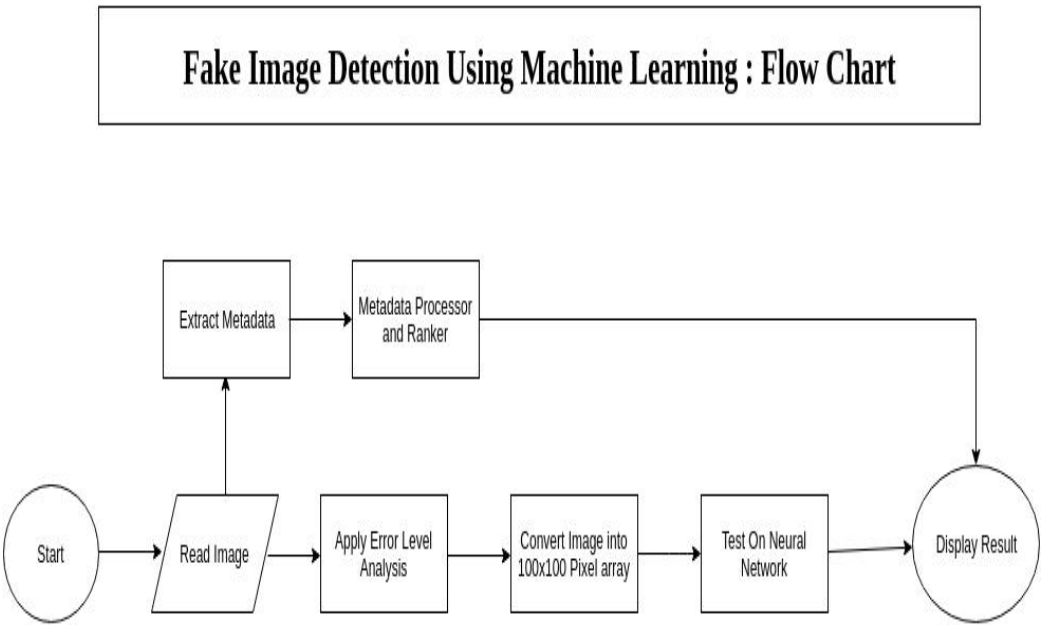

Fig 3. SYSTEM ARCHITECTURE

7. CONCLUSION

In conclusion, we proposed a Fake Image Detection System that is capable of recognize non native images. Which are edited or not real. This system is integrated with 'Error Analysis or Error Level Analysis' (ELA) algorithm which is dexterous to find faults in uploaded images with 95.00% plus of accuracy. The detection process of non native images without any human involvement which makes it diligently faster. In future, this system combined with the tools like Googleassistant , Alexa , Siri, etc the system will become more capable and intense

8. REFERENCES

[1] Abdalla Y, Iqbal T, Shehata M (2019) Copy- move forgery detection and localization using a generative adversarial network andconvolutional neural-network.

[2] Information10(09):286.https: //doi.org/10.3390 /info 10090 286

[3] Agarwal R, Verma O (2020) An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimed Tools Appl 79.https://doi.org/10.1007/s11042-019- 08495-z

[4] Bas P, Filler T, Pevn`y T (2011) Break our steganographic system the ins and outs of organizing BOSS. In: International workshop on information hiding, pp 59–70. https://doi.org/10.1007/978-3-642- 24178-9 5

[5] Christlein V, Riess C, Angelopoulou E (2010)On roatation invariance in copy-move forgery detection. In: 2010 IEEE international workshop on information forensics and security, Pp 1–6. https://doi.org/10.1109/WIFS.2010.5711472

[6] Elaskily M, Elnemr H, Sedik A, Dessouky M, El Banby G, Elaskily O, Khalaf AAM, Aslan H, Faragallah O, El-Samie FA (2020) A novel deep learning framework for copy-move forgery detection in images. Multimed Tools Appl 79. https://doi.org/10.1007/s11042-020- 08751-7