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

Image And Video Forgery Detection Using Machine Learning

Arsh Shaikh
Information Technology
Pillai College of Engineering
New Panvel, India

Prof. Rasika Thakare
Computer Engineering
Pillai College of Engineering
New Panvel, India

Hashim Deshmukh
Information Technology
Pillai College of Engineering
New Panvel, India

Mustafiz Siddiqui
Information Technology
Pillai College of Engineering
New Panvel, India

Rudein Karbari
Information Technology
Pillai College of Engineering
New Panvel, India

Abstract: With the widespread use of sophisticated manipulation techniques such as splicing, copy-move, and deepfake attacks, there is an urgent need for a comprehensive solution that combines computer vision, machine learning, and deep learning methodologies. The proposed framework leverages advanced feature extraction and convolutional neural networks to identify manipulated regions in images and videos. Additionally, a novel fusion of image and document forensics and video analysis extends the system's capabilities to detect forgeries in moving sequences. The system is designed to identify a spectrum of forgery types, including splicing, copy-move, and deepfake attacks. By demonstrating the effectiveness of machine learning in handling the changing issues of digital manipulation, this effort advances the field of forgery detection. The suggested framework highlights the potential of machine learning in bolstering the security and authenticity of multimedia content in the digital era and provides a workable and trustworthy method for detecting image and video forgeries.

Keywords— Machine learning, Forgery Detection, CNN, ELA, SVM, PBFD, DRBL

I Introduction

1.1 Fundamentals

The fundamentals of image and video forgery detection center on understanding digital media manipulation and the detection techniques tailored to it. Key methods include Error Level Analysis (ELA) and Convolutional Neural Networks (CNNs). ELA highlights discrepancies in compression levels across an image, often indicating areas of tampering. Meanwhile, CNNs, leveraging deep learning, can learn complex patterns and features to discern authentic media from manipulated versions. These techniques, combined with analysis of metadata and statistical properties, form the cornerstone of forgery detection systems. Mastery of these fundamentals is essential for creating effective tools to combat the evolving landscape of digital forgery.

1.2 Scope

The project scope entails developing robust methods for detecting image and video forgeries and creating a comprehensive framework integrating these techniques. Goals include enhancing accuracy and efficiency while providing practical tools for users to verify digital media authenticity effectively. Deliverables encompass research findings, a cohesive forgery detection system, and comprehensive documentation. Tasks involve research, implementation, testing, and evaluation phases, with associated costs and deadlines. Users include forensic analysts, law enforcement agencies, digital media professionals, and concerned general users. Product features include forgery detection, user-friendly interfaces, detailed documentation, and regular updates.

1.3 Objective

1. Develop novel algorithms for image and video forgery detection: This objective involves researching and designing new algorithms and methodologies to detect various forms of digital manipulation in images and videos. It includes exploring innovative approaches, such as deep learning techniques or hybrid methods combining different detection strategies, to improve the effectiveness and efficiency of forgery detection systems.

2. Enhance the accuracy and robustness of existing detection techniques: This objective focuses on refining and optimizing current forgery detection methods to achieve higher accuracy and resilience. It involves fine-tuning parameters, improving feature extraction processes, and addressing weaknesses or limitations in existing algorithms to enhance their performance in detecting a wide range of forgery types.

3. Investigate the impact of different types of forgeries on detection performance: This objective aims to analyze how various forms of digital manipulation, such as image splicing, copy-move forgery, or video tampering, affect the effectiveness of forgery detection techniques. It involves conducting empirical studies and experiments to understand the strengths

and limitations of different detection approaches in detecting specific types of forgeries.

4. Collaborate with domain experts and stakeholders for insights and feedback: This objective emphasizes the importance of collaboration with professionals in fields such as forensic science, law enforcement, and digital media analysis. By engaging with domain experts and stakeholders, researchers can gain valuable insights into the practical challenges and requirements of forgery detection in real-world scenarios, ensuring that detection techniques are relevant, effective, and applicable in practical settings.

2.LITERATURE REVIEW

"IDENTIFYING FAKE IMAGES THROUGH CNN BASED CLASSIFICATION USING FIDAC" [1] by Shraddha Pawar presents an exploration into fake image identification through Convolutional Neural Networks (CNNs), leveraging the FIDAC dataset . The techniques utilized are tailored to cater to the specific requirements and preferences of users or society. Image classification using CNNs involves the automatic extraction of relevant features from the data, allowing for accurate identification of fake images. The FIDAC dataset likely provides a curated collection of images specifically designed for training and testing CNN-based classification models for this purpose. This approach enables the detection of subtle differences and patterns in fake images that may not be discernible to the human eye. Through the integration of CNNs and the FIDAC dataset, the study aims to develop a robust and effective system for identifying fake images with high accuracy and reliability.

"Image Forgery Detection Using Error Level Analysis and Deep Learning" [2] by Suyuto Suyuto delves into the fusion of Error Level Analysis (ELA) and deep learning techniques for image forgery detection . The methodologies employed in this study are customized to meet the specific needs, interests, and preferences of users or society. ELA, a method analyzing discrepancies in compression levels across different regions of an image, is integrated with deep learning, particularly Convolutional Neural Networks (CNNs). This fusion enables the system to automatically learn complex patterns and features indicative of image manipulation. ELA provides insights into potential areas of manipulation, while deep learning enhances the detection accuracy by effectively capturing intricate forgery artifacts. By combining these techniques, the study aims to develop a comprehensive approach to image forgery detection that offers improved accuracy and reliability.

"Image Forgery Detection Using Deep Learning by Recompressing Images" [3] by Syed Sadaf Ali explores the application of deep learning techniques in detecting image forgeries through image recompression . The techniques employed in this study are tailored to address the specific needs, interests, and preferences of users or society. Image recompression involves altering the compression levels of images, which can reveal subtle inconsistencies indicative of manipulation. By leveraging deep learning methodologies, such as Convolutional Neural Networks (CNNs), the system can automatically learn and extract relevant features from recompressed images to identify potential forgeries. This approach offers a novel and innovative way to detect image manipulations by focusing on the changes introduced during recompression. Through the integration of deep learning and image recompression, the study aims to develop a robust and effective system for image forgery detection with high accuracy and reliability.

"A Detailed Analysis of Image and Video Forgery Detection Techniques" [4] by Shobhit Tyagi and Divakar Yadav delves into a comprehensive examination of various methodologies employed in detecting image and video forgeries. The paper discusses traditional techniques like Error Level Analysis (ELA), which scrutinizes compression artifacts to pinpoint potential areas of manipulation within images. Furthermore, modern approaches such as Convolutional Neural Networks (CNNs) are explored, leveraging deep learning to automatically identify forged images and videos. Spatial Analysis and Digital Image Ballistic Examination (DIBE) are also analyzed, highlighting their respective strengths, limitations, and applications in forensic analysis and digital security. Through this detailed comparison and evaluation, the paper provides valuable insights into the current landscape of image and video forgery detection.

“Spatial Video Forgery Detection and Localization using Texture Analysis of Consecutive Frames” by Mubbashar SADDIQUE, Khurshid ASGHAR, Usama Ijaz BAJWA, Muhammad HUSSAIN Zulfiqar HABIB [5] the paper proposes utilizing texture analysis of consecutive frames for this purpose. By examining the texture patterns within successive frames, the proposed method aims to identify inconsistencies that may indicate tampering. The approach likely involves preprocessing the video frames, extracting texture features, and applying a detection algorithm to analyze and localize potential forgeries. The paper likely discusses experimental results demonstrating the effectiveness of the proposed method in detecting and localizing spatial video forgeries, highlighting its potential contribution to the field of digital video forensics.

"Detection of video forgery: A review of literature" published in the Journal of Theoretical and Applied Information Technology in January 2015 [6] provides a comprehensive review of existing literature on the detection of video forgery. Authored by various researchers, the paper surveys the methodologies, techniques, and algorithms employed in the field of video forgery detection. It likely covers topics such as copy and move forgery detection, splicing detection, detection of video tampering through frame duplication, and other forms of video manipulation. Additionally, the paper may discuss the challenges, limitations, and future directions in video forgery detection research. Through this review, the authors aim to provide insights into the state-of-the-art approaches and advancements in the field, offering a valuable resource for researchers and practitioners in digital video forensics.

2.3 Literature Summary

SN	Paper	Advantages and Disadvantages
1.	Shraddha Pawar et al.[1]	Advantages: CNNs offer robust feature learning capabilities. Disadvantages: May require a large amount of labeled data for training.
2.	Suyoto Suyoto [2]	Advantages: Comprehensive approach combining the strengths of ELA and deep learning for forgery detection. Disadvantages: May require careful tuning of parameters and architecture for optimal performance.
3.	Syed Sadaf Ali et al. [3]	Advantages: Explores innovative approach using image recompression for forgery detection. Disadvantages: Specific details

SN	Paper	Advantages and Disadvantages
		and results of the approach are not provided in the summary.
4.	Shobhit Tyagi et al.[4]	Advantages: insightful analysis and comparisons of different methodologies, helping readers identify the strengths and weaknesses of each approach. Disadvantage:the paper reiterates well-established techniques without introducing new insights or methodologies, it may not offer significant contributions to the field.
5	Mubbashar Saddiqui et al.[5]	Advantages: Effective detection of spatial video forgeries.Precise localization of forged regions.Resilience to traditional forgery techniques. Disadvantages: Computational complexity.Sensitivity to noise.Requirement for ample training data.
6	Ankita Malage et al.[6]	Advantages: High accuracy due to pattern recognition.Automation reduces manual effort.Versatility in detecting various forgery types. Disadvantages: Dependency on quality training data.Complexity in implementation.High computational resource requirements.
7	Omar Ismael Al-Sanjary et al.[7]	Advantages: Effective detection enhances security.Likely introduces innovative techniques.Contributes to the field of digital forensics. Disadvantages: Scope may be limited, Techniques might be resource-intensive, Implementation may require advanced expertise.

Table 2.1 Summary of literature survey

3. Methodology

Error Level Analysis (ELA) is a crucial technique in image forensics, detecting changes or manipulations in digital images by compressing and re-recording them. Convolutional Neural Networks (CNN) are also effective for image forgery detection, learning to distinguish real from fake images through training on a diverse dataset. Combining ELA and CNN can improve detection accuracy, although both methods have limitations like false positives. Digital retinal localization (DRBL) and passive blind forgery detection are a promising duo for detecting video spoofing. DRBL accurately locates suspicious areas in video frames using human retina properties, providing input for passive blind detection algorithms. By integrating DRBL with passive blind detection, this method offers a comprehensive solution for detecting fake segments in videos, enhancing integrity and reliability. Utilizing a multi-method approach with ELA, CNN, DRBL, and passive blind detection can create a more accurate and reliable image and video forgery detection system.

A. Existing system architecture for image and video

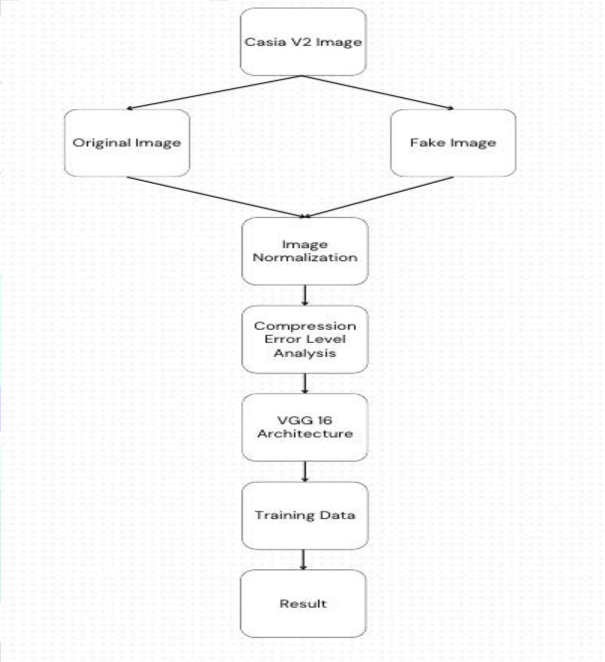

Fig. 3.1 existing architecture for image forgery detection

Image normalization standardizes images by adjusting scale, orientation, and intensity range, ensuring consistency across datasets. It reduces variations caused by lighting and camera settings, improving feature distinguishability. Common techniques include brightness adjustment, histogram equalization, and scaling pixel values. These images undergo Compression Error Level Analysis By comparing the error levels across different parts of an image, forensic analysts can determine the likelihood of tampering and identify suspicious areas for further investigation. VGG16 concentrates on having 3x3 filter convolution layers with a stride 1 and always using the same padding and maxpool layer of a 2x2 filter of stride 2. Throughout the architecture, the convolution and max pool layers are organized in the same way.

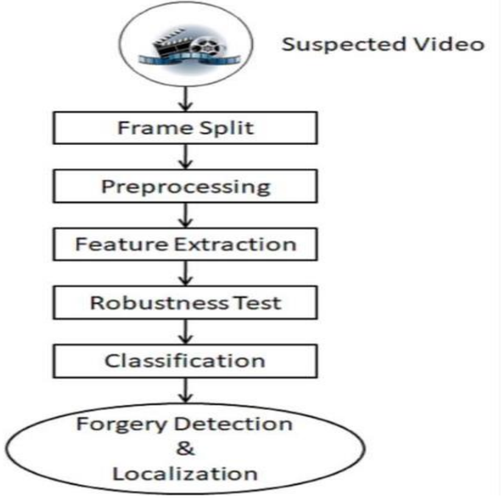

Fig. 3.2 Existing system architecture for video forgery detection

The process of analyzing a suspected video for forgery involves several steps, including segmenting the video into frames, applying preprocessing techniques to enhance quality, and feature extraction techniques such as frame prediction, mean square error, photo response non-uniformity, and frame correlation. Techniques used to detect forged videos include SIFT, optical flow, and block division. Robustness tests are crucial to ensure the efficiency of an algorithm or model, as post-processing operations may need to be applied to conceal forged evidence. Classification is then examined to determine the suitability of each classifier for differentiating between original and forged videos. The SVM and RBF-MSVM are used to detect all types of forgeries, particularly when establishing the authenticity of an original video. Overall, robustness tests are essential to ensure the system's performance and accuracy in detecting forgeries.

B. proposed system architecture

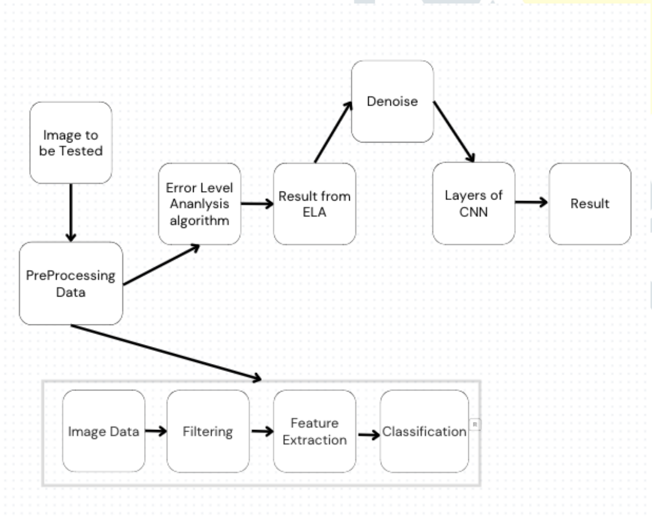

Fig. 3.3 proposed architecture for image forgery detection

The proposed system architecture for image fraud detection involves several steps, starting with dataset preparation. The open image dataset's annotations are converted into a format accessible by the model during the training process. The testing process involves converting the image into an ELA image format, calculating the noise and signal ratio, denoising the image, and converting it to a black-and-white format. The model is split into two datasets using the train/test method, with 80% used for training and 20% for testing. The CNN model is applied to high-scoring regions within the image considered forgeries. A confusion matrix technique summarizes the performance of the classification algorithm. A table plots all predicted and actual values of the classifier, and a confidence score is calculated as an evaluation standard. If the confidence score is below a threshold (0.9), decisions may be made to hold back from making decisions. Each label is assigned a numerical value called Confidence, while Predict evaluates an issue.

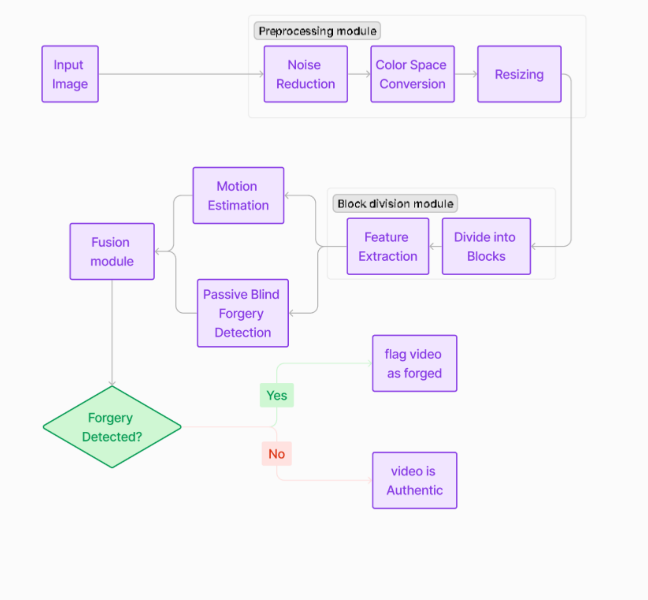

Fig. 3.4 proposed architecture for video forgery detection

The system starts by analyzing an input video sequence for forgery detection. It undergoes tasks like noise reduction, color space conversion, and resizing to prepare the frames for analysis. The Block Division module divides each frame into smaller blocks or patches, extracting features like texture features, color histograms, and gradient information. The Differentially-Robust Block Matching Algorithm (DRBL) is used to estimate motion vectors between consecutive frames, identifying regions with significant motion. The Passive Blind Forgery Detection module analyzes video frames and motion vectors to detect anomalies or inconsistencies without prior knowledge of the original video. The Fusion module integrates the results from DRBL motion estimation and passive blind forgery detection, generating a combined forgery detection map. Post-processing refines the combined detection results, removing false positives and enhancing detection accuracy. Spatial and temporal filtering smooths the forgery detection map. The Output module presents the final forgery detection results, indicating suspected tampered regions and their confidence levels. A feedback loop continuously improves the system's performance based on user feedback and evaluation results.

C. Algorithms / Techniques

1. Convolutional Neural Networks (CNNs) are widely used for image forgery detection, utilizing hierarchical layers of learned features to capture complex patterns and structures in images. They can distinguish between authentic and forged content, eliminating the need for manual feature engineering. However, CNNs may suffer from overfitting when trained on limited datasets and their performance relies heavily on the availability of large, diverse training data.

2. Error Level Analysis(ELA): Error Level Analysis (ELA) is a pivotal technique in the field of digital image forensics, offering insights into potential areas of manipulation within images. Used by Author Two et al. [3], ELA operates by highlighting discrepancies in compression levels across various regions of an image. These discrepancies often signify alterations introduced during the editing process, such as cloning or pasting. ELA's simplicity and effectiveness make it a valuable tool for both researchers and forensic analysts in identifying suspicious areas within images.
3. DRBL (Differentially-Robust Block Matching Algorithm):DRBL is a specific algorithm used for motion estimation in video processing.It is employed to find the motion vectors between consecutive frames of a video sequence.The algorithm breaks down each frame into smaller blocks and searches for the best match between blocks in consecutive frames to estimate the motion between them.DRBL aims to be robust against inconsistencies and noise in the video frames, providing accurate motion estimation even in challenging conditions.
4. Passive blind forgery detection : Passive blind video forgery detection refers to a method that aims to detect video forgeries without requiring any additional information or prior knowledge about the original video. In this approach, the detection algorithm analyzes the video content itself to identify inconsistencies or anomalies that may indicate tampering. This could involve detecting discrepancies in motion patterns, inconsistencies in lighting or shadows, or inconsistencies in object trajectories. The algorithm relies solely on the observable characteristics of the video frames to flag potential instances of forgery, without needing access to the original unaltered video or any watermarking or authentication techniques.

4. Application

A. Social Applications:

1. Combating Misinformation: Image and video forgery detection helps combat the spread of misinformation by identifying manipulated media content before it spreads widely.

2. Preserving Trust in Media: Forgery detection ensures the authenticity of digital images and videos, preserving trust in media sources and content creators.

3. Protecting Individuals' Rights: By identifying manipulated images, forgery detection helps protect individuals' rights and privacy, particularly in cases of image-based harassment or revenge porn.

4.Supporting Legal Proceedings: Forgery detection provides crucial evidence in legal investigations and court proceedings, establishing the authenticity of digital media content.

B. Technical Applications:

1. Digital Forensics: Forgery detection is essential in digital forensics investigations, where it helps uncover tampered or manipulated media content for criminal investigations.

2.Content Authentication: Forgery detection verifies the authenticity of digital images and videos in content authentication systems, ensuring they have not been altered for deceptive purposes.

3. Digital Security: Forgery detection is crucial for digital security applications, such as detecting forged documents or currency to prevent fraud and counterfeiting.

4.Media Integrity Verification: In media production workflows, forgery detection ensures the integrity of digital media content from creation to distribution, maintaining quality and authenticity standards.

5. Conclusion

The Image and Video Forgery Detection Project focuses on developing and refining techniques to accurately detect digital manipulation in images and videos. Utilizing a blend of traditional methods like Error Level Analysis (ELA) and contemporary approaches such as Convolutional Neural Networks (CNNs), along with Differentially-Robust Block Matching Algorithm (DRBL) and Passive Blind Forgery Detection. The project aims to bolster the accuracy, efficiency, and resilience of forgery detection systems. Key objectives include developing novel algorithms aligned with user and societal needs, exploring practical applications in forensic analysis and digital security, and collaborating with experts to ensure operational efficacy. Additionally, the project addresses video forgery techniques and algorithms, extending its focus beyond static images to encompass dynamic media content. Socially, the project strives to combat misinformation, preserve media trust, protect individual rights, support legal proceedings, and prevent social unrest by identifying and debunking forged media content. Technically, it holds implications in digital forensics, content authentication, security, media integrity verification, and privacy protection, all contributing to a safer digital landscape. In summary, the Image and Video Forgery Detection Project is a multifaceted endeavor aimed at advancing forgery detection technology, bolstering trust in digital media, and fostering a safer online environment. Through a combination of cutting-edge techniques, interdisciplinary collaboration, practical applications, and an expanded focus on video forgery, the project aims to address real-world challenges and contribute to the development of robust and reliable forgery detection systems.

Acknowledgment

We would like to express our special thanks to Prof. Rasika Thakare, our major project-I guide and project coordinator. who guided us through the project and who helped us in applying the knowledge that we have acquired during the semester and learning new concepts.

We would like to express our special thanks to Dr. Satishkumar Varma, Head, Department of Information Technology, who gave us the opportunity to do this major project-I because of which we learned new concepts and their application.

Finally we would like to express our special thanks to Principal Dr. Sandeep Joshi who gave us the opportunity and facilities to conduct this major project-I.

References

[1] Shraddha Pawar, "IDENTIFYING FAKE IMAGES THROUGH CNN BASED CLASSIFICATION USING FIDAC", August 2022, [Online]. Available: https://ieeexplore.ieee.org/document/9862034

[2] Suyuto Suyuto, "Image Forgery Detection Using Error Level Analysis and Deep Learning" August 2018, [Online]. Available: https://www.researchgate.net/publication/332561655_Image_forgery_detection_using_error_level_analysis_and_deep_learning

[3] Syed Sadaf Ali, "Image Forgery Detection Using Deep Learning by Recompressing Images", January 2022 [Online]. Available: https://www.mdpi.com/2079-9292/11/3/403

[4] Shobhit Tyagi and Divakar Yadav, "A Detailed Analysis of Image and Video Forgery Detection Techniques". January 2022, [Online]. Available: https://www.researchgate.net/publication/357808453_A_detailed_analysis_of_image_and_video_forgery_detection_techniques

[5] Mubbashar SADDIQUE, Khurshid ASGHAR, Usama Ijaz BAJWA, Muhammad HUSSAIN Zulfiqar HABIB, “Spatial Video Forgery Detection and Localization using Texture Analysis of Consecutive Frames” , August 2019, [Online]. Available https://www.researchgate.net/publication/343007097_Spatial_Video_Forgery_Detection_and_Localization_using_Texture_Analysis_of_Consecutive_Frames

[6] Ankita Malage, Vidya Kesarakar, Bhavana Sarapure, Asma Nadaf, and Prof. Neelamma Shivannavar, “Video Forgery Detection Using Machine Learning”, June 2023, [Online]. Available https://ijsret.com/wp-content/uploads/2023/05/IJSRET_V9_issue3_208.pdf

[7] Omar Ismael Al-Sanjary, “Detection of video forgery: A review of literature”, January 2015, [Online]. Available https://www.researchgate.net/publication/281940622_Detection_of_video_forgery_A_review_of_literature