Journal of Advanced Research in Computer Graphics and Multimedia Technology
Volume 11, Print Issue 1 - 2024, Pg. No. 24-31
Peer Reviewed Journal

Review Article

Visual Truth in the Digital Age: A Review of Image and Video Authentication and Verification Approaches

Khushwant Virdi[1], Navjot Singh Talwandi[2]

[1,2]Department of Computer Science Engineering Chandigarh University Punjab, India.

I N F O

Corresponding Author:
Navjot Singh Talwandi, Department of Computer Science Engineering Chandigarh University Punjab, India.
E-mail Id:
navjotsingh49900@gmail.com
Orcid Id:
https://orcid.org/0009-0000-7491-4663
How to cite this article:
Visual Truth in the Digital Age: A Review of Image and Video Authentication and Verification Approaches. *J Adv Res Comp Graph Multim Tech.* 2024; 11(1): 24-31.

Date of Submission: 2024-03-20
Date of Acceptance: 2024-04-23

A B S T R A C T

The authenticity and integrity of multimedia con- tent, including photos and videos, have become crucial in the age of the explosion of digital information. Concerns about the relia- bility of visual information have increased with the emergence of sophisticated tools for picture and video manipulation. Through a thorough investigation of multimedia forensics and an emphasis on the authentication of images and videos, our research aims to address these concerns. Through a thorough examination of the available literature and methodological analysis, this study digs into the diverse world of multimedia forensics. It examines the methods, algorithms, and strategies now in use for identifying modifications, digital forgeries, and tampering with photographs and videos. This review goes beyond the theoretical to offer useful approaches and ideas for judging the reliability of multimedia content in a variety of settings, including journalism, forensics, and the examination of digital evidence. The complexity of mul- timedia authenticity verification is explained in this study, which adds to the continuing conversation on digital media integrity and security. The conclusions and methodologies discussed here not only contribute to preserving the credibility of multimedia content but also have implications for improving digital forensic investigations, safeguarding intellectual property, and enhancing the reliability of visual data in the digital age. This study is an important resource for academics, professionals, and decision- makers who are debating how to uphold authenticity and trust in our visual media landscape as the lines between reality and digital representation become more and more hazy.

Keywords: Forgery Detection, Deepfake Detection, Image Tampering, Video Authentication, Audio Authentication, Multi- Media Analysis, Media Integrity Verification, Content Authentic- Ity Verification

Introduction

The reliability of multimedia content, which includes both photos and videos, is a hot topic in today's digital age. Multi-media manipulation, tampering, and outright falsification are widespread problems brought on by the development of digital media technologies and the simplicity of internet distribution. The legitimacy of multimedia content has never been more at risk, nor have the repercussions been more severe, from the falsification of photographic

evidence to the production of convincing deepfake videos. Multimedia forensics is a crucial field that provides a complex strategy to handle the pressing issues around image and video authenticity in this age of digital disinformation. Its primary goal is to scrutinize multimedia information meticulously in an effort to separate authentic from fake using scientific approaches, technology, and analytical tools. Multimedia forensics aims to provide investigators, media professionals, and the general public with the tools and knowledge required to ascertain the integrity of visual media in an increasingly ambiguous environment by drawing on principles from a variety of fields, including computer science, image processing, and forensic science.

This review paper's aim is to delve into the complex field of multimedia forensics, with an emphasis on the authentication of images and videos. This paper sets out on a quest to understand the approaches, developments, and difficulties that make up this dynamic sector. Here, the main aim is to illuminate the future in the unrelenting search for truth and reliability in the field of multimedia material through a synthesis of existing literature, exploration of cutting-edge approaches, and the pre-sensation of useful case examples. The pursuit of multimedia forensics gains greater significance in a world where the distinction between fact and fiction becomes hazier every day. The focus is to set out on a quest to strengthen the pillars of accuracy, reliability, and trust in our digital visual environment by investigating the broad field of multimedia forensics and its function in authenticating images and videos. Research in the field of multimedia forensics, particularly image and video authenticity verification, is continuously evolving due to the increasing sophistication of digital manipulation techniques. Authenticating visual evidence is crucial in court processes. Media that has been incorrectly vetted can result in false convictions or the rejection of reliable evidence. Research in multimedia forensics addresses the requirement for precise authentication while also bringing attention to the moral and legal implications of using multimedia evidence.

In a variety of fields, such as journalism, law enforcement, and digital advertising, trust in visual media is crucial. The effects on public perception and decision-making can be severe when trust is lost as a result of the presence of fake news. By creating methods that enable consumers to confirm the validity of images and videos, this study area helps reestablish and perpetuate trust in visual media. Maintaining the trustworthiness of information sources depends on this. The ease with which photos and videos can be altered in the digital age has resulted in a rise in the production of fraudulent and deceptive media content. The propagation of false information, libel, and even the possible disruption of crucial operations like law enforcement and journalism are all major repercussions of this. Fighting this problem requires research in multimedia forensics for video and image authenticity verification. It offers techniques and tools for separating real content from edited or fraudulent media, maintaining the validity of visual data.

It is critical that detection techniques keep up with technological developments in false media production as they progress. By fostering the development of sophisticated detection techniques, machine learning algorithms, and forensic tools that can accurately identify corrupted media, research in this area contributes to a strong defense against new threats. With more knowledge about multimedia forensics, content producers and digital artists are urged to apply their abilities in an ethical and responsible manner. By highlighting the dangers and repercussions of media manipulation and offering advice on how to produce and distribute genuine content, this research promotes a culture of responsible media creation. Join us on this journey to decipher, authenticate, and reveal the truth buried behind the pixels and frames of multimedia content—a vital task for the preservation of veracity and correctness in the digital age.

Literature Review

The field of multimedia forensics has advanced greatly over time, with a particular emphasis on the authentication of images and videos. To solve the problems brought forth by the digital age, researchers have investigated a wide range of strategies and techniques. This survey of the literature gives a broad overview of important studies and significant advancements in the field.

Peng, M. Long, et al., " FD-GAN: Face De-Morphing Generative Adversarial Network for Restoring Accomplice's Facial Image," which facilitates the identification of identity morphing and restores the facial images of two identities that are fused. This system also helps in restoring two levels of loss and helps in recovering features of individual images. It shows huge potential to be used in criminal investigations and passport-related crimes.[1]

Rathgeb, C. Busch et al.," Face Morphing Attacks: A Threat to eLearning?" In their work, they focused on how the use of image morphing has increased substantially, especially during COVID-19. In remote education (online mode), various incidents have taken place wherein the students use morphing techniques and some other individuals take the online examination without being noticed. They observed a dataset and found that most of the face detection systems are unable to identify such discrepancies.[2]

Gupta, S. Gupta, et al., "Video authentication in digital forensic," underscored h how online editing tools and software are widely used for manipulating the content of videos. They proposed an algorithm that helps identify the edited and tampered videos in two stages. In the first

stage, they processed the pixels of the images to produce data frame by frame motion energy time. In the second stage, they located the attacks where editing is done with the help of support vector machines.[3]

Li, "Design of Video Forensics and Storage Framework Based on Embedded Technology," worked on improving the efficiency and technicalities of the SPCE3200 processor and its platform that is used for research and development of analysis. They built a new system platform that is used for video forensics. They also focused on the storage and processing of the video-forensic platform.[4]

Alghafli and T. Martin, "Identification and recovery of video fragments for forensic file carving," focused on the imperative role of file carving technique in the criminal investigation of video file evidence. They proposed a method that would process the video fragments and identify if they were overwritten. In this technique, they used detectors and validators for processing and accepting or rejecting a fragment. They designed a prototype called VidCarve, performed several experiments, and found that the method is more efficient and provides more accurate results in comparison to the online tools and methods available.[5]

Yu-Ming Liang, "Video condensation for video forensics," proposed a video condensation technique that can be used for searching for and pointing out criminal incidents from a large number of surveillance and security cameras. They designed a condensation technique that can be used to compress long-duration video into short video clips by removing redundant data and keeping only important information. Their proposed technique followed three major steps: image and sequence transformation, motion and time-oriented data filter, and ribbon carving.[6]

M. Bagkratsas and N. Sklavos, "Digital Forensics, Video Forgery Recognition, and Cybersecurity Systems," Their objective was to suggest a novel counterfeit detection technique based on the properties and features of dense optical flow. This technique is used in cheap gadgets that can record static CCTV video. Their framework was tested to see whether it could identify, copy-move, insert, and delete frauds.[7] A. Raj and D. Sankar," Counter Forensics: A New PRNU-Based Method for Image Source Anonymization," In order to conceal the identity of the image from attackers, a new counter-forensic technique is presented in this study. To obscure the identity, the PRNU (Photo Response Non-Uniformity) (visual "fingerprint") of the image is subtracted and replaced with a variation from the PRNU of a different camera. Multiple pictures of the identical events were taken by five separate cameras and were used to test the procedure.[8]

Figure 1.Earlier Findings by different people

Paper Title	Authors	Research Focus	Key findings
Image Forgery Detection and Classification Using Deep Learning and FIDAC Dataset	Shraddha Pawar, Gaurangi Pradhan, et al.	Used CNN with FIDAC dataset to determine image forgery	Introduced the FIDAC dataset, proposed a CNN model for picture forgery detection, and carried out experimental analysis contrasting their model with pre-defined models on other datasets.
FD-GAN: Face De-Morphing Generative Adversarial Network for Restoring Accomplice's Facial Image	F. Peng, M. Long, et al.	Image and video authenticity and restoration for criminal investigations and passport crimes	Development of FD-GAN for restoring facial images of accomplices and recovering individual features. Potential use in criminal investigations.
Video authentication in digital forensic	A. Gupta, S. Gupta, et al.	Detection of edited and tampered videos; algorithm using motion energy time and support vector machines	Proposed algorithm identifies edited videos in two stages, processing pixel motion energy and locating editing attacks.
Design of Video Forensics and Storage Framework Based on Embedded Technology	Y. Li	Efficiency and technical enhancements in the SPCE3200 processor for video forensics and storage	Improvement of SPCE3200 processor platform for video forensics research and development, focusing on storage and processing.
Identification and recovery of video fragments for forensics file carving	K. Alghafli, T. Martin	Role of file carving in video forensics investigations; method for processing video fragments	Proposed method processes video fragments, identifies overwrites, and uses detectors and validators for efficient and accurate results compared to online tools.
Digital Forensics, Video Forgery Recognition, for Cybersecurity Systems	I. M. Bagkratsas, N. Sklavos	Detection of counterfeit videos using dense optical flow; application in low-cost CCTV devices	Suggested a counterfeit detection technique based on dense optical flow properties in low-cost CCTV video recording devices.
Anti-Forensics for Face Swapping Videos via Adversarial Training	G. Zhu, Y. Li, et al.	Development of a GAN model for anti-forensics in face-swapping videos	Innovative GAN model with overseeing modules to improve image quality and a loss function to attack DeepFake forensics detectors. Demonstrated effectiveness through experiments.

Integration of Machine Learning and Blockchain for Vetoing Forgeries in the Education Sector	Dhruvil Shah, Devarsh Patel, et al.	Use of machine learning and blockchain to prevent educational forgeries	Developed a system combining machine learning and blockchain to address challenges like forgery of educational records and fake degrees, providing a decentralized database for student records.
Easy-to-Use Verification Mechanism for Electronic and Printed Documents	Md. Majharul Haque, Muhammad Shakil Pervez, et al.	Verification mechanism for document authenticity using smartphones and modern technologies	Designed a user-friendly verification system for electronic and printed documents, ensuring originality using readily available technologies like smartphones.
Pixel-Based Techniques for Image Forgery Detection	Mohd Dilshad Ansari, S.P. Ghrera, et al.	Pixel-based methods for image forfeited picture identification	Discussed several pixel-based methods for spotting fake images, with a particular emphasis on copy-move and splicing methods.
Document Manipulation Detection and Authenticity Verification Using Machine Learning and Blockchain	Shantanu Sarode, Utkarsha Khandare, et al.	Detection of manipulated documents and authenticity verification using neural networks and blockchain	Proposed a system using neural networks and Error Level Analysis for document manipulation detection, shifting from the traditional metadata-based method.

W. Fan, K. Wang, et al., ”Median Filtered Image Quality Enhancement and Anti-Forensics via Variational Deconvolution,” Using median-filtered (MF) pictures, this research suggests an image variational deconvolution framework for both quality improvement and anti-forensics. The convolution term, fidelity term in relation to the MF image, and prior term make up the suggested optimization-based framework. Their method is used to denoise images and is widely accepted in forensics.[9]

F. Ding, Y. Li, et al., ”Anti-Forensics for Face Swapping Videos via Adversarial Training,” suggested a GAN model to function as an anti-forensics model in this paper. It has an innovative architecture with additional overseeing modules to improve the visual quality of images. In addition, a loss function is created to increase the effectiveness of the suggested model. We demonstrate through experimental assessments that the proposed strategy may launch attacks against the fake forensics detectors.[10]

Shraddha Pawar, Gaurangi Pradhan, et al.’s research paper titled ”Image Forgery Detection and Classification Using Deep Learning and the FIDAC Dataset” was published in IEEE Explore. In this paper, they suggested a model that uses CNN for classification after being fed with ELA-preprocessed images to detect image forgery. They also introduced their own dataset, FIDAC (Forged Images Detection and Classification), which consists of the original camera-clicked images along with their tampered versions. Additionally, they performed an experimental investigation in which they combined their suggested CNN model with well-known pre-defined models on a variety of dataset combinations.[11] Dhruvil Shah, Devarsh Patel, et al. Blockchain and machine intelligence were combined to create a system that could veto forgeries and deliver effective outcomes in the education industry. To address issues like false degrees and educational records, a method combining machine learning and blockchain was developed. With the proposed approach, the institution would have access to a formal, decentralized database of student records.[12]

Siddharth Solaiyappan and Yuxin Wen, in their paper “Machine learning-based medical image deepfake detection,” addressed the detection of medical deepfakes in cases of injection and removal of tumors from medical scans. They used eight distinct machine learning algorithms: support vector machines, decision trees, and random forests. These are conventional machine learning methods: Dense Net121, DesnseNet201, ResNet50, ResNet101, and VGG19. These five deep learning models are used to tell apart photographs that have been altered from those that haven’t.[13]

Shantanu Sarode, Utkarsha Khandare et al., in the paper “Document manipulation detection and authenticity verification using machine learning and blockchain,” developed a method to use neural networks to identify altered photographs and documents and to confirm the legitimacy of specific identity documents. Instead of using the document’s metadata, which was the current approach for detection, the proposed system used neural network principles under image processing using the error level analysis method.[14]

Md. Majharul Haque, Muhammad Shakil Pervez, et al. proposed a new method of document verification that applies to printed and electronic documents. In contrast to the majority of the current methods for verifying authenticity and integrity with contemporary technologies like digital signatures, blockchain, etc., the suggested system would provide a way to certify the uniqueness of the document. The bulk of individuals cannot use these existing methods since they are generally expensive. This suggested method is made to be simple to use, even with just a smartphone, and the result is produced quickly.[15]

Mohd Dilshad Ansari, S.P. Ghrera, et al., without any prior knowledge of the original image, use pixel-based techniques to identify forgeries and verify the validity of digital images. This paper discusses several pixel-based methods for spotting fake images, including copy-move and splicing methods.[16]

Michihiro Kobayashi, Takahiro Okabe, et al. developed a method for digital video forensics based on noise properties. The proposed technique accomplishes per-pixel evaluation with a high degree of precision for detecting authenticity by analyzing the noise characteristics of each pixel by employing temporal averaging.[17] From its early days in picture forensics to cutting-edge video authenticity verification, the area of multimedia forensics has grown remarkably. To address the dynamic terrain of digital media manipulation, researchers have created a wide range of methodologies, from sensor-based studies to deep learning applications. Despite persistent obstacles, the future is bright thanks to developing technologies and coordinated efforts that are essential for preserving the legitimacy and authenticity of multimedia material in our digital age.

An interdisciplinary area called multimedia forensics is devoted to the investigation, confirmation, and authenticity of digital multimedia content, with a focus on pictures and videos. To understand the complexities of image and video authenticity verification, it is crucial to be familiar with the fundamental vocabulary, concepts, and approaches used in multimedia forensics. A specialized area of forensic science called multimedia forensics focuses on the examination and authentication of multimedia data, including pictures, audio files, videos, and other digital media. The following are some essential words and ideas in multimedia forensics:

1. **Multimedia Forensics:** The area of forensic science concerned with the evaluation, improvement, verification, and interpretation of numerous multimedia evidence types.
2. **Digital Forensics:** The broader field that encompasses the recovery, preservation, and analysis of digital evidence, including multimedia data, from electronic devices and storage
3. **Image forensics:** is the examination of digital images to detect manipulation, tampering, or forgery and to determine their authenticity and origin.
4. **Video forensics:** is the analysis of video recordings to verify their authenticity, enhance video quality, and identify objects or individuals within the footage.
5. **Audio Forensics:** The examination of audio recordings to identify and analyze sounds, voices, and background noise, as well as to detect any tampering or alterations.

Methodology

Image Forensics Methodologies

1. **Error Level Analysis (ELA):** To identify areas of an image that may have been digitally altered, ELA analyzes compression artifacts.
2. **Noise analysis:** analyzing an image's noise patterns to look for alteration or tampering indicators.
3. **Source identification:** is the process of identifying the camera or equipment that took the shot by looking for sensor pattern noise or a non-uniform photo response.
4. **Image enhancement:** methods to enhance images and bring out details that were previously hidden, such as sharpening, contrast modification, and filtering.

Video Forensics Methodologies

1. **Video Authenticity Analysis:** Verifying the authenticity of video footage by examining temporal inconsistencies, compression artifacts, and frame duplication.
2. **Video Stabilization:** Reducing shakiness in videos to improve stability and enhance visual clarity.
3. **Frame Rate Analysis:** Analyzing frame rates to identify possible edits or splicing in video sequences.
4. **Object and Motion Analysis:** Tracking objects or individuals in video frames to understand their movements
5. **Video Tampering Detection:** Identifying signs of video tampering, such as frame removal or alteration.

Audio Forensics Methodologies

1. **Audio Authentication:** Verifying the authenticity of audio recordings by analyzing waveform patterns, noise profiles, and acoustic properties.
2. **Voice Analysis:** Comparing and identifying speakers' voices through techniques like voiceprint analysis and speaker
3. **Audio Enhancement:** Reducing background noise, filtering out unwanted sounds, and improving audio quality.
4. **Audio Time and Date Analysis:** Examining audio metadata to determine the recording date and time

Deepfake Detection Methodologies

1. **Deep Learning Models:** Utilizing deep neural networks to detect fake videos or audio recordings by identifying inconsistencies in facial movements, lip-syncing, and audio-visual synchronization.
2. **Face Recognition:** Comparing facial features in videos to known databases to identify manipulated faces.
3. **Audio-Visual Synchronization Analysis:** Assessing the alignment of audio and visual elements in multimedia content to spot anomalies.

Image Forgery Detection

Active and passive authentication are the two basic categories used to classify image forgery detection or image authenticity verification.

Video Authenticity Verification

The verification of the authenticity of digital videos is a critical endeavor in the realm of multimedia forensics. As videos continue to play a pivotal role in communication and information dissemination, ensuring their credibility

and integrity becomes paramount. In this section, we will explore various techniques and tools employed for video authenticity verification, including video forensics methods, and present case studies that exemplify their practical applications.

Video Tampering Detection

Video tampering detection techniques aim to identify unanalyzed alterations or manipulations in video content. These alterations can range from simple splicing and editing to more sophisticated deep-fake technology.

Deep learning-based approaches

Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have been used more frequently in video forensics with the development of deep learning. These AI-based techniques are excellent at spotting subtle hints and manipulating artifacts.

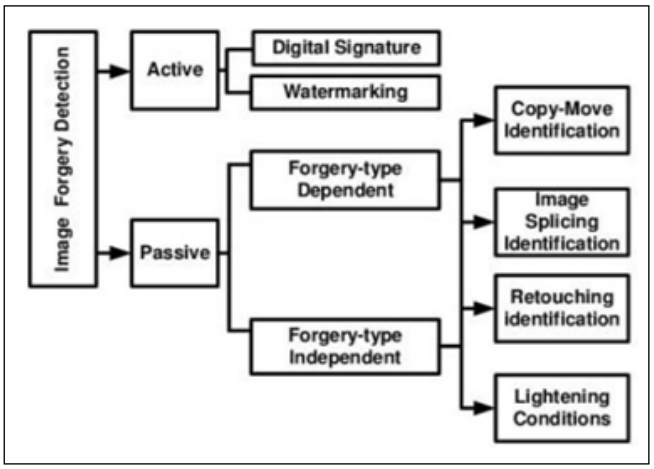

Figure 2.Image Forgery Detection Classifications

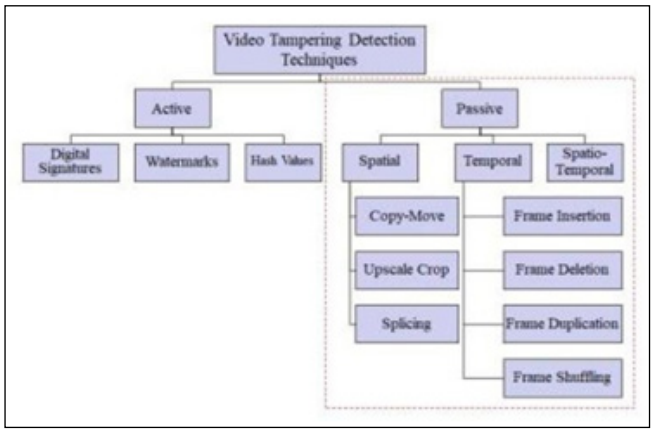

Figure 2.Image Forgery Detection Classifications

Result

In the digital age, the authenticity and integrity of images and videos have become increasingly important due to the ease of manipulation and alteration. Various approaches have been developed to authenticate and verify the visual truth of digital media.

Some Common Approaches Include

Digital Watermarking: This technique involves embedding a unique identifier or watermark into the image or video, which can be used to verify its authenticity.

Hash Functions: Hash functions generate a unique hash value for an image or video based on its content. Any alteration to the content will result in a different hash value, allowing for verification.

Forensic Analysis: Forensic analysis techniques examine various aspects of an image or video, such as metadata, compression artifacts, and inconsistencies, to detect signs of manipulation or tampering.

Blockchain Technology: Blockchain technology can be used to create a decentralized and tamper-proof record of image and video transactions, ensuring their authenticity and integrity.

Machine Learning: Machine learning algorithms can be trained to detect and classify manipulated or fake images and videos based on patterns and anomalies in the data.

Conclusion

This paper focuses on the fact on the fact that the need for image and video authentication verification methods is increasing. With the widespread availability of powerful image and video editing tools, it has become easier than ever to alter media content. This makes it essential to authenticate the authenticity of images and videos to ensure that they have not been tampered with. Multimedia is easily manipulated these days to align with the goals of the manipulator. This results in a loss of reliability for the data, and thus it needs to be verified for forgery detection. Authenticity is paramount in journalism, forensics, legal proceedings, and various other fields. Ensuring the integrity of visual content helps maintain trust and credibility in these areas. This is one of the most important parts of multimedia forensics, and since video and images can be presented in court as evidence, it is important to prove the authenticity of the evidence, as the evidence could have been manipulated. Deepfake technology has advanced significantly, allowing for the creation of highly convincing fake videos. Image and video authentication can help detect and counteract the spread of fakes, which can be used for malicious purposes, and in order to stop these activities, we need a reliable verification method to check the authenticity of files. There has been much research conducted, and this paper tries to summarize some of the most important contributions in this field. This paper discusses the focus of their research and the key findings. In this multimedia, forensic methods are briefly explained.

This paper also includes some case studies to demonstrate the importance of image and video authentication.

References

1. F. Peng, L. -B. Zhang and M. Long, ”FD-GAN: Face DeMorphing Gen- erative Adversarial Network for Restoring Accomplice’s Facial Image,” in IEEE Access, vol. 7, pp. 75122- 75131, 2019, doi: 10.1109/ACCESS.2019.2920713.
2. C. Rathgeb, C. Busch et al. ”Face Morphing Attacks: A Threat to eLearning?,” 2021 IEEE Global Engineering Education Con- ference (EDUCON), Vienna, Austria, 2021, pp. 1149-1154, doi:
3. A. Gupta, S. Gupta and A. Mehra, ”Video authentication in digital forensic,” 2015 International Conference on Futuristic Trends on Com- putational Analysis and Knowledge Management (ABLAZE), Greater Noida, India, 2015, pp. 659- 663, doi: 10.1109/ABLAZE.2015.7154945.
4. Y. Li, ”Design of Video Forensics and Storage Framework Based on Embedded Technology,” 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2021, pp. 135-138, doi: 10.1109/ICIRCA51532.2021.9544666.
5. K. Alghafli and T. Martin, ”Identification and recovery of video frag- ments for forensics file carving,” 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 2016, pp. 267-272, doi: 10.1109/ICITST.2016.7856710.
6. Yu-Ming Liang, ”Video condensation for video forensics,” 2012 IEEE International Conference on Computational Intelligence and Cybernetics (CyberneticsCom), Bali, Indonesia, 2012, pp. 180-184, doi: 10.1109/Cy- berneticsCom.2012.6381642.
7. I. M. Bagkratsas and N. Sklavos, ”Digital Forensics, Video Forgery Recognition, for Cybersecurity Systems,” 2021 24th Euromicro Confer- ence on Digital System Design (DSD), Palermo, Italy, 2021, pp. 510- 513, doi: 10.1109/DSD53832.2021.00082.
8. A. Raj and D. Sankar, ”Counter Forensics: A New PRNU Based Method for Image Source Anonymization,” 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), Coimbatore, India, 2019, pp. 1-7, doi: 10.1109/ICECCT.2019.8868948.
9. W. Fan, K. Wang, F. Cayre and Z. Xiong, ”Median Filtered Image Qual- ity Enhancement and Anti-Forensics via Variational Deconvolution,” in IEEE Transactions on Information Forensics and Security, vol. 10, no. 5, pp. 1076-1091, May 2015, doi: 10.1109/TIFS.2015.2398362.
10. F. Ding, G. Zhu, Y. Li, X. Zhang, P. K. Atrey and S. Lyu, ”Anti- Forensics for Face Swapping Videos via Adversarial Training,” in IEEE Transactions on Multimedia, vol. 24, pp. 3429-3441, 2022, doi: 10.1109/TMM.2021.3098422.
11. S. Pawar, G. Pradhan, B. Goswami and S. Bhutad, ”Identifying Fake Images Through CNN Based Classification Using FIDAC,” 2022 In- ternational Conference on Intelligent Controller and Computing for Smart Power (ICICCSP), Hyderabad, India, 2022, pp. 01-06, doi: 10.1109/ICICCSP53532.2022.9862034
12. Shah, D., Patel, D., Adesara, J. et al. Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector. Vis. Comput. Ind. Biomed. Art 4, 18 (2021). https://doi.org/10.1186/s42492- 021-00084-y.
13. Solaiyappan, Siddharth, and Yuxin Wen. ”Machine learning based med- ical image deepfake detection: A comparative study.” Machine Learning with Applications 8 (2022): 100298.
14. Sarode, Shantanu, Utkarsha Khandare, Shubham T. Jadhav, Avinash Jannu, Vishnu Kamble and Digvijay Patil. “Document Manipulation Detection and Authenticity Verification Using Machine Learning and Blockchain.” (2020)
15. Md. Majharul Haque, Md. Nasim Adnan, Mohammod Akbar Kabir, Mohammad Rifat Ahmmad Rashid, Abu Sadat Mohammad Yasin and Muhammad Shakil Pervez, “An Innovative Approach of Verification Mechanism for both Electronic and Printed Documents” International Journal of Advanced Computer Science and Applications (IJACSA), 11(8), 2020. http://dx.doi.org/10.14569/IJACSA.2020.0110876
16. Mohd Dilshad Ansari, S. P. Ghrera and Vipin Tyagi (2014) PixelBased Image Forgery Detection: A Review, IETE Journal of Education, 55:1, 40-46, DOI: 10.1080/09747338.2014.921415
17. Kobayashi, M., Okabe, T., Sato, Y. (2009). Detecting Video Forgeries Based on Noise Characteristics. In: Wada, T., Huang, F., Lin, S. (eds) Advances in Image and Video Technology. PSIVT 2009. Lecture Notes in Computer Science, vol 5414. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-92957-427.
18. Redi, J., Taktak, W., Dugelay, J. (2010). Digital image forensics: a booklet for beginners. Multimedia Tools and Applications, 51, 133-162. https://doi.org/10.1007/s11042-010-0620-1.
19. Ding, W., Xie, Y., Wang, Y. (2019). Image authentication and tamper localization based on relative difference between DCT coefficient and its estimated value. Multimedia Tools and Applications, 78, 5305-5328. https://doi.org/10.1007/s11042-018-5732-z.
20. Tzeng, C., Tsai, W. (2001). A new technique for authentication of image/video for multimedia applications.

, 23-26. https://doi.org/10.1145/1232454.1232464.
21. Han, S., Chu, C. (2009). Content-based image authentication: current status, issues, and challenges. International Journal of Information Security, 9, 19-32. https://doi.org/10.1007/s10207-009-0093-2.
22. Han, S., Chu, C., Yang, S. (2007). Content-based image authentication: current status, issues, and challenges. International Journal of Informa- tion Security, 9, 19-32. https://doi.org/10.1007/s10207-009-0093-2.
23. Debnath, S., Ramalakshmi, K., Senbagavalli, M. (2022). Multimodal Authentication System based on Audio-Visual data: A Review. 2022 International Conference for Advancement in Technology (ICONAT), 1-5. https://doi.org/10.1109/ICONAT53423.2022.9725889.
24. Queluz, T. (2001). Authentication of digital images and video: Generic models and a new contribution. Signal Process. Image Commun., 16, 461-475. https://doi.org/10.1016/S0923-5965(00)00010-2.
25. Mohan, J., Rajesh, R. (2020). ENHANCING home security through visual CRYPTOGRAPHY. Microprocess. Microsystems, 80, 103355. https://doi.org/10.1016/j.micpro.2020.103355.