Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 07, July : 2022

IMAGE AND VIDEO FORENSICS FOR DETECTING FORGERY AND TEMPERED MEDIA

Raj Kewlani

Assistant Professor

Electronics & Communication Engineering

Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Prachi Goyal

Assistant Professor

Computer Science Engineering

Arya Institute of Engineering and Technology, Jaipur, Rajasthan

Raghav Vijay

Science Student

Apex Sr. Sec. School, Baran, Rajasthan

Rudhra Pratap Singh Naruka

Science Student

B.S.N Academy Sr. Sec. School, Kota, Rajasthan

Abstract:

Thanks to technical improvements in different video and photo processing tools, digital video may now be manipulated rapidly and efficiently. This review focuses on passive techniques for spotting fake digital videos. Instead of employing pre-embedded data, passive forgery detection techniques may be used to assess a video's authenticity. The techniques for detecting forgeries make use of statistical or mathematical properties that are altered as a result of video manipulation. The passive video forgery detection approach has great promise for pattern recognition, information security, and multimedia security. The methodologies used for passive video forensics are divided into three categories in this study: statistical video feature correlation, frame-based statistical anomaly

http://doi.org/10.36893/IEJ.2022.V51I7.016-021

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 07, July : 2022

detection, and inconsistent features of different digital devices. The discussion also covers trends and limits, as well as ideas for enhancing passive forgery detection methods.

The current state of image and video forensics, as well as its applications and datasets, are all critically examined in this paper using a thorough, in-depth, and methodical approach. By emphasizing the issues in the field of image and video forensics that will receive attention in the future, the survey also provides future directions for academics by giving them ideas for future research topics. An extensive literature review and comparative analysis are part of the survey.

Keywords:

Copy-move forgery detection (CMFD), image forgery detection, video forgery detection, deep learning-based forgery detection, machine learning-based forgery detection, forensic analysis of images and videos, digital image forensics, digital video forensics

I. Introduction:

As imaging technology progresses, digital images are developing into tangible information sources thanks to improvements in imaging technology. In the meantime, a wide range of image manipulation technologies have jeopardized the authenticity of photographs. The goal of visual content forgeries is to carry out the modifications in a manner that makes them difficult to see with the unaided eye and then exploit these products for evil.

In the context of the current, larger conversation about fake news, we examine the phenomena of "deepfakes," a revolutionary technology that allows for the low-cost alteration of video content through the use of artificial intelligence. We explore technical countermeasures and talk about the history and current advancements of the technology, along with how it differs from previous manipulation methods. Although there has been much talk in recent years about the threat posed by deepfake films with significant political ramifications, the technology has had little effect on politics thus far. We look into the causes of this and predict the kinds of deepfake films that we might see in the future.

the two main techniques used to modify images are region duplication by copy-move forgeries and image splicing. Image splicing is the process of combining portions of different photographs to produce a fabricated image. To hide or amplify certain crucial content in the portrayed image, copy-move forgery, on the other hand, involves copying and pasting image portions onto the same image. It becomes difficult to distinguish the tempered sections from legitimate parts because replicated regions appear to be identical with suitable components (such as color and noise). Additionally, to hide the visual signs of image forgeries, counterfeiters use various postprocessing techniques like blurring, edge smoothing, and noise. The below figure depicts a copy move forgery instance.

http://doi.org/10.36893/IEJ.2022.V51I7.016-021

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 07, July : 2022

Figure-1. The original image

Figure-2. The copy-move forged images

The image is made with a watermark or digital signature incorporated as opposed to the passive technique. The use of these embeddings allows for later analysis to determine whether or not the image has been altered.

Any pre-embedded information, such as a watermark implanted to identify image counterfeiting, cannot be relied upon in the passive technique. Due to the lack of extra information needed to detect image counterfeiting, this method is often referred to as the "blind approach." based on features that are taken straight from the photos, this method is used.

Additionally, there are two variations of the passive strategy: independent and dependent. Resampling and compression forgeries are caught by the independent technique while splicing and copy/move forgeries are caught by the dependent approach.

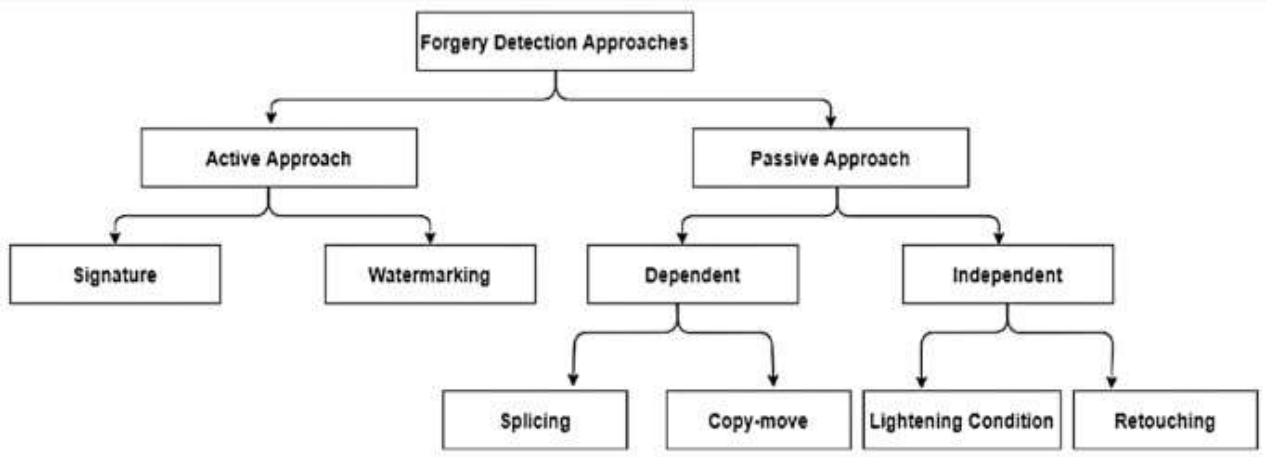

Figure 3. Energy detection approaches

http://doi.org/10.36893/IEJ.2022.V51I7.016-021

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 07, July : 2022

Digital video data is subject to authenticity, integrity, and identity checks in addition to being used in social media. Authenticity is the capacity to assess if the evidence is reliable, whereas integrity guarantees that video evidence has not been manipulated before seizure.

Digital video processing has become simpler and faster because to technological advancements in a variety of video and image processing technologies. For the purpose of forgery detection, the techniques take advantage of statistical or mathematical aspects that are affected by video tampering. The identification of fake videos using a passive method has several applications in pattern recognition, information security, and multimedia security.

Copy-move tampering is the most basic kind of video falsification that is visible to the naked eye. Since more sophisticated procedures are required to detect a fabricated movie, video falsifying is a more sophisticated form of video forgery than copy-move. Editing, merging, or producing new video content might make it more difficult to detect video faking attacks since the bogus videos change the semantic meaning of the original videos.

Among the multimedia that is most commonly used in daily life are digital videos. Social networking services like facebook, instagram, whatsapp, youtube, and others are popular channels for the online transfer of these. Modifying the content of digital videos has been made easier by the availability of contemporary, user-friendly editing software. As such, the validity, reliability, and authenticity of these digital recordings have become critical concerns. Determining the film's alterations and verifying its legitimacy are the goals of digital video forgery detection. Both passive and aggressive strategies can be used with these. There has been a thorough analysis of passive methods for detecting video forgeries.

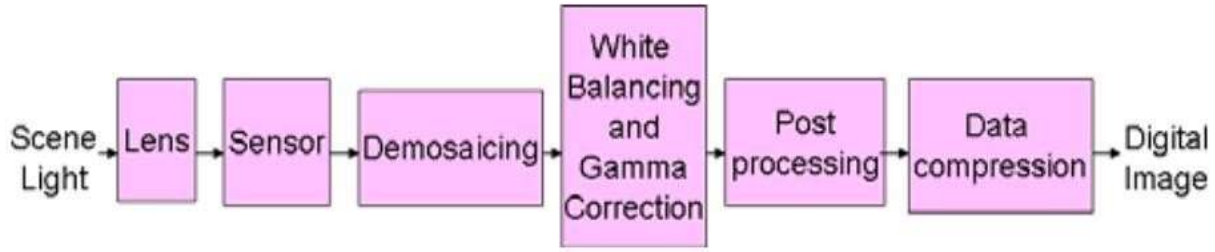

Figure 4. Detection of video forgeries

This survey aims to investigate and evaluate the current methods for passively detecting video forgeries. The basic knowledge needed to comprehend video forgery detection is first provided. The available passive video forgery detection methods are then briefly examined, with an emphasis on their shortcomings and features, datasets used, and performance factors. Deepfake detection in the video and anti-forensics method are then covered. Subsequently, the generalized architecture for passive video forgery detection approaches and standard benchmark video forgery datasets are explored.

II. Conclusion:

http://doi.org/10.36893/IEJ.2022.V51I7.016-021

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 51, Issue 07, July : 2022

In order to overcome challenges imposed by the wide availability of fake and altered material, image and video forensics are crucial. A combination of conventional techniques and recent developments in deep learning and blockchain technology present intriguing ways to identify altered multimedia content and stop it from spreading. To remain ahead of emerging risks in the constantly changing field of manipulating digital media, continued study and interdisciplinary collaboration are crucial.

III. Future scope

Deep learning advancements: Deep learning techniques will probably need to be further developed and integrated in order to make further progress in image and video forensics. The detection of several kinds of image and video modifications has demonstrated significant promise for convolutional neural networks (CNNS) and recurrent neural networks (RNNS).

Multimodal analysis: future systems will need to provide multimodal analysis as media forgeries get more complex. This entails integrating metadata, audio, and other data with image and video analysis to find anomalies and manipulations.

Generative adversarial networks (GANS): in addition to being used to produce deepfake content, GANS may also be used to identify it. In the future, GANS might be used in forensic instruments to spot minute irregularities or artifacts added during the forgery process.

Blockchain and distributed ledger technology: digital media can have a safe and impenetrable chain of custody established with the aid of distributed ledger technology and blockchain. The integrity and validity of media files can be confirmed with the use of this technology.

Quantum computing challenges: the development of quantum computing may pose a threat to encryption techniques. In order to ensure the authenticity of digital media in the post-quantum computing age, future advancements might entail creating quantum-resistant digital forensics methods.

Advancements in steganography and watermarking: better watermarking and steganography methods will be developed continuously to conceal information in digital material as forgers grow more skilled. These developments will mean that forensic instruments must also evolve.

Collaboration and opensource tools: researchers, organizations, and governments will probably work together more in the future to create open-source databases and tools for forgery detection. Remaining ahead of counterfeiters will require sharing resources and expertise.

Education and training: law enforcement, forensic specialists, and the general public will receive more education on the dangers and identification of fake media. Public awareness campaigns and training initiatives will become increasingly important.

Reference:

1) T.-t. Ng, s.-f. Chang, c.-y. Lin, and q. Sun, "passive-blind image forensics", in multimedia security technologies for digital rights, w. Zeng, h. Yu, and c.-y. Lin (eds.), Elsevier, 2006.

http://doi.org/10.36893/IEJ.2022.V51I7.016-021

2) Swaminathan, m. Wu, and k. J. R. Liu, "digital image forensics via intrinsic fingerprints," IEEE trans. Information forensics and security, vol.3, no.1, pp.101-117, mar. 2008.
3) A.c. popescu and h. Farid, "exposing digital forgeries in color filter array interpolated images," IEEE trans. Signal Process., vol. 53, no.10, pp. 3948-3959, oct. 2005.
4) s. Bayram, h. T. Sencar, and n. Memon, "source camera identification based on CFA interpolation," in Proc. IEEE int. Conf. Image processing, vol.3, no., pp. Iii-69-72, 11-14, Sept. 2006.
5) y.-f. Hsu and s.-f. Chang, "Image splicing detection using camera response function consistency and automatic segmentation," in proc. IEEE conf. Multimedia expo., pp. 28-31, July 2007, Beijing, China.
6) J. Lukáš, j. Fridrich, and m. Goljan, "digital camera identification from sensor pattern noise," IEEE trans. Information forensics security, vol.1, no.2, pp. 205-214, June 2006.
7) J. Lukáš, j. Fridrich, and m. Goljan, "detecting digital image forgeries using sensor pattern noise," in Proc. Spie electronic imaging, photonics west, pp. 60720y-1-11, Jan. 2006.
8) M. Chen, j. Fridrich, and j. Lukáš, "determining image origin and integrity using sensor pattern noise," IEEE trans. Information forensics security, vol.3, no.1, pp. 74-90, mar. 2008.
9) S. Ye, q. Sun and e.-c. Chang, detecting digital image forgeries by measuring inconsistency of blocking artifact, July 2007, Beijing, China.
10) A.c. popescu and h. Farid, "Exposing digital forgeries by detecting traces of re-sampling," IEEE trans. Signal Process., vol. 53, no.2, pp. 758-767, Feb. 2005.
11) q. Shi, c. Chen, and w. Chen, "a natural image model approach to splicing detection," in proc. Acm multimedia security workshop, pp. 51-62, sept. 2007, Dallas, Texas.
12) Fan and r. L. De Queiroz, "Identification of bitmap compression history: jpeg detection and quantizer estimation," IEEE Trans. Image Process., vol. 12, no. 2, pp. 230-235, Feb. 2003.
13) K. A. Patwardhan, g. Sapiro, and m. Bertalmio, "video inpainting under constrained camera motion," ie trans. Image Process., vol.16, no. 2, pp. 545-553, Feb. 2007
14) A. Criminisi, p perez, and k. Toyama, "region filling and object removal by exemplar-based image inpainting," in trans. Image Process., vol.13, no.9, pp. 1200-1212, Sept. 2004.
15) Simiran Kuwera, Sunil Agarwal and Rajkumar Kaushik, "Application of Optimization Techniques for Optimal Capacitor Placement and Sizing in Distribution System: A Review", International Journal of Engineering Trends and Applications (IJETA), vol. 8, no. 5, Sep-Oct 2021.
16) Guru Saran Chayal, Bharat Bhushan Jain and Rajkumar Kaushik, "A Detailed Study of Electrical Vehicle with Improved Applications: A Review", International Journal of Engineering Trends and Applications (IJETA), vol. 8, no. 6, pp. 31, Nov-Dec 2021.
17) T. Manglani, A. Vaishnav, A. S. Solanki and R. Kaushik, "Smart Agriculture Monitoring System Using Internet of Things (IoT)," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 501-505.

http://doi.org/10.36893/IEJ.2022.V51I7.016-021