Received: 9 May. 2023 | Revised: 20 May. 2023 | Accepted: 12 Jun. 2023 | Published online: 26 Jun. 2023

RESEARCH ARTICLE

Contemporary Education and Teaching Research
2023, Vol. 4(6)278-282
DOI: 10.47852/bonviewCETR232011480604

BON VIEW PUBLISHING

A Study on the Application of Deep Learning-based Media Tampering Detection Technology in Higher Education Teaching Resource Protection

Tao Luan[1,*]**& Maria Amelia E. Damian**[2]
[1]*Graduate School, University of the East，Philippines*
[2]*Faculty College of Engineering University of the East,　Philippines*

Abstract: With the rapid development of digital technology, the problem of media tampering has become increasingly serious, and higher education teaching resources are facing a crisis from image tampering and sound tampering to video tampering and even deep forgery, which brings great challenges to education work. Through deep learning, tampering can be automatically detected and self-learning and optimized in the process of detection, so that it can remain efficient and accurate in the face of new tampering techniques. The purpose of this paper is to discuss in detail the application of deep learning in media tampering detection and to explore its application in the protection of higher education teaching resources.

Keywords: deep learning; tampering detection; higher education; resource protection

Introduction

Media tampering can be used to create false information and events by tampering with individuals' photos, videos, or voices to commit aggression, defamation, or extortion against individuals. In addition, doctored media content may be used to spread rumors, incite hatred, or create social disorder. Such information tampering and misuse can easily lead to social unrest, crowd panic, and public safety incidents, causing serious damage to social order and public safety. Therefore, the development of effective media tampering detection technologies and protection measures is crucial to ensure public access to truthful and credible information, protect personal privacy and reputation, and maintain social stability and security, as well as strengthen the public's media literacy and recognition ability, increase vigilance against tampered media, and jointly build a healthy, safe, and credible media environment.

1. Overview of media tampering detection technology based on deep learning

Deep learning-based media tampering detection technology is an advanced detection technology using artificial intelligence, which has achieved remarkable success in the field of image and video analysis to detect and prevent media content tampering. The basic principle of deep learning is to mimic the way the human brain processes information by building neural networks, by which machines can learn and extract valuable information from large amounts of data. In the application of media tampering detection, deep learning is mainly used to identify possible inconsistencies or anomalies in media content, such as unnatural edges in images, color discontinuities, unreasonable lighting illumination, etc., and then identify possible tampered areas. Deep learning-based media tampering detection technology has a variety of specific application methods, such as convolutional neural networks (CNNs), which can extract key features from images and distinguish normal and abnormal patterns through self-learning and

Corresponding Author: Tao Luan
Graduate School, University of the East，Philippines
Email:luantao319@gmail.com

self-optimization, and are therefore very suitable for image recognition and analysis; generative adversarial networks (GANs) can generate and recognize fake images and thus is also often used in media tampering detection. The advantages of deep learning-based media tampering detection techniques are mainly reflected in their high accuracy and automation. Since deep learning techniques can learn complex laws and patterns from a large amount of training data, detection results are usually more accurate than traditional methods, and the whole detection process can be completely automated by machines, thus improving detection efficiency and reducing the need for human involvement (Zhu et al., 2021).

2. The problem of media tampering in the protection of higher education teaching resources

2.1The impact of media tampering on higher education teaching resources

Media tampering not only destroys the integrity of teaching resources, but also negatively affects the learning process of students, and may even cause doubts about the fairness and credibility of the whole higher education system (Lv et al., 2022). With the development of technology and the promotion of digital teaching, higher education institutions have started to widely use various types of teaching resources, such as video lectures, online courses, and teaching software. However, media tampering may change the original teaching content in an undetectable way. Assuming that key steps in an instructional video are tampered with or deleted, students may not understand the course content correctly as a result, thus affecting learning outcomes, and if such tampering is intentional, students may be misled to receive the wrong information. If test materials or videos of instructional assessments are tampered with, then this may cause injustice to the grading process and may even raise questions about the impartiality of the school. Once students or staff discover tampering with instructional resources, they may have doubts about the credibility of the school, which will have a long-term negative impact on the reputation of the school. Media tampering may also have an impact on the communication and sharing of higher education teaching resources. In the current educational environment, the communication and sharing of teaching resources can help teachers make teaching innovations and provide more learning opportunities to students. If there is a risk of tampering with teaching resources, students may have a distrust of the shared resources as a result, which will hinder the communication and utilization of teaching resources.

2.2 Types of media tampering faced by higher vocational teaching resources

In the current digital era, higher education teaching resources may face various types of media tampering. The diversity of tampering types mainly stems from the advancement of modern technology and the technical proficiency and intention of tamperers, and the importance of identifying and understanding these tampering types cannot be overstated (Zhang et al., 2023). Image tampering can occur on any type of image resource, including still images, diagrams, or even a frame in a video, and includes adding, removing, or altering a part of an image to change the information it conveys. For example, a chart in an instructional PPT is tampered with, changing the display of data and communicating the wrong data to the viewer. In addition to image tampering, media tampering can also imitate anyone's voice or change the content of the original recording through sound synthesis techniques, which is particularly dangerous for instructional resources that contain speech, such as audio lectures or video courses. Video tampering is a more complex type of tampering, covering image tampering and sound tampering, and may also include timeline tampering. For example, the tamperer may delete a segment of the video or rearrange the playback order of the video to mislead the viewer. Video tutorials and live online courses require higher content coherence and integrity, so video tampering has a more serious impact on such teaching resources.

3. Application of media tampering detection technology based on deep learning in the protection of higher education teaching resources

3.1 Data set construction and Preparation

To effectively respond to the real media tampering incidents faced by higher education institutions, a real, diverse, and representative dataset needs to be established. The construction of the dataset needs to consider the sources and types of data collected. Higher education teaching resources include various types of courseware, teaching videos, lab reports, etc. Therefore, the dataset should cover these different types of teaching resources (Liu & Xu , 2022). To obtain real samples of media tampering events, real events that have occurred in higher education institutions and involve different subject areas need to be collected as the basis of the dataset to ensure diversity and representativeness of the dataset. For each teaching resource, the original version with authenticity and integrity without any tampering or modification needs to be collected as the benchmark, and the corresponding post-tampering version, i.e., the version containing various types and degrees of tampering operations, also needs to be collected to provide a basis for learning and discrimination for the deep learning model by comparing and analyzing the differences between the original version and the post-tampering version. To determine the information about the location, type, and degree of tampering, the collected data need to be annotated and annotated with the region of tampering in images and videos, the location of text tampering, the part of the content modification, etc., to provide the deep learning model with key features and patterns about tampering and to improve the accuracy and robustness of the detection algorithm, and the annotation can also include information about the means of tampering, the motive of tampering and the impact on teaching resources The annotations can also include relevant information about the means of tampering, the motivation of tampering, and the impact on instructional resources for further research and analysis. Preprocessing and enhancement of the dataset are to improve the diversity and robustness of the dataset. Preprocessing includes operations such as resizing, color space conversion, and denoising of images and videos to ensure the consistency and comparability of the data, increasing the diversity of the data by rotating, flipping, and cropping, and improving the generalization ability of the model to enhance the data. In addition, methods such as fuzzing and adding noise can be used to simulate uncertainties and disturbances in real scenes to enhance the model's adaptability to noise and changes (Zhang et al., 2022).

3.2 Design and training of deep learning models

The design of the model needs to be solved based on the type of media tampering, and for image and video tampering detection tasks, convolutional neural networks (CNN) can be used as the base model to capture local and global features of images and videos, and to better understand and analyze the tampering behavior, spatiotemporal information modeling can be introduced, such as using techniques such as spatiotemporal convolutional neural networks (3D-CNN) or optical flow estimation (Zhu, Xu , et al., 2022). The structure of the model should include two main parts, feature extraction and classification, and multi-layer convolution and pooling layers are used in the feature extraction phase to gradually extract abstract features of images and videos, adding techniques such as batch normalization and residual connectivity to accelerate the training process and improve model performance; the classification phase should use fully connected layers or other classifiers to map the extracted features to different tampering classes and perform classification judgment. Prepare labeled and annotated datasets containing tampered and non-tampered samples and corresponding label information for the training of deep learning models, and train and evaluate the models by dividing the training set, validation set, and test set. Gradient descent-based optimization algorithms, such as stochastic gradient descent (SGD) or Adam optimizer, are used during the training process to minimize the loss function and update the parameters of the model, and data enhancement techniques, such as random rotation, flipping, and cropping, are employed to increase the diversity of data and improve the generalization ability of the model. Overfitting and underfitting of the model are also problems that need to be addressed in model training; overfitting can be done by adding regularization terms, such as L1 or L2 regularization, or using dropout techniques to reduce the complexity of the model and improving the generalization ability, and underfitting can be solved by increasing the capacity of the model or adjusting the hyperparameters (Zhu, Tang, et al., 2022). In addition, to improve the performance of the model, pre-trained models, and migration learning techniques can be used. Pre-training models can be pre-trained using large-scale datasets and then fine-tuned on the target task. Migratory learning, on the other hand, applies the model obtained by training on one task to another related task to speed up the training process and improve the accuracy of the model.

3.3 Deployment and application of media tampering detection system

System deployment requires selecting appropriate computing devices, such as high-performance servers and GPU gas pedals, according to the task and scale of media tampering detection, and configuring the corresponding software environment, including deep learning frameworks, image, and video processing libraries, etc., to support the operation and inference of the models (Tian et al., 2021). After that, the trained deep learning models are loaded into the system for real-time tampering detection, either by using model compression and optimization techniques to reduce the computational and storage overhead of the models and improve the efficiency and performance of the system, or by using distributed deployment to distribute the models to multiple computing nodes to handle large-scale data and requests. Web interfaces or mobile applications should be designed in the media tampering detection system to enable users to upload, process, and view the tampering detection results of teaching resources, and the system should also be integrated with other teaching resource management systems or platforms to achieve seamless workflow and data interaction. The system application is customized for the actual needs of higher education institutions (Hu et al., 2021). For example, corresponding tampering detection algorithms and rules are customized according to the characteristics and needs of different subject areas, and combined with other technical means, such as watermarking technology and digital signature, to increase the protection and traceability of teaching resources. Meanwhile, through interaction with teachers and students, the system's performance and user experience are continuously optimized to improve the effectiveness and accuracy of media tampering detection. The media tampering detection system also needs to ensure security in the process of data transmission and storage, adopt measures such as encryption and permission control to prevent leakage and tampering of sensitive data, and for data involving personal privacy, such as teachers' and students' information, it needs to comply with relevant laws and regulations and privacy policies to protect users' privacy rights (Li et al., 2015).

4. Conclusion

In the modern digital environment, the problem of media tampering has become a norm. To protect the integrity and authenticity of higher education teaching resources, advanced technologies, such as deep learning, are needed to combat this situation, which can not only effectively detect and prevent media tampering, but also enhance teachers' and students' awareness of media tampering, thus achieving the goal of comprehensive protection of higher education teaching resources. However, the problem of media tampering is still complex and challenging and needs further research and improvement. It is recommended to strengthen the protection strategies and measures for higher education teaching resources, combine other technical means such as watermarking technology and digital signatures to improve the effectiveness and reliability of media tampering detection, enhance the public's media literacy and recognition ability, and jointly build a healthy, safe and trustworthy media environment.

Conflict of Interest

The authors declare that they have no conflicts of interest to this work.

References

Zhu, X. T., Tang, Y. Q., & Geng, P. C. (2022). A review of digital image tampering detection techniques. *Journal of the Chinese People's Public Security University (Natural Science Edition)*, *28*(04), 87–99.

Lv, J., Lu , W., Wang, M., Liu, Y., Shi, K., Huang, H., & Zhao, H. (2022). Image stitching tampering detection based on multi-scale feature prior. *China Science and Technology Paper*, *17*(11), 1267–1275.

Zhang, J., Wang, H., & He, P. (2023). Transformer-based multi-task image stitching tampering detection algorithm. *Computer Science*, *50*(01), 114–122.

Liu , Y., & Xu , S. (2022). A review of digital image tampering localization research. *Journal of Beijing Institute of Electronic Science and Technology*, *30*(03), 41–54.

Zhang, Y., Zhao , X., & Cao , Q. (2022). A review of blind detection of digital image tampering. *Journal of Information Security*, *07*(03), 56–90.

Zhu, K., Xu , W., Lu , W., & Zhao, X. (2022). Multi-keyframe feature interaction for face tampering video detection. *Chinese Journal of Graphics*, *27*(01), 188–202.

Zhu, X., Tang , Y., & Geng, P. (2021). Feature fusion-based algorithms for tampering and deep forgery image detection. *Information Network Security*, *21*(08).70-81.

Tian, X., Li , H., Zhang , Q., & Zhou , A. (2021). A two-channel R-FCN-based image tampering detection model. *Journal of Computer Science*, *44*(02), 370–383.

Hu, Y., Gao, Y., Liu , C., & Liao, G. (2021). Deep vacation face video tampering detection based on image segmentation network. *Journal of Electronics and Information*, *43*(01), 162–170.

Li, Y., Liu , N., Zhang, B., & Yang, Y. (2015). FI-SURF algorithm in image mirror copy-paste tampering detection. *Journal of Communication*, *36*(05), 58–69.

How to Cite: Luan, T., & Damian, M. A. E. (2023). A Study on the Application of Deep Learning-based Media Tampering Detection Technology in Higher Education Teaching Resource Protection. *Contemporary Education and Teaching Research,* 04(06), 278-282. https://doi.org/10.47852/bonviewCETR232011480604