China Petroleum Processing and Petrochemical Technology

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

A COMPREHENSIVE STUDY OF DATA FORGERY TECHNIQUES FOR VIDEO FORGERY DETECTION WITH CHALLENGES AND FUTURE DIRECTION

Mr. Hemant A. Tirmare
Ph.D. Scholar CSE DYP ATU Talsande, Kolhapur, Assistant Professor, Department of Technology, Shivaji University, Kolhapur, India, hat_tech@unishivaji.ac.in

Dr. Jaydeep B. Patil
Ph.D. Guide & Asso. Dean Academics Engg. & Technology, School of Engineering and Technology, D.Y.Patil Agriculture and Technical, University, Talsande, Kolhapur, India, jaydeeppatil@dyp-atu.org

Dr. Sangram T. Patil
Associate Dean CSE, School of Engineering and Technology, D.Y.Patil Agriculture and Technical, University Talsande, Kolhapur, India, sangrampatil@dyp-atu.org

***Corresponding Author: Mr. Hemant A. Tirmare**
*Ph.D. Scholar CSE DYP ATU Talsande, Kolhapur, Assistant Professor, Department of Technology, Shivaji University, Kolhapur, India, hat_tech@unishivaji.ac.in

ABSTRACT
The incidence of video forgery on the internet has increased in recent years, corresponding with the spread of malicious software, which has aided the seamless uploading, downloading, and sharing of various digital objects such as audio, photos, and videos. Video Editor and Adobe Photoshop, multimedia software extensively used for modifying and tampering with media files, are prominent among these manipulative tools. Concurrently, video sequence manipulation, involving the addition or deletion of objects within frames, has evolved as a common kind of malicious video counterfeiting. This study goes into the world of video forgery detection, focusing on passive blind techniques and addressing three types of forgery: clone forgery, source camera identification, and splice forgery.
Keywords: forgery, video, machine learning, active passive approaches

INTRODUCTION
The widespread availability of digital video and image editing software has created a huge difficulty in the field of multimedia content authentication. The current landscape of manipulation techniques, combined with the dynamic evolution of multimedia technology, has lowered the threshold for even the most inexperienced user to effortlessly remove objects from video sequences, incorporate elements from disparate video sources, or insert objects generated by graphic design software. As a result, differentiating between an original, unedited video and one that has been tampered with has become a difficult task. This complexity arises from the multitude

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

of forgery methods accessible to the general public, resulting in a substantial hurdle in the realm of video processing [1, 2].

In recent times, the domain of blind digital video forgery detection has emerged as a pivotal avenue for establishing the credibility of digital video content. This subject has garnered notable attention within the research community, owing to its significance and relevance.

Based on their methodology, video forgery is divided into two categories: active approaches and passive-blind approaches. The former category includes approaches involving the inclusion of invisible data prior to identification, which necessitates the pre-embedding of features such as watermarks, fingerprints, or digital signatures into images. These elements are subsequently detected through integrity checks of the pre-embedded data [3-6]. Conversely, the latter approach, more suitable for scenarios involving video, photo images, or audio, holds particular relevance [7].

A broader taxonomy of passive-blind techniques includes three primary categories [8, 9]: splicing, source identification, and copy-move forgery detection. These techniques prove valuable for detecting various forms of digital video manipulation, including instances of double compression, such as those seen in MPEG or H.264 formats. Evidently, a plethora of research has been dedicated to detecting digital video tampering, a testament to the significance of these methods [10-15].

These passive approaches effectively address conventional forgery operations, offering a valuable toolset for determining the authenticity of digital videos. They leverage techniques like video object detection, video double compression analysis, identification of duplicated regions within video frames, as well as frame-based tampering detection and identification of images subjected to double JPEG compression. The multifaceted nature of these methods collectively contributes to enhancing the accuracy and reliability of determining the legitimacy of digital video content.

Figure 1: Forged and original Image Sequence

Figure 1 illustrates the utilization of a replicated sequence of video frames to obscure or imitate a particular event [71]. To elucidate, consider a scenario where an individual is captured in a video via a camera. If a segment of the video encompassing the some parts intentionally added, an alternate sub-sequence frame can be duplicated and repositioned to mask the excised portion.

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

Detecting such a form of video forgery proves to be an intricate endeavour, particularly if the copy-move process is meticulously executed. This underscores the critical significance of video forgery detection, as it plays a pivotal role in unveiling instances where the visual integrity of video content has been compromised [16, 17].

This study conducts a comprehensive review of existing literature pertaining to video forgery detection, with a specific emphasis on passive blind approaches. The primary focus lies in exploring the detection methodologies that effectively identify instances of cloning forgery, source camera identification, and splice forgery. Notably, this study presents a novel video authentication system capable of detecting and characterising region and frame duplication as significant markers of video fabrication. Furthermore, this technique seeks to uncover and analyse the underlying elements that influence video forgery perpetration.

To achieve these objectives, the study adopts a meticulous video processing technique, involving the segmentation of videos into distinct sub-blocks. Subsequently, geometric features inherent to each macro-block are extracted and analyzed. This meticulous feature extraction process significantly contributes to the heightened precision and accuracy of forgery detection. Furthermore, the study undertakes a systematic investigation into optimizing the sorting algorithm, resulting in a streamlined computational process. This optimization takes into account crucial factors, including the number of blocks and the quantity of extracted features.

FRAMEWORK OVERVIEW IN VIDEO FORGERY DETECTION

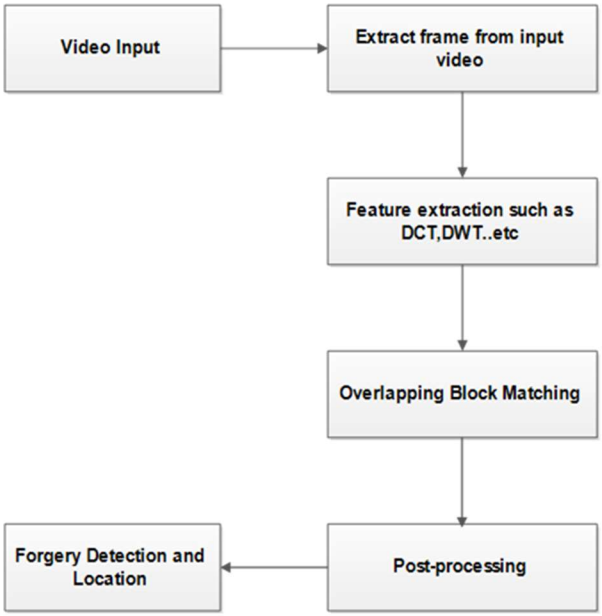

Figure 2: General Detection Method

Digital Image Forensics vs. Video Forgery Detection

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

While several studies [40-47] have been conducted on digital image forensics, research on digital video forgery detection has been very limited. Copy-move forgery appears as a popular tampering technique in the domain of video forgery. Detecting forged regions or frames in this scenario presents a distinct problem due to potential differences in the tampered content's size and compression rate. Methods for detecting video forgeries largely rely on distinguishing both the spatial and temporal features of copy-move manipulation.

General Detection Methodology

Figure 2 depicts a basic detection strategy that includes crucial stages such as frame extraction from the source video, feature extraction, overlapping block matching, and the final determination of the presence of forgery. This adaptable method supports numerous extraction techniques such as DCT, DWT, and PCA while also supporting the use of various matching methods such as K-SVD tree and radix sort [39].

Another significant research, Xiaoling [35], using Compressing Sensing Theory to present a unique approach that combines content authentication and tamper detection utilising a semi-fragile watermark hidden inside DCT coefficients. This technology was used to MPEG-2 compressed films, enabling for content authentication and tamper detection within inner I-frames and P-frames. The results showed that the Semi-fragile Watermarking method performed exceptionally well in terms of effectiveness and accuracy.

Wang et al. [36] developed a strategy to detect frame duplication using both temporal and spatial correlation in a related study. However, when working with small forged sections, this approach encountered accuracy difficulties. Another study [37] devised a solution customised to two specific attack types: 1) spatial (pixel) copy-move attack identified by Histogram of Oriented Gradients (HOG), and 2) temporal copy-move attack detected via MPEG-2 GOP structure.

Wang and Farid [38] also presented a separate video tampering detection approach based on the detection of duplicate frames. This technique takes advantage of the presence of unique static and temporal statistical abnormalities in a sequence of doubly compressed MPEG video frames. These irregularities serve as indicators of tampering, similar to the original MPEG compression approach, in which frames are edited and saved as a twice compressed MPEG movie.

Hsu et al. [40] presented a video splicing method that uses noise residue correlation to identify forged frame patches within a film. The basic concept of this approach is the modification of noise residue correlation caused by tampered frames, which distinguishes them from untampered parts. Despite its vulnerability to noise quantization, experimental results revealed the dependability of noise correlation as a feature, particularly in high-quality movies. However, noise residue extraction is a complex operation that involves both spatial (intra-frame) and temporal (inter-frame) forgery detection. In the former, entire videos are utilised as a reference, while inter-frame frames are used to detect tampering.

A unique technique based on Tamura texture features and algorithms was also proposed. The method computes disparities between the Tamura texture feature vector and adjacent vector matrices using the vector matrix of the movie obtained from video frame extraction. If the

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

disparities are less than a certain threshold, their distances are compared to the threshold. To determine the location of copy-move sequences, pairs of serial numbers that exceed the distance threshold are logged.

Davarzani et al. [41] presented an efficient technique for copy-move forgery detection using Multiresolution Local Binary Patterns (MLBP) in another related paper. This approach performs well even when subjected to rotation, scaling, JPEG compression, blurring, and noise addition. To discover duplicated parts and retain robustness against a range of changes, the image is separated into blocks, each of which is exposed to LBP and the RANSAC algorithm.

Table 1: Method and approach with key finding

Reference	Detection Method and Approach	Key Findings and Contributions
[35]	Semi-fragile Watermarking with Compressing Sensing Theory	Authentication and tamper detection using DCT-based watermarking in MPEG-2 compressed videos
[36]	Temporal and Spatial Correlation for Frames Duplication	Detection of frames duplication with temporal and spatial correlation; limitations in small forged areas
[37]	HOG for Spatial Copy-Move, Exploitation of MPEG-2 GOP Structure	Detection of spatial and temporal copy-move attacks using HOG and MPEG-2 GOP structure
[38]	Duplicate Frame Detection using Doubly Compressed	Detection of duplicate frames using doubly compressed
	MPEG Video Frames Sequence	MPEG video frames sequence
[39]	Noise Correlation for Forged Frame Detection	Detection of tampered frame regions based on noise residue correlation
[40]	Tamura Texture Features for Copy-Move Detection	Copy-move detection using Tamura texture features
[41]	Multiresolution Local Binary Patterns for Copy-Move	Efficient copy-move detection using MLBP and RANSAC
	Forgery Detection	algorithm across various manipulations

TYPES OF FORGERY

Active Approaches to Video Tampering Detection:

Based on the usage of watermarks and digital signatures, active video forgery detection systems are divided into two categories [44]. To identify faked films, these approaches use fragile and semi-fragile watermarks [45]. Fragile watermarking includes embedding invisible information into the video that changes when the video content is changed, allowing forging detection. Semi-fragile watermarking is less sensitive to modifications, allowing for minor changes while detecting large tampering [46].

Both solutions necessitate the insertion of a watermark during video recording, making them reliant on algorithmic and hardware implementations that may not be generally supported. When tampering happens prior to watermark placement, there is also a constraint.

Passive Approaches to Video Tampering Detection:

Passive solutions for detecting video tampering do not rely on embedded information in videos such as digital watermarks or signatures. These approaches make use of imperceptible traces left by tampering within video frames, which may or may not be visible to the naked eye. While these changes are disguised, they have an effect on the statistical properties of the video frames. These statistical changes cause inconsistencies in many properties such as noise, residues, texture, and optical flow (OF) anomalies. Passive techniques use these disparities to discover anomalies.

Furthermore, forensic professionals must base their judgements on the present seen video when a video requires forensic examination and the source video is unavailable. Active approaches are impractical in such instances, hence passive techniques are the preferable option.

Review of Spatial (Intra-Frame) Video Tampering Detection Techniques

Deep learning, a branch of machine learning based on neural networks, provides a reliable method for extracting problem-specific, complicated, high-dimensional characteristics useful for classification tasks. Several deep learning algorithms have been utilised in the context of spatial video forgery detection, with promising results.

Zampoglou et al. [47] used pre-trained ResNet and GoogLeNet networks, as well as Q4 and Cobalt forensic filters, to detect spatial video counterfeiting. The accuracy was 85.09% and the mean average precision was 93.69% on the Dev1 and Dev2 datasets.

Convolutional Neural Networks (CNNs) were used by Yao et al. [48] to extract complicated high-dimensional features, and successive frame differences were used to reduce temporal redundancy. A max pooling layer was added to reduce computational complexity, and a high-pass filter layer improved residual identification post-tampering. Their method yielded impressive accuracy metrics such as 89.90% forged frame accuracy (FFACC), 98.45% pristine frame accuracy (PFACC), and 94.07% F1 score.

Kono et al. [49] used their generated Inpainting-CDnet2014 and Modification Database datasets to combine a CNN and a recurrent neural network for video forgery detection, yielding an area under curve (AUC) of 0.977 and an equal error rate (EER) of 0.061.

For detection, Avino et al. [50] investigated auto-encoders and recurrent neural networks. The receiver operating curve (ROC) demonstrated the method's performance with a limited set of 10 videos.

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

Kaur et al. [51] proposed a Deep Convolutional Neural Network (DCNN)-based technique for inter-frame forgery detection. The approach displays real application potential by reaching 98% accuracy on REWIND and GRIP datasets.

Aditi et al. [52] developed a spatiotemporal video forgery detection and localization approach using CNNs, successfully distinguishing tampered and authentic frames while training with motion residuals. On the SYSU-OBJFORG dataset, the approach produced equivalent findings. While these algorithms produce high-dimensional features with excellent accuracy, a recurring theme emerges: the requirement for cross-validation and larger data validation to ensure generalisation and robustness.

Reference	Method and Approach	Dataset and Evaluation	Achieved Metrics
[47]	ResNet and GoogLeNet with Forensic Filters	Dev1 and Dev2 datasets	Accuracy: 85.09%, Mean AP: 93.69%
[48]	CNN for Feature Extraction	100 authentic, 100 forged videos	FFACC: 89.90%, PFACC: 98.45%, F1: 94.07%
[49]	CNN and Recurrent Neural Network Combination	Inpainting-CDnet2014, Modification DB	AUC: 0.977, EER: 0.061
[50]	Auto-encoders and Recurrent Neural Network	Limited experiments on 10 videos	ROC-based performance assessment
[51]	Deep Convolutional Neural Network (DCNN)	REWIND and GRIP datasets	Accuracy: 98%, Potential for application
[52]	Spatiotemporal Detection based on CNN	SYSU-OBJFORG dataset	Comparable results, need for cross-validation

Exploring Approaches Based on Pixel and Texture Features:

The pixel, a fundamental unit, is at the heart of every image frame. RGB (Red-Green-Blue), YCbCr (with luminance Y and chroma components Cb and Cr), HSI (Hue-Saturation-Intensity), and CMY (Cyan-Magenta-Yellow) are several colour representation formats used in images. These models allow for the mathematical derivation of several properties such as colour, gamma, intensity, and contrast. Multiple pixel-based features, such as HOG (Histogram of Oriented Gradients) and LBP (Local Binary Pattern), can be computed using these colour models to detect passive forgery [52].

Subramanyam et al. [41] investigated compression characteristics and HOG to detect spatial counterfeiting. 6000 frames from 15 different videos were analysed for spatial manipulation using their methods. In parallel, 150 GOPs (Groups of Pictures) of 12 frames each were used to detect temporal forgeries. The original movie was compressed at 9 Mbps using the MPEG-2 video codec and then spatially manipulated by copying and pasting sections of varied dimensions (40 40, 60 60, and 80 80 pixels) within and across frames. The detection accuracy (DA) for 40 40, 60 60, and 80 80 pixels was notable, reaching 80%, 94%, and 89%, respectively. While this technique demonstrated improved spatial forgery detection accuracy, it is important to note that the model was trained and tested on a relatively limited dataset. Importantly, this method has drawbacks,

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

such as failing to detect forgery when post-processing procedures such as scale and rotation were applied to tampered regions, as well as failing to localise the fabricated regions.

Meanwhile, Al-Sanjary et al. [107] investigated optical flow inconsistency to detect and localise instances of copy-move forgeries. In this study, nine movies were used to evaluate the technique's performance, yielding a 96% accuracy rate. However, it should be noted that the method's efficiency decreases when used to high-resolution videos, offering a constraint.

Method	Key Concepts and Features	Evaluation	Achieved Metrics	Limitations
Pixel-based and Texture Features Inconsistency	Various color models (e.g., RGB, YCbCr, HSI, CMY), Derived features (HOG, LBP), Subramanyam et al. [41]	6000 frames from 15 videos for spatial forgery, 150 GOPs of 12 frames each for temporal forgery accuracy achieved	DA: 40x40 pixels - 80%, 60x60 pixels - 94%, 80x80 pixels - 89%	Detection limitations after post-processing like scaling and rotation. Inability to localize forged regions. videos.

Review of Temporal (Inter-Frame) Video Tampering Detection Techniques

Optical flow, which calculates apparent velocities of brightness pattern movement, and motion residuals, which calculate motion in videos, are both critical techniques. Shanableh et al. [13] detected tampering using SVM classifiers and characteristics such as prediction residuals, intra-coded macro-blocks, and quantization scales. Chao et al. [31] used optical flow fluctuations to detect frame insertion and deletion, however they did not do varied compression testing.

Feng et al. [53] proposed a motion residuals-based approach for detecting frame deletion sites, which achieved successful localization but did not take compression ratios into account. Feng et al. [54] created fluctuation characteristics based on motion residuals that detect frame deletion with high accuracy in both speedy and slow-motion films. Kingra et al. [55] suggested a hybrid method integrating optical flow and prediction residuals that performed well for detection and localization of frame tampering but struggled with high illumination.

Jia et al. [56] and Joshi et al. [57] classified authentic and counterfeit films using optical flow for detecting duplicated frames and frame prediction error, respectively. While Joshi et al. achieved an accuracy of 87.5%, its performance is limited to movies less than 7 seconds in length. The summarised approaches show a range of strengths and limitations, from effective tamper detection to issues with certain video qualities and circumstances.

RESEARCH CHALLENGE

Dataset Every recognition system's success is dependent on its training, testing, and assessment methods, which are all dependent on the dataset employed. During these stages, the dataset is

critical to guaranteeing the proper operation of any proposed method. Existing video forgeries datasets, however, have proven insufficient due to their limited size and lack of post-processing procedures such as rotation, scaling, blurring, and compression. Despite the fact that numerous academics have created their own datasets for inter-frame forgery detection tests, these datasets are still inaccessible to other communities and researchers that want to evaluate the effectiveness of their proposed algorithms.

Performance and Evaluation

Because many video forgery techniques are based on camera source identification, their performance degrades as the number of cameras grows. Furthermore, camera source identification algorithms rely significantly on intrinsic camera hardware properties such as lens and charge-coupled device (CCD) sensor characteristics, which might degrade algorithm performance. The presence of video double compression artefacts adds to the difficulty of detecting video forgeries, especially when the analysed video is compressed with a low-quality factor, as seen in the majority of modern approaches.

Similarly, video forgery detection is dependent on post-processing procedures such as edge blurring, compression, noise, scaling, and rotation. These operations can dramatically increase the likelihood of false positives. Unfortunately, most existing video forgery detection algorithms are vulnerable to such post-processing alterations, reducing their performance.

Existing approaches are evaluated using a variety of measures, making direct comparisons impossible. As a result, there is an urgent need for standardised evaluation measures based on factors such as shifting lighting conditions and pixel correlation. Such standardised measurements would allow for smooth comparisons amongst algorithms, allowing for more significant insights into their comparative performance.

Localization

While video forgery detection can provide consumers with information about the validity of a video, improving the credibility of forgery detection systems requires precisely detecting the fabricated segments within the movie. Accurately localising video tampering remains a serious difficulty. Although certain developed algorithms can detect altered portions in a video, their accuracy rates have frequently fallen short. Furthermore, the challenge of locating tampered zones has received little attention in various research. As a result, significant advances in localising remnants of manufactured regions in edited videos have yet to materialise. The difficulty of existing approaches to effectively simulate structural changes caused by spatial forgery in movies has exacerbated the problem, making precisely localising the fabricated region a continuing challenge.

Robustness

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

The ability to detect and localise multiple types of forgery extensively, rather than being limited to certain datasets, is a hallmark of algorithmic resilience. Many described algorithms show great accuracy on narrow evaluation datasets, but their performance does not always translate to a broader context. This makes comparing existing techniques difficult. The insufficient validation against standardised datasets is a key shortcoming of these approaches. As a result, there is an urgent need to create benchmark datasets that cover the detection and localization of all forgeries types in movies with high accuracy. Such benchmarks would be critical for confidently adopting these strategies in real-world applications.

FUTURE DIRECTION

Figure 7 depicts a thorough methodology for identifying and localising video forgeries, with the goal of aiding the research community for algorithm training, testing, and evaluation. There are several stages to the process:

1. Feature Extraction: To extract features, various multi-resolution techniques such as Local Binary Pattern (LBP), Weber's Law Descriptor (WLD) [144], and Discriminative Robust Local Binary Pattern (DRLBP) are used. These strategies give complimentary data that is combined to generate a more distinct feature set.
2. Feature Integration and Selection: To improve the efficacy of the extracted features, Principle Component Analysis (PCA) is used to identify the most relevant and distinguishing characteristics. The goal is to fine-tune the feature set and keep the features with the greatest discriminative potential.
3. SVM classification: The features that were chosen are then supplied into a Support Vector Machine (SVM), which executes the classification task. Based on the discriminative features, the SVM distinguishes between real and fabricated films, which is an important stage in the forgery detection process.
4. Edge Analysis: Recognising that edges frequently show tampering artefacts, the chrominance channels of the YCbCr colour model are scrutinised for edge anomalies. The Cb and Cr channels have been used by researchers to extract characteristics that signify structural changes and edge information. These channels were selected because they vividly capture the sharp edges caused by manipulation.
5. Texture vs. Edge Information: While LBP approaches excel at capturing texture information, they may fall short of recognising edge abnormalities effectively. DRLBP and WLD are presented as improved options to alleviate this restriction. Because these approaches use both texture and edge data, they are more successful at detecting tampering cues in the spatial domain.
6. geographical/Temporal Localization: The process includes the geographical or temporal localization of damaged regions. This localisation can be accomplished using either block-based or clustered-based approaches, allowing the identification of locations within the video that have been modified.

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

Because of the large number of video frames that must be analysed, efficiency is a major challenge. Exploration of Convolutional Neural Network (CNN)-based techniques, such as deep learning (DL), auto encoders, or deep belief networks (DBN), becomes critical to strike a balance between accuracy and efficiency [58]. The success of these approaches in a variety of artificial intelligence (AI) fields, such as image recognition [59], speech recognition [60], and natural language processing (NLP) [61], demonstrates their utility.

Deep learning [62] has not only accelerated advances in various machine learning techniques, but it has also found use in predicting drug molecule activities [63], reconstructing brain circuits [64], online particle detection [65], and forecasting the effects of non-coding DNA mutations on gene expression and disease [66], among other domains. The Convolutional Neural Network (CNN) [67] component has gained popularity due to its completely connected layers and ease of training. Google, Facebook, Yahoo!, Twitter, Microsoft, and IBM have all used CNN-based algorithms to power their endeavours.

While the breadth of CNN's application is great, it frequently comes at the expense of speed. As a result, NVIDIA, Mobileye, Intel, Qualcomm, and Samsung have created dedicated CNN-based hardware chips to shorten training times. The concept of Extreme Learning Machines (ELM) develops in the pursuit for increased efficiency. ELM not only produces cutting-edge results, but it also dramatically cuts training periods from days to minutes, as opposed to days in deep learning. ELM has proven to be effective in a wide range of applications, including complex chemical process soft-sensing [68] and facial recognition [69].

Transfer learning [70] is still a hot topic in the machine learning community. This strategy involves transferring knowledge from a related, previously learned task to improve learning in a new task, especially when training data is limited. Training data scarcity can occur due to variables such as data sparsity, costly collecting and labelling costs, or unavailability.

Efforts to investigate CNN-based methodologies, leverage the efficiency of ELM, and harness the knowledge transfer capabilities of transfer learning all contribute to addressing the challenge of maintaining accuracy while maintaining efficiency in the complex realm of video tampering detection and localization.

CONCLUSION

In conclusion, this research underscores the escalating concerns surrounding video forgery in the digital landscape. By synthesizing insights from a diverse range of passive blind detection approaches, the study enhances our understanding of effective forgery detection methodologies. The proposed video authentication method, characterized by its adeptness at detecting region and frame duplication, stands as a pivotal contribution to the field. Ultimately, this research aspires to

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

foster a more secure digital environment by combatting the proliferation of malicious video manipulations.

REFERENCES

1. Wang, W. (2009). Digital video forensics (Doctoral dissertation, Dartmouth College Hanover, New Hampshire).
2. Sun, T., Wang, W., & Jiang, X. (2012, March). Exposing video forgeries by detecting MPEG double compression. In Acoustics, Speech and Signal Processing (ICASSP), 2012 IEEE International Conference on (pp. 1389-1392). IEEE.
3. Suhail, M. A., & Obaidat, M. S. (2003). Digital watermarking-based DCT and JPEG model. Instrumentation and Measurement, IEEE Transactions on, 52(5), 1640-1647.
4. Di Martino, F., & Sessa, S. (2012). Fragile watermarking tamper detection with images compressed by fuzzy transform. Information Sciences, 195, 62-90.
5. Chen, H., Chen, Z., Zeng, X., Fan, W., & Xiong, Z. (2008, December). A novel reversible semi-fragile watermarking algorithm of MPEG-4 video for content authentication. In Intelligent Information Technology Application, 2008. IITA'08. Second International Symposium on (Vol. 3, pp. 37- 41). IEEE.
6. Ram, S., Bischof, H., & Birchbauer, J. (2009). Active fingerprint ridge orientation models. In Advances in Biometrics (pp. 534-543). Springer Berlin Heidelberg.
7. Peng, F., Nie, Y. Y., & Long, M. (2011). A complete passive blind image copy-move forensics scheme based on compound statistics features. Forensic science international, 212(1), e21-e25.
8. Shivakumar, B. L., & Santhosh Baboo, L. D. S. (2010). Detecting copy-move forgery in digital images: a survey and analysis of current methods. Global Journal of Computer Science and Technology, 10(7)..
9. R. Esmaeilani, “Source Identification Of Captured Video Using Photo Response NonUniformity Noise Pattern And Svm Classifiers,” 2014.
10. Lin, C. S., & Tsay, J. J. (2014). A passive approach for effective detection and localization of region-level video forgery with spatio-temporal coherence analysis. Digital Investigation.
11. Davarzani, R., Yaghmaie, K., Mozaffari, S., & Tapak, M. (2013). Copy-move forgery detection using multiresolution local binary patterns. Forensic science international, 231(1), 61-72.
12. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Del Tongo, L., & Serra, G. (2013). Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Processing: Image Communication, 28(6), 659-669.
13. Shanableh, T. (2013). Detection of frame deletion for digital video forensics. Digital Investigation, 10(4), 350-360.

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

14. Sheng, YL.,& Tian, Q H. (2013). Video Copy-Move Forgery Detection and Localization Based on Tamura Texture Features. In International Congress on Image and Signal Processing (CISP 2013) (pp. 864- 868).
15. Dong, Q., Yang, G., & Zhu, N. (2012). A MCEA based passive forensics scheme for detecting frame-based video tampering. Digital Investigation, 9(2), 151- 159.
16. Lin, G. S., & Chang, J. F. (2012). Detection of frame duplication forgery in videos based on spatial and temporal analysis. International Journal of Pattern Recognition and Artificial Intelligence, 26(07).
17. Qadir, G., Yahaya, S., & Ho, A. T. (2012). Surrey university library for forensic analysis (SULFA) of video content.
18. A. Rocha, W. Scheirer, T. Boult, S. Goldenstein, "Vision of the Unseen: Current Trends and Challenges in Digital Image and Video Forensics", ACM Computing Surveys (CSUR), Volume 43 Issue 4, October 2011, Article No. 26, doi: 10.1145/1978802.1978805.
19. W. Wang and H. Farid, "Exposing digital forgeries in video by detecting duplication," MM&Sec'07, September 20–21, 2007, Dallas, Texas, USA.
20. Kobayashi, M.; Okabe, T.; Sato, Y.: Detecting forgery from static scene video based on inconsistencies in noise level functions. IEEE Trans. Info. Forensics Secure 5(4) (2010), 883–892.
21. Subramanyam, A. V. and Emmanuel, S., "Video forgery detection using HOG features and compression properties," in Proc. IEEE 14th International Workshop on Multimedia Signal Processing (MMSP 2012), Sept 17- 19,2012. Pp.8994 DOI:10.1109/MMSP.2012.634342.
22. Wang, W., Farid, H.: Exposing digital forgeries in video by detecting duplication. In: Proceedings of the Multimedia and Security Workshop, Dallas, TX, pp. 35–42 (2007)
23. Hsu, C., Hung, T., Lin, C., Hsu, C.: Video forgery detection using correlation of noise residue. In: Proceedings of IEEE Workshop Multimedia Signal Processing (MMSP), Cairns, Queensland, Australia, pp. 170–174 (2008).
24. Kobayashi, M., Okabe, T., Sato, Y.: Detecting Forgery From Static-Scene Video Based on Inconsistency in Noise Level Functions. IEEE Transactions on Information Forensics and Security 5(4), 883–892 (2010).
25. A. R¨ossler, D. Cozzolino, L. Verdoliva, C. Riess, J. Thies, M. Nießner, "Faceforensics: A large-scale video dataset for forgery detection in human faces", arXiv preprint arXiv:1803.09179.
26. Su, Y.T.; Ning, W.Z.; Zhang, C.Q. A frame tampering detection algorithm for MPEG videos. In Proceedings of the IEEE Joint International Information Technology and Artificial Intelligence Conference, Chongqing, China, 20– 22 August 2011; pp. 461–464.
27. Dong, Q.; Yang, G.B.; Zhu, N.B. A MCEA based passive forensics scheme for detecting frame-based video tampering. Digit. Investig. 2012, 9, 151–159.
28. Feng,C.;Xu,Z.;Jia,S.;Zhang,W.;Xu,Y.Motion adaptive frame deletion detection for digital video forensics. IEEE Trans. Circuits Syst. Video Technol. 2017, 27, 2543– 2554.

29. Chao,J.;Jiang,X.H.;Sun,T.F.AnovelvideoInter frame for gerymodel detections cheme based on optical flow consistency. In Digital Forensics and Water making; Springer: Berlin/Heidelberg, Germany, 2013; pp. 267–281.
30. Wu, Y.; Jiang, X.; Sun, T.; Wang, W. Exposing video inter-frame forgery based on velocity field consistency. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, Italy, 4–9 May 2014; pp. 2674–2678.
31. Zhang, Z.; Hou, J.; Li, Z.; Li, D. Inter-frame forgery detection for static-background video based on MVP consistency. Proc. Lect. Notes Comput. Sci. 2016, 9569, 94–106.
32. Zhang,Z.;Hou,J.;Ma,Q.;Li,Z.Efficient video frame insertion and deletion detection based on inconsistency of correlations between ocal binary pattern coded frames. Secur. Commun. Netw. 2015,8,311–320.
33. Xiaoling, C., & Huimin, Z. (2012). A Novel Video Tamper Detection Algorithm Based on Journal of Theoretical and Applied Information Technology 20th April 2015. Vol.74 No.2 © 2005 - 2015 JATIT & LLS. All rights reserved. ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195 219 Semi-fragile Watermarking. In Advances in Information Technology and Industry Applications (pp. 489-497). Springer Berlin Heidelberg.
34. Wang, W., & Farid, H. (2007, September). Exposing digital forgeries in video by detecting duplication. In Proceedings of the 9th workshop on Multimedia & security (pp. 35-42). ACM.
35. Subramanyam, A. V., & Emmanuel, S. (2012, September). Video forgery detection using HOG features and compression properties. In Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on (pp. 89-94). IEEE.
36. Wang, W., & Farid, H. (2006, September). Exposing digital forgeries in video by detecting double MPEG compression. In Proceedings of the 8th workshop on Multimedia and security (pp. 37-47). ACM.
37. Su, L., Huang, T., & Yang, J. (2014). A video forgery detection algorithm based on compressive sensing. Multimedia Tools and Applications, 1-16.
38. Hsu, C. C., Hung, T. Y., Lin, C. W., & Hsu, C. T. (2008, October). Video forgery detection using correlation of noise residue. In Multimedia Signal Processing, 2008 IEEE 10th Workshop on (pp. 170-174). IEEE.
39. Kancherla, K., &Mukkamala, S. (2012). Novel blind video forgery detection using markov models on motion residue. In Intelligent Information and Database Systems (pp. 308-315). Springer Berlin Heidelberg.
40. Sheng, YL., & Tian, Q H. (2013). Video Copy-Move Forgery Detection and Localization Based on Tamura Texture Features. In International Congress on Image and Signal Processing (CISP 2013) (pp. 864- 868).
41. Davarzani, R., Yaghmaie, K., Mozaffari, S., &Tapak, M. (2013). Copy-move forgery detection using multire solution local binary patterns. Forensic science international, 231(1), 61-72

Catalyst Research Volume 23, Issue 2, September 2023 Pp. 1411-1426

42. Hernandez-Ardieta, J.L.; Gonzalez-Tablas, A.I.; De Fuentes, J.M.; Ramos, B. A taxonomy and survey of attacks on digital signatures. Comput. Secur. 2013, 34, 67–112.
43. Chen, H.; Chen, Z.; Zeng, X.; Fan, W.; Xiong, Z. A novel reversible semi-fragile watermarking algorithm of MPEG-4 video for content authentication. In Proceedings of the Second International Symposium on Intelligent Information Technology Application, Shanghai, China, 20–22 December 2008.
44. Di Martino, F.; Sessa, S. Fragile watermarking tamper detection with images compressed by fuzzy transform. Inf. Sci. 2012,195, 62–90
45. Zampoglou, M.; Markatopoulou, F.; Mercier, G.; Touska, D.; Apostolidis, E.; Papadopoulos, S.; Cozien, R.; Patras, I.; Mezaris, V.;Kompatsiaris, I. Detecting Tampered Videos with Multimedia Forensics and Deep Learning. In Proceedings of the International Conference on Multimedia Modeling, Thessaloniki, Greece, 8–11 January 2019.
46. Yao, Y.; Shi, Y.; Weng, S.; Guan, B. Deep learning for detection of object-based forgery in advanced video. Symmetry 2017, 10, 3.
47. Kono, K.; Yoshida, T.; Ohshiro, S.; Babaguchi, N. Passive Video Forgery Detection Considering Spatio-Temporal Consistency. In
48. Proceedings of the International Conference on Soft Computing and Pattern Recognition, Porto, Purtugal, 13–15 December 2018.
49. D'Avino, D.; Cozzolino, D.; Poggi, G.; Verdoliva, L. Autoencoder with recurrent neural networks for video forgery detection.
50. Electron. Imaging 2017, 2017, 92–99
51. Kaur, H.; Jindal, N. Deep Convolutional Neural Network for Graphics Forgery Detection in Video. Wirel. Pers. Commun. 2020, 14, 1763–1781.
52. Kohli, A.; Gupta, A.; Singhal, D. CNN based localisation of forged region in object-based forgery for HD videos. IET Image Process.2020, 14, 947–958.
53. Feng, C.; Xu, Z.; Zhang, W.; Xu, Y. Automatic location of frame deletion point for digital video forensics. In Proceedings of the 2nd ACM Workshop on Information Hiding and Multimedia Security, Salzburg, Austria, 11–13 June 2014.
54. Feng, C.; Xu, Z.; Jia, S.; Zhang, W.; Xu, Y. Motion-adaptive frame deletion detection for digital video forensics. IEEE Trans. Circuits Syst. Video Technol. 2016, 27, 2543–2554.
55. Kingra, S.; Aggarwal, N.; Singh, R.D. Inter-frame forgery detection in H. 264 videos using motion and brightness gradients. Multimed. Tools Appl. 2017, 76, 25767–25786
56. Jia, S.; Xu, Z.; Wang, H.; Feng, C.; Wang, T. Coarse-to-fine copy-move forgery detection for video forensics. IEEE Access 2018, 6,25323–25335
57. Joshi, V.; Jain, S. Tampering detection and localization in digital video using temporal difference between adjacent frames of actual and reconstructed video clip. Int. J. Inf. Technol. 2019, 78, 11527–11562.
58. Chen, J.; Kang, X.; Liu, Y.; Wang, Z.J. Median Filtering Forensics Based on Convolutional Neural Networks. Signal Process. Lett. IEEE 2015, 22, 1849–1853.

59. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. Imagenet classification with deep convolutional neural networks. In Proceedings of the Advances in Neural Information Processing Systems, Montréal, QC, Canada, 3–6 December 2012.
60. Hinton, G.; Deng, L.; Yu, D.; Dahl, G.E.; Mohamed, A.-R.; Jaitly, N.; Senior, A.; Vanhoucke, V.; Nguyen, P.; Sainath, T.N. Deep neural networks for acoustic modeling in speech recognition: The shared views of four research groups. Signal Process. Mag. IEEE 2012, 29, 82–97.
61. Sutskever, I.; Vinyals, O.; Le, Q.V. Sequence to sequence learning with neural networks. In Proceedings of the Advances in Neural Information Processing Systems, Montreal, QC, Canada, 8–13 December 2014.
62. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. Nature 2015, 521, 436–444.
63. Ma, J.; Sheridan, R.P.; Liaw, A.; Dahl, G.E.; Svetnik, V. Deep neural nets as a method for quantitative structure–activity relationships. J. Chem. Inf. Model. 2015, 55, 263–274.
64. Helmstaedter, M.; Briggman, K.L.; Turaga, S.C.; Jain, V.; Seung, H.S.; Denk, W. Connectomic reconstruction of the inner plexiform layer in the mouse retina. Nature 2013, 500, 168–174.
65. Xiong, H.Y.; Alipanahi, B.; Lee, L.J.; Bretschneider, H.; Merico, D.; Yuen, R.K.; Hua, Y.; Gueroussov, S.; Najafabadi, H.S.; Hughes, T.R. The human splicing code reveals new insights into the genetic determinants of disease. Science 2015, 347, 1254806.
66. Leung, M.K.; Xiong, H.Y.; Lee, L.J.; Frey, B.J. Deep learning of the tissue-regulated splicing code. Bioinformatics 2014, 30, i121–i129.
67. Le Cun, B.B.; Denker, J.S.; Henderson, D.; Howard, R.E.; Hubbard, W.; Jackel, L.D. Handwritten digit recognition with a back-propagation network. In Proceedings of the Advances in Neural Information Processing Systems, Lakewood, CO, USA, 26–29 June 1990.
68. Peng, D.; Xu, Y.; Wang, Y.; Geng, Z.; Zhu, Q. Soft-sensing in complex chemical process based on a sample clustering extreme learning machine model. IFAC-PapersOnLine 2015, 48, 801–806.
69. Peng, Y.; Wang, S.; Long, X.; Lu, B.-L. Discriminative graph regularized extreme learning machine and its application to face recognition. Neurocomputing 2015, 149, 340–353.
70. Pan, S.J.; Yang, Q. A survey on transfer learning. IEEE Trans. Knowl. Data Eng. 2010, 22, 1345–1359.
71. Jalab, H.A.; Subramaniam, T.; Ibrahim, R.W.; Kahtan, H.; Noor, N.F.M. New Texture Descriptor Based on Modified Fractional Entropy for Digital Image Splicing Forgery Detection. Entropy 2019, 21, 371. https://doi.org/10.3390/e21040371