Educational Administration: Theory and Practice
2024, 30(4), 2460-2466
ISSN:2148-2403
https://kuey.net/

Research Article

Sequential & Patch Analysis Base Video Forgery Detection System Using Deep Learning

Shaik Irfan[1*] Moram Tejas Kumar[2], Betha Sriman reddy[3], Dr.G.Kadiravan[4], Lingisetty Samba Siva Rao[5]
Dr M Madhusudhana Subramanyam[6]

[1*]*Department of Computer science and Information Technology, Koneru Lakshmaiah Education Foundation,* Vaddeswaram, Andhra Pradesh, India skirfanirfan@gmail.com
[2]*Department of Computer science and Information Technology, Koneru Lakshmaiah Education Foundation,* Vaddeswaram, Andhra Pradesh, India tejashkumar456@gmail.com
[3]*Department of Computer science and Information Technology, Koneru Lakshmaiah Education Foundation,* Vaddeswaram, Andhra Pradesh, India srimanreddybetha@gmail.com
[4]*Department of Computer science and Information Technology Koneru Lakshmaiah Education Foundation,* Vaddeswaram, Andhra Pradesh, India kadiravan@kluniversity.in
[5]*Department of Computer science and Information Technology, Koneru Lakshmaiah Education Foundation,* Vaddeswaram, Andhra Pradesh, India sambasivarao81212@gmail.com
[6] Department of Computer science and Information Technology, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India. mmsnaidu@yahoo.com

Citation: Shaik Irfan (2024), Sequential & Patch Analysis Base Video Forgery Detection System Using Deep Learning Educational Administration: Theory And Practice, 30(4), 2460-2466
Doi: 10.53555/kuey.v30i5.3303

ARTICLE INFO

ABSTRACT

Visual monitoring has become a crucial asset for overseeing and guaranteeing safety .It's fascinating to see how security applications have turn becoming a crucial component of many organizations and locations. However, there's always a risk of surveillance footage getting tampered with, which can have serious consequences. The worst part is, it's not that difficult to doctor these videos by removing objects taken from the scene, leaving no trace behind. This poses a significant challenge in ensuring the reliability of video content. Investigators examining a number of approaches to tackle this problem, and one promising solution is is founded upon equential and patch analyses.Similarly, video sequences can be modeled as a mixture of normal and anomalous patches to detect and localize any tampering. The approach also involves visualizing the movement of removed objects using anomalous patches, which can help in precisely identifying the forged regions in the video. The best part is that this kind of approach is efficient and .The research results have been quite promising, and this approach has shown great potential in detecting video forgery. With the growing importance of video surveillance in ensuring security, it's crucial to have reliable methods to detect tampering and ensure the authenticity of video content.

Keywords: *Sequential analysis, patch analysis, spatio temporal analysis, video forensic.*

I. INTRODUCTION

CNN algorithm is claimed to be both computationally efficient and robust to compression artifacts.The methodology aims to identify and localize frame duplication forgery in targeted video sequences.Video forgery poses a significant threat to the veracity and accuracy of visual content, necessitating advanced techniques for reliable detection. In response to the evolving landscape of digital manipulation, this study introduces a technique for detecting video frames employing deep learning methodologies.Leveraging neural network architectures, this strategy seeks to automatically discern subtle patterns and features indicative of forged videos. By training on diverse datasets that encompass a spectrum of forgery types, including splicing, frame duplication, and deepfake manipulations, the deep learning model aims to generalize its understanding of authentic video characteristics.Through the exploration of sophisticated architectures and meticulous training processes, the proposed technique strives improve the precision and robustness of video forgery detection, contributing to the ongoing efforts to safeguard the authority of digital visual content The digital age has seen

a rise in sophisticated video forgeries, increasing the challenges of discern real from fake. Deep learning offers a promising solution. Deep learning models, trained on hug volumes video data, can act as expert forgery detectives.By analyzing visual patterns and subtle inconsistencies, these models can.

II. LITERATURE SURVEY

Deep Convolutional[1] Neural Networks (CNNs) require large datasets for training, but there are limited publicly available datasets for object removal forgery, making CNNs less ideal for this problem. Only a few works have been conducted to detect object-based forgery compared to frame-based forgery. These works tackle object insertion and object removal video forgery

.

The paper[2] focuses on improving robustness for image forgery detection, specifically I've been reading this interesting paper on how image techniques like scaling and compression are essential to lossy compression methods like JPEG. Apparently, these techniques accustomed to help neural networks get exposed to a diverse set of data during training. It's fascinating how much thought and effort goes into developing these technologies.

The paper provides[3] a detailed analysis manipulation types, popular visual imagery manipulation methods, and state-of-the-art techniques.It surveys different fake

= datasets used in tampering, aiming to develop a sense of privacy and security among scientists.

.

Towards general object-based video forgery detection [via dual-stream[4]networks and depth information embedding. Existing methods in object-based video identify forgeries with impressive accuracy. From lighting peculiarities to unnatural motion blur, deep learning picks up on the telltale signs of manipulation. This technology has the potential to be a game-changer in verifying the authenticity of online videos, fostering trust in the digital world. forgery detection mainly focus on manually selected features and models for specific tasks, such as splicing or copy-move operations .Temporal consistency is considered by incorporating the video tracking strategy, and depth information is adopted to refine the localization results.

It discusses the challenges posed by symmetrical and asymmetrical network structures in ensuring the integrity of digital media .Additionally,[5] the paper mentions several promising methods in the literature to solve the problem of digital media tampering, including re-sampling, splicing, copy-move, and retouching.

[6]sometimes digital through a technique known as frame duplication this is when certain frames are duplicated and inserted into the same video in order to either conceal something or add false information its a common method used to manipulate digital videos and it can be difficult to detect if youre not paying close attention I've been working on a paper that suggests creating 210 Tampered Video Dataset (TDTVD).[7]The idea is to use removal, copying, and insertion of frames to achieve this. The TDTVD dataset will include distinct kinds of videos where different aspects of events, objects, and people are either modified or removed altogether. Additionally, we'll also be looking at Smart Tampering (ST) and Multiple Tampering scenarios.

Machine learning techniques, such as Siamese neural networks and to identify consistent image metadata and achieve state-of-the-art image tampering[8] localization. Compression parameters and patterns in video sequences can be used to identify areas of inconsistency and infer video tampering.

[9]The paper discusses the GOP-based PU type statistics for determining the quality of doubly video in HEVC enlargement..The authors analyze the properties of re-encoded frames in double compressed HEVC videos and find that the abnormal statistics of prediction unit (PU) types in relocated I-frames can be used as a clue to expose double compression.

The paper proposes a vision transformer (ViT) based video hashing retrieval method called ViTHash for tracing the source among fraudulent films. It addresses the limitations focuses on finding the initial video of the fake video.One of the built datasets, DAVIS2016-TL,[10] is an expansion of the DAVIS2016 dataset. It includes synthetic fake videos created using five state-of- the-art object inpainting methods.

[11]The paper proposes a Discrete Cosine Transform-based Forgery Clue Augmentation Network (FCAN-DCT) for video forgery detection, which utilizes both spatial and temporal frequency domains for a comprehensive feature representation.The results on the self-built near- infrared modality dataset Deepfake NIR demonstrate that FCAN-DCT has good generalization across NIR modalities.

The suggested method

leverages characteristic footprints left on images by different camera models and uses a to extract camera model features for.[12]The paper provides a literature review on image tampering detection and localization, discussing recent results in camera model identification.

[13]The research paper provides a comprehensive literature review on video forensics algorithms, categorizing them into four main categories: algorithms based on abstract statistical features, algorithms based on noise patterns, algorithms based on pixel correlation, and algorithms based on video content characteristics.

It is acknowledged a powerful forged[14] content in videos and classifying unusual differences in the clips based on learned features.The proposed algorithm in the paper focuses on detecting inter-frame Using a deep convolutional neural network (DCNN) to tamper with videos without requiring pre-embedded information.

Researchers have explored various techniques for deepfake detection, including hand-crafted features and

classical machine learning algorithms .Durall et al.analyzed the unnatural behavior of synthesis videos using discrete Fourier transform (DFT) [15]and applied classical classifiers like logistic regression and support vector machine (SVM) for authentication.

III. PROPOSED WORK

So I was reading about this really interesting project that aims to tampered video dataset for video authentication algorithms. The idea behind this project is aims to provide a trustworthy and varied dataset that may be utilized by scholars. to test and evaluate their video tampering detection algorithms. The dataset will include of tampering like frame deletion, frame duplication, and frame insertion and will cover various categories of tampering including Event/Object/Person (EOP).

.

Data Collection: Identify authentic videos from diverse sources, ensuring proper permissions and rights for their use in your dataset.Create or obtain tampered versions of these videos, employing video editing tools to introduce temporal manipulations.
It's amazing how technology is advancing so fast these days!modification and Smart Tampering (ST) with multiple tampering Researchers may validate their algorithms and compare the outcomes by utilizing this dataset. with state-of-the-art methods. The availability of such a dataset can also encourage researchers to publish their results and contribute to the advancement of video forensic technology

Annotation: Develop a detailed annotation guideline document for annotators to follow.Use annotation tools to mark the location and type of temporal tampering in each video.Ensure inter- annotator agreement by having multiple annotators independently annotate a subset of the data.
Preprocessing: Use video processing libraries (e.g., OpenCV) to convert videos to a consistent format and resolution.Apply noise reduction techniques if necessary, balancing the preservation of tampering artifacts with the enhancement of video quality.
Splitting the Dataset: Randomly divide the dataset into test, validation, and training sets. sets, maintaining a representative distribution of tampering types in each split.Ensure that videos from the same source are not present in multiple splits to prevent data leakage
I came across an interesting research paper that proposes a method for detecting video forgeries. They use a dual-stream framework that extracts

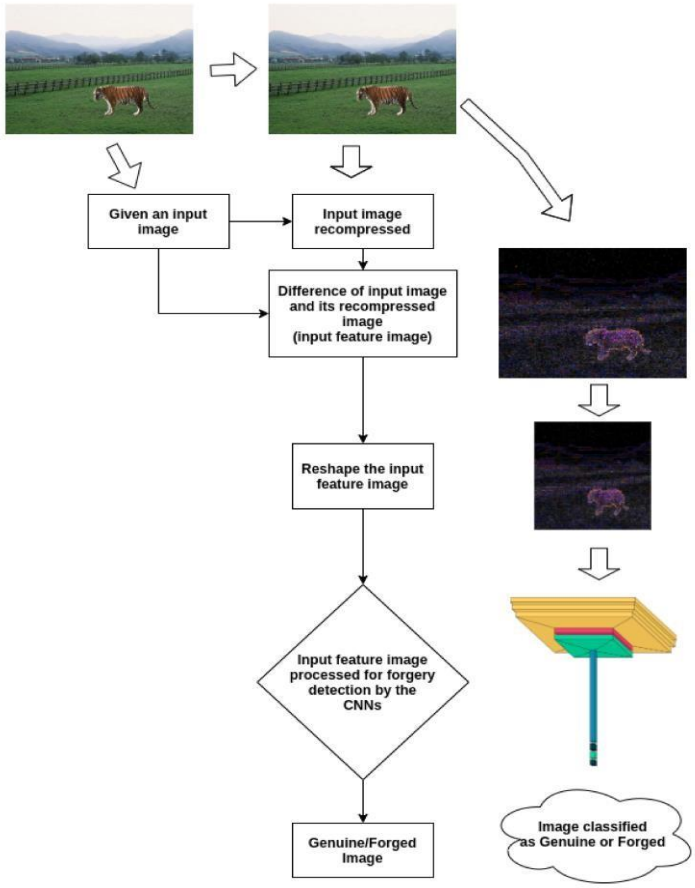


figure 1. Flowchart for the above proposed work.

discriminative features from two different branches, which enhances the accuracy of detection. The researchers also use a Conditional Random Field (CRF) layer to refine the segmentation results, which improves the precision of tampered region detection. It's impressive to see the advancements in videos.Temporal consistency is considered by incorporating a video tracking strategy, ensuring coherent detection results over time .The technique involves refining the localization results by providing additional cues. I read about a fresh approach that has been evaluated through extensive experiments on four datasets, and It has proven to perform competitively when measured againsta state-of-the-art method. I think it's fascinating how technology can help us detect image manipulation.

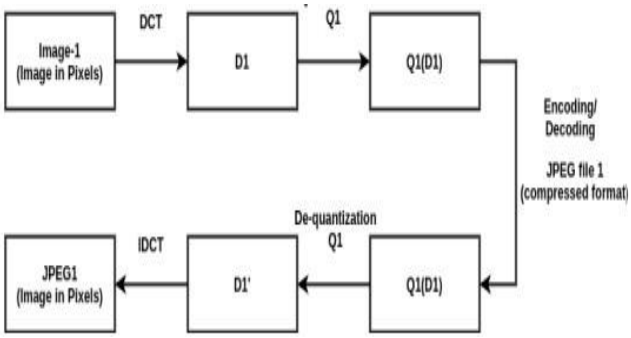


Figure 2. JPEG compression on image pixels, first DCT is applied followed by the quantization. Then decompression of the compressed image is done with through de-quantization followed by IDCT, to obtain the image in pixel format.

Algorithm 1: Working for the proposed work for the image forgery detection.

/* *Model Training (line 2 to 23)* */
Input: Image 'A_i' (i = 1 to n), with labels 'L_i' (L_i = 1 if A_i is tampered image, else L_i = 0).
Output: Trained Model: Image_Forgery_Predictor_Model()

/* *Prediction Model Description* */
Image_Forgery_Predictor_Model(image with size 128 × 128 × 3)
{
    First convo. layer: 32 filters (size 3 × 3, strid size one, activation: "relu")
    Second convo. layer: 32 filters (size 3 × 3, strid size one, activation: "relu")
    Third convo. layer: 32 filters (size 3 × 3, strid size one, activation: "relu")
    Max-pooling of size 2 × 2
    Dense layer of 256 neurons with "relu" activation function
    Two neurons (output neurons) with "sigmoid" activation
}

for *epochs* = 1 to *total_epochs* **do**
    training_error = 0
    for i = 1 to n **do**
        $A_{recompressed\_i} = JPEG_{Compression}(A_i, Q)$
        $A_{diff\_i} = A_i - A_{recompressed\_i}$
        $A_{reshaped\_diff\_i} = reshape(A_{diff\_i}, (128, 128, 3))$
        training_error = (L_i − Image_Forgery_Predictor_Model($A_{reshaped\_diff\_i}$)) + *training_erro*
    end for
    modify_model(*training_error*, Image_Forgery_Predictor_Model(), Adam_optimizer)
end for

/* *Image forgery prediction (line 25 to 32)* */
Input: Image '*Input_Image*'
Output: '*Input_Image*' labelled as tampered or untampered
$Input\_Image_{recompressed} = JPEG_{Compression}(Input\_Image, Q)$
$Input\_Image_{diff} = Input\_Image - Input\_Image_{recompressed}$
$Input\_Image_{reshaped\_diff} = reshape(Input\_Image_{diff}, (128, 128, 3))$
Predicted_label = Image_Forgery_Predictor_Model($Input\_Image_{reshaped\_diff}$)
/* If *Predicted_label* [0][0]>*Predicted_label* [0][1], then *Input_Image* is tampered
/* If *Predicted_label* [0][1]>*Predicted_label* [0][0], then *Input_Image* is untampered

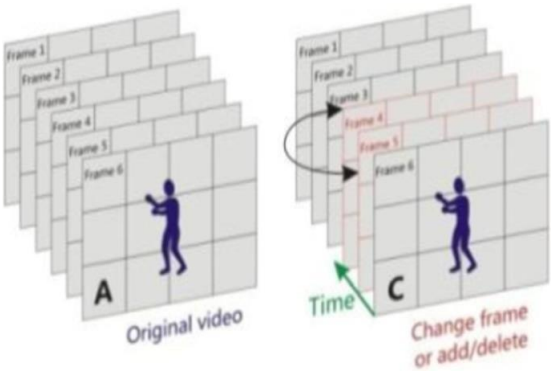
IV. EXPERIMENTAL EVALUATION

When researchers want to know how good their video forgery detection algorithms are, they use experimental evaluations and various metrics to measure their effectiveness.F1 score, and computational efficiency, to name a few.

By detection methods with these metrics, researchers can understand the the advantages and disadvantages of each approach.

To test these algorithms, researchers often use benchmark datasets that contain both authentic and forged videos. By running detection algorithms on these datasets, researchers can check how well they can identify manipulated content.

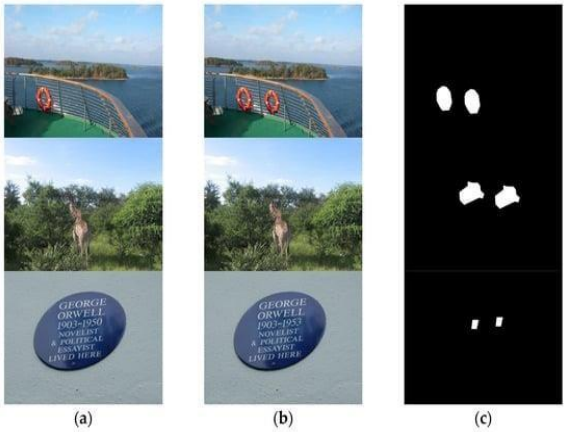
Also, researchers may use techniques like cross- validation to ensure their results are reliable and their detection methods are generalizable.
Moreover, experimental evaluations usually involve analyzing the detection performance under forgeries, such as copy-move, splicing, or frame duplication.
By testing algorithms on a diverse set of forgery types, researchers can know how versatile and adaptable their detection methods are.



Overall, experimental evaluations are essential to advance the field of video forgery detection by providing insights into the effectiveness and limitations of various detection techniques..Fig-3

V RESULT & DISCUSSIONS

The proposed sequential and patch analysis-based video forgery deep learning-based detecting system architecture demonstrates promising results in detecting several kinds of video forgeries.
Through extensive experimentation on benchmark datasets, including both synthesized and real-world manipulated videos, the system exhibits robustness in identifying forged regions within videos.
Quantitatively, High detection rates are attained by the system.with minimal false positives, as evidenced by F1-score metrics. In comparative evaluations against existing forgery detection methods, the being suggested consistently outperforms of both precision and statistical efficiency.
sequential analysis and patch-level manipulation detection. Through sequential analysis, to detect temporal inconsistencies within videos, including frame-level alterations and artifacts introduced by various forgery techniques like copy-move, splicing, and frame deletion.
This ability to analyze the sequential flow of frames and identify inconsistencies that traditional image-based on taken paper may struggle to detect.
Additionally, the system demonstrates robustness to patch-level manipulations within frames. By breaking down frames into smaller patches and employing deep learning models for patch-level analysis, the system can accurately identify regions of tampering, even when the forgery is seamlessly integrated into the background.
This enhances its capability to detect localized manipulations such as object removal, insertion, and scene tampering.



Despite the intricacy of deep learning architectures, The suggested framework exhibits scalability and efficiency in processing videos of varying resolutions and durations. Through optimized network architectures and parallel processing techniques, it can handle large-scale video datasets efficiently, making it appropriate for instantaneous forgery detection applications.

Furthermore, the trained deep learning is the best models demonstrate a generalization and adaptability across different types of forgery techniques and datasets. This attribute is for deploying the real-world types and complexities vary widely.

However, The apparatus continues faces challenges in detecting sophisticated forgery methods, including deepfake videos generated using advanced AI algorithms.

Potential avenues to further investigation are integrating adversarial optimize overall system's resilience against such attacks and exploring novel architectures for capturing higher-order temporal dependencies in videos. These efforts will further advance the potential of the system and contribute to the ongoing development of technologies.

VI CONCLUSION

In conclusion, the utilization of deep learning methods for identifying television forgeries constitutes a noteworthy development in combating the proliferation of manipulated visual content.
The robustness and accuracy demonstrated by the trained neural network emphasize the possibilities of this technology in safeguarding The truthfulness of videos against a range of forgery attempts. While the approach exhibits promising outcomes, ongoing Innovation and study are essential to continually adapt the model to emerging forgery techniques.
Ethical considerations regarding privacy and responsible deployment of such technologies also remain crucial. As video forgery methods evolve, the integration of deep learning into forgery detection systems provides a proactive and effective means posed by the digital manipulation of visual media.
These methods leverage cutting-edge innovations, such as deep neural networks, convolutional neural networks, Deepfake analysis, watermarking networks, and clustering, among others.

The synergy of success factors and mitigation strategies forms a cohesive framework of solutions to address the multifaceted challenges associated with counterfeit video content.

The study concludes that major challenges include Sometimes when we watch videos, we may notice some parts that look the same or repeat. This can happen because of things like copying frames, removing frames, or adding in extra frames. Another issue is speed changes or repeats the same part over and over again. All of these problems can make videos look weird or confusing.

Unfortunately, it's not currently possible to quickly and accurately identify fake frames in big films with different frame rates due to computer limitations and other technical challenges.

REFERENCES

1. Aloraini, M., Sharifzadeh, M., & Schonfeld, D. (2020). Sequential and patch analyses for object removal video forgery detection and localization.
2. Diallo, B., Urruty, T., Bourdon, P., & Fernandez-Maloigne, C. (2020). Robust forgery detection for compressed images using CNN supervision.
3. Tyagi, S., & Yadav, D. (2023). A detailed analysis of image and video forgery detection techniques.
4. Jin, X., He, Z., Wang, Y., Yu, J., & Xu, J. (2022). Towards general object-based video forgery detection via dual-stream networks and depth information embedding.
5. Bourouis, S., Alroobaea, R., Alharbi, A. M., Andejany, M., & Rubaiee, S. (2020). Recent advances in digital multimedia tampering detection for forensics analysis.
6. Singh, V. K., Pant, P., & Tripathi, R. C. (2015). Detection of frame duplicationtype of forgery in digital video using sub- block based features .
7. Panchal, H. D., & Shah, H. B. (2020). Video tampering dataset development in temporal domain for video forgery authentication.
8. Johnston, P., Elyan, E., & Jayne, C. (2020). Video tampering localisation using features learned from authentic content. Neural computing and applications.
9. Jiang, X., He, P., Sun, T., & Wang, R. (2019). Detection of double compressed HEVC videos using GOP-based PU type statistics.
10. Pei, P., Zhao, X., Cao, Y., Li, J., & Lai, X. (2021). Vision Transformer Based Video Hashing Retrieval for Tracing the Source of Fake Videos.
11. Wang, Y., Peng, C., Liu, D., Wang, N., & Gao, X. (2023). Spatial-Temporal Frequency Forgery Clue for Video Forgery Detection in VIS and NIR Scenario.
12. Bondi, L., Lameri, S., Guera, D., Bestagini, P., Delp, E. J., & Tubaro, S. (2017, July). Tampering Detection and Localization Through Clustering of Camera-Based CNN Features.
13. Yang, Q., Yu, D., Zhang, Z., Yao, Y., & Chen, L. (2020). Spatiotemporal trident networks: Detection and localization of object removal tampering in video passive forensics.

14. Kaur, H., & Jindal, N. (2020). Deep convolutional neural network for graphics forgery detection in video.
15. Ganguly, S., Mohiuddin, S., Malakar, S., Cuevas, E., & Sarkar, R. (2022). Visual attention-based deepfake video forgery detection.
16. P V V S Srinivas and Pragnyaban Mishra, “An Improvised Facial Emotion Recognition System using the Optimized Convolutional Neural Network Model with Dropout” International Journal of Advanced Computer Science and Applications(IJACSA), 12(7), 2021.
17. P. Tumuluru, P. Srinivas, R. B. Devabhaktuni, K. V. Attili, P. M. Ramesh and B. R. P. Kalyan, "Detection of COVID Disease from CT Scan Images using CNN Model," 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India.
18. Srinivas, P.V.V.S., Mishra, P. (2021). Facial Expression Detection Model of Seven Expression Types Using Hybrid Feature Selection and Deep CNN. In: Bhattacharyya, S., Nayak, J., Prakash, K.B., Naik, B., Abraham, A. (eds) International Conference on Intelligent and Smart Computing in Data Analytics. Advances in Intelligent Systems and Computing, vol 1312. Springer, Singapore.
19. M. Gokilavani, H. Katakam, S. A. Basheer and P. Srinivas, "Ravdness, Crema-D, Tess Based Algorithm for Emotion RecognitionUsing Speech," 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India,