video forgery

by Dilkeshwar pandey

Submission date: 03-Mar-2025 12:16PM (UTC+0530)
Submission ID: 2587447307
File name: VIDEO_FORGERY_DETECTION_Research_Paper.pdf (398.71K)
Word count: 3137
Character count: 18139

VIDEO FORGERY DETECTION SYSTEM

Dr. Dilkeshwar Pandey
Department of Computer Science and Engineering KIET Group of Institutions, Delhi-NCR, Ghaziabad, U.P. India
dilkeshwar.pandey@kiet.edu

Abhishek Dubey
Department of Computer Science and Engineering KIET Group of Institutions, Delhi-NCR, Ghaziabad, U.P. India
abhishek.2125cse1175@kiet.edu

Ayush Kumar
Department of Computer Science and Engineering KIET Group of Institutions, Delhi-NCR, Ghaziabad, U.P. India
ayush.2125cse1025@kiet.edu

Ayush Yadav
Department of Computer Science and Engineering KIET Group of Institutions, Delhi-NCR, Ghaziabad, U.P. India
ayush.2125cse1016@kiet.edu

Abstract—*The accelerated advancement of digital technology has resulted in the widespread distribution of video content on various platforms, thus exposing it to greater susceptibility to forgery. Splicing, cloning, and deepfake creation are some of the processes that are characteristic of the tools used in video counterfeiting, which have enormous implications for media authenticity, security protocols, and judicial systems. This paper provides a comprehensive overview of video forgery detection systems with focus on the techniques utilized in identifying tampered content. A review of state-of-the-art deep learning methods, including generative adversarial networks (GANs) and convolutional neural networks (CNNs), and conventional pixel-based and temporal analysis methods is provided. The study covers various approaches, datasets, and the challenges that come with identification of highly advanced forgeries. We conclude by noting the major applications of these systems in law enforcement, journalism, and digital verification, and we propose*.

Keywords— Video Forgery, Deepfake Detection, Splicing Detection, Cloning Detection.

1. Introduction

Video content has emerged as the primary medium for sharing information, communication and entertainment in the digital age. But this increase in the use of videos has also led to the worrying issue of video forgery, which is the fabrication or manipulation of recordings in order to deceive viewers or distort the facts. Video forgeries are a huge threat to public safety, privacy of individuals, and the integrity of sources of information. Forgeries may be as basic as splicing and cloning or as sophisticated as highly developed deepfakes. The process of identifying between realistic forgeries has been made easier due to easier access to high-end editing software and artificial intelligence (AI) technology; therefore, identification of such alterations is crucial.

Video forgery detection tools are now important in addressing and mitigating the problem of video manipulation, which has become increasingly problematic.

2. Types of Video forgery

Slicing:

Slicing is the method of dividing and reconstructing video recordings to alter the original message. The method is used in reshaping events by omitting or relocating segments of the video content. An example is that a speech may be sliced in a way to omit key statements, hence leading the audience to believe that the speaker delivered a completely different message.The process is frequently used in fraudulent media content to shape public opinion.

Copy-Move(Cloning):

Copy-move forgery is the act of selecting an item of video material and moving it within the same visual content. The technique is commonly applied to surveillance objects or concealment of specific areas. A surveillance video shows concealment when copied background pixels are positioned above what needs to be hidden. The identification of this type of forgery requires expert forensic analysis because the altered section of the video originally came from the same source.

Frame Insertion/Deletion:

A modification of a video timeline occurs when frames get either added or eliminated during Frame Insertion/Deletion processes. Both the duration of an action grows longer when inserting additional frames yet deleting frames results in key point removal. Detectives use this process on surveillance video fakes to eliminate critical evidence for altering the perception of what happened in an incident. While these imitations may be unsuspected by ordinary observers, there are programs designed for forensic purposes that can detect irregularities of movement and frames.

Deepfakes:

Deepfakes are the latest technology of video manipulation, using artificial intelligence to swap a person's facial and voice features with another's. The method utilizes deep learning algorithms to interpret facial movements, gestures, and patterns of speech and, as such, generate extremely realistic yet false content. Deepfakes tend to be deployed in disinformation operations, deceptive plots, and identity theft scenarios. Their deceptive nature necessitates the use of AI-driven detection systems, forensic examination, and sensitization of the public regarding this emerging menace.

3. Prerequisites of Video Forgery Detection

Video Compression and Formats: Understanding popular video formats (e.g., MP4, AVI, MOV) and compression techniques (e.g., H.264, MPEG) is beneficial because compression creates artifacts that may make forgery detection easier or harder.

Frame Rate and Resolution: Understanding the structure of video frames, i.e., frame rate (FPS), resolution, and how frames are interdependent in a video stream.

Keyframes and Inter-frame Compression: Understanding how videos compress with keyframes and inter-frame compression to conserve file space is crucial for identifying changes in temporal coherence.

Pixel-level Analysis: Knowledge of how to work with and analyze pixels in images and video. The system must detect any abnormal patterns within pixels and synthetic artifacts throughout the video.

Video noise patterns and artifacts: It demand evaluation about their appearance points together with noise sources including sensor noise and compression artifacts to establish every possible noise behavior following video authenticity modification.

Image Filters and Feature Detection: Familiarity with image filters (e.g., edge detection, Gaussian blur) and feature detection algorithms (e.g., SURF, SIFT) in order to search video frames for evidence of tampering.

Optical Flow: Optical flow is one of the most significant temporal analysis concepts that helps in motion tracking between two successive frames in a video to detect anomalies.

Supervised Learning: The development of AI-based forgery detection requires knowledge of supervised machine learning because models operate through a supervised process with labeled examples (actual or simulated videos).

Convolutional Neural Networks (CNNs):

Understandings of Convolutional Neural Networks (CNNs) serve the detection of manipulation primarily through deepfakes since these networks identify patterns from visual data.

Generative Adversarial Networks (GANs): GANs are widely used in the production of deepfakes and therefore it is essential to understand how they function so that they can be detected.

Linear Algebra: Most of the algorithms of video processing such as image transformation and deep learning models rely on operations such as matrix operations, eigenvalues, and vector spaces.

Statistics and Probability:

Probability theory is employed to characterize noise, statistical inconsistency is investigated, and machine learning algorithms to detect forgery are built.

4.Methodology

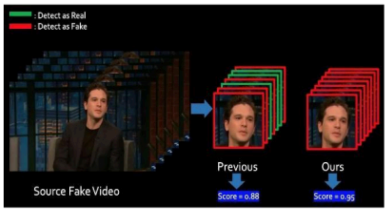
People use different digital techniques to manipulate images by changing their form and appearance. The translate tool provides users with straightforward tools such as cropping as well as advanced features including object removal and deepfake creation capabilities. Methods employed for authentic purposes in film as well as journalism and digital art can also be misused to produce purposefully deceptive or deliberately incorrect information. Manipulation for malign intentions can change the meaning of an image, stage a false scenario, or mislead people, and thus is a large issue in the digital era.

Altered image detection is a blend of manual and automated techniques. One of the primary techniques is metadata analysis, where investigators look for the concealed information in an image file, such as timestamps, device data, and editing history, to detect inconsistencies. Another significant technique is compression artifact analysis, which looks for distortions introduced by different compression processes. Altered images will display inconsistencies in compression patterns, especially in areas where changes have been made. Last, pixel-level discrepancy detection helps detect unnatural transitions or cloned areas that indicate tampering. With the introduction of artificial intelligence, machine learning based detection is also an effective technique of image forgery detection. Deep learning models can read through millions of images to detect patterns of manipulation, like discrepancies of light, irregularities in shadows, and texture discrepancies that are difficult to detect for the human eye. The models receive training through extensive genuine and tampered image collections which enables accurate detection of forgeries. The detection system for deepfakes uses the analysis of facial expressions and abnormal eye tracking together with lisped facial expressions to identify artificial content made by deepfakes.

Research along with development work needs to continue because manipulation technologies evolve at a rapid pace. The Internet world benefits from continuous enhancement of detection methods which forensic digital experts and social media platforms and companies develop to battle misinformation and discourage fraud while authenticating visual content.

5. Image manipulation and detection

Image manipulation is the use of computer software to adjust or alter digital images to meet a desired effect. Typical image manipulations to be performed on photos are changes in brightness, removal of objects, and integration of parts of other images, often for commercial or artistic use. Image manipulation can, nonetheless, be used to disseminate false information, and thus in domains such as legal investigations, media integrity, and digital forensics, detection is of paramount importance.



5.1. Image manipulation methods

Cropping: Removing unwanted areas of an image to emphasize a specific area.

Resizing: Image resizing changes dimensions by modifying original dimensions but does not affect the aspect ratio.

Color Adjustment:

The appearance receives visual enhancement through adjustments of brightness levels contrast structure as well as saturation and hue values.

Spot Removal:

Blemishes together with scratches and imperfections can be removed using spot removal techniques from images.

Sharpening: Enhancing image sharpness by increased contrast between adjacent pixels.

Blurring: The process of softening areas in images exists for both detail reduction and artistic effects.

5.2. Graphic based methods

Graphic-based methods utilize standard image processing methods for analyzing visual features and image anomalies. The methods search for differences in the form of noise pattern, pixel-level difference, and other visual anomalies.

Shared Graphical Techniques:

Error Level Analysis (ELA): ELA detects inconsistencies in the error levels of the original and the forged image. Manipulated areas of an image have a varying error level from the neighboring areas when they are altered.

Noise analysis:

Seeks out abnormal patterns of noise since, as opposed to in original images, manipulated images typically have abnormal patterns of noise.

Pixel-Based Analysis: It evaluates the image by searching for irregularities in pixel values together with irregular pattern distributions and discontinuous changes in edge features texture and hue.

5.3. Learning based approaches

Automatic picture manipulation detection uses machine learning and deep learning methods which operate through machine learning-based approaches. The training process of machine learning models with extensive real images and fakings enables identification of distinctive patterns which signal image modification.

Shared Learning-Based Strategies:

Convolutional Neural Networks (CNNs): CNNs serve as a learning tool to automatically extract visual features between real images and generated images. CNNs learn hierarchical features in the format of convolutional layers.

Generative Adversarial Networks (GANs): GANs can be used for manipulation detection as well as manipulation

Detection models are trained to identify real and fake images by using generated fake samples.

Recurrent Neural Networks (RNNs): RNNs, especially Long Short-Term Memory (LSTM) networks, are able to scan time sequences between frames of video or sequential images for the purpose of detecting anomalies with time.

6. Active and Passive methods

Image forensics techniques organize themselves into two major groups known as active and passive forensics. LPR treats image recognition ability as its central principle along with advantages and disadvantages.

6.1 Active Techniques

Additional data introduced by active methods appears in images to serve as verification points at a later stage. The embedding process or normalization must occur at either image capture time or generation period.

Typical Active Techniques:

Digital watermarking:

The procedure known as digital watermarking enables insertion of an ID within an image-based watermark. This watermark may exist either visible to the eye or hidden if you wish. The selected embedded data gets extracted for authenticating purposes before a verification process occurs against the original data.

Digital Signatures:

An image obtains its digital signature through cryptographic processes.

6.2 Inactive Techniques

Passive systems do not necessitate any modifications to an image before application. The analysis of picture attributes helps establish alterations and manipulations through their detection methods.

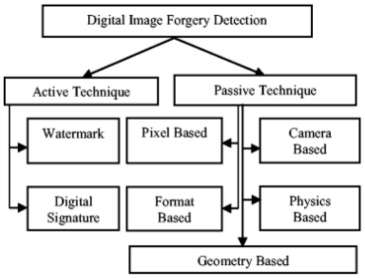
Typical Passive Techniques:

Error Level Analysis (ELA) detects differences between error levels of specific locations within an image that displays modification compared to its unmodified state. Normal areas of the image remain accurate when compared to other image sections while modifications will show increased inaccuracy levels.

The analysis of noise patterns in images under examination reveals any deviations through anomaly detection while authentic images tend to show regular noise consistency.

6.3 Image Forensics Methods:

The identification process uses multiple forensic techniques to detect differences between pixel quantities and compression artifacts and everything else that exists in the analysis.



7. Calculations

7.1 Error Level Analysis (ELA)

This technique would be used to look for variations in compression, suggesting manipulation. The key steps involve:

Calculate compression error: recompress each video frame and compare it to the original to find the error levels. Forged areas also typically display different levels of error than untouched sections.

Formula:

$$\text{Error Level} = \text{Original Frame} - \text{Compressed Frame}$$

7.2 Optical Flow Analysis

Optical flow is the pattern of apparent motion of objects in a video, it is the motion of object between two consecutive frames in a video. Inconsistent motion patterns may be a sign of forgery (if a manipulated region moves differently than its neighbor, for example).

The value of a pixel is calculated across two frames, with optical flow vector estimation

$$I(x,y,t)=I(x+u,y+v,t+1)$$

Where **I(x,y,t)** is the pixel intensity at position **(x,y)** and time *t*, and **(u,v)** is the estimated displacement between consecutive frames.

Inconsistent or abrupt motion indicates potential tampering.

7.3 Spatial Temporal Correlation Analysis:

Videos contain spatial (individual frame) and temporal (across frames) content.

After you can spot unnatural changes by studying the correlations either within frames (spatial) or between frames.

Spatial Analysis: Spatial correlation of neighboring pixels in all frames. Imperfect regions may show ebbs and flows of correlations based on the existence of foreign objects or edits.

Correlation calculation:

Spatial Correlation:

$$(\Sigma (X_i - \bar{X}) (Y_i - \bar{Y})) / sqrt (\Sigma (X_i - \bar{X}) ^2 \Sigma (Y_i - \bar{Y}) ^2)$$

Where XXX and YYY are pixel intensities in neighboring regions.

Temporal analysis: Compute correlations between frames over time. A sudden change in correlation could signal frame insertion deletion or swapping.

7.4 Video Hashing-based Integrity Verification

Video hashing is where you generate a hash value from the pixel/block data of each frame (or the entire video). Any change, even to one pixel, will result in a different hash, i.e., forgery.

Block-based hashing: Divide a frame into blocks and compute a single hash for each block.

Hashing function:

$$H(F) = \Sigma P(i,j) * W(i,j)$$

Where P(i,j) is the pixel at location (i,j) and W(i,j) is the weight at location (i,j). Hash comparison between different frames can detect frame-level forgery like duplication or deletion.

7.5 Deep Learning-Based Detection

Using deep learning, contemporary approaches detect forgeries by learning from data automatically. It contains the calculations of the feature extraction and classification.

CNNs Feature extractors extract spatial features from a video frame. The CNN learns the patterns of the forged images and extracts higher level features, making predictions based on these criteria.

The standard CNN feature extraction equation:

$$Z = ReLU(W * X + b)$$

Where X is input image, W are learned weights, b is bias and Z is output feature map.

Generative Adversarial Networks (GANs):

Forgery and forgery detection using GAN-based models. How a discriminator network learns the real from the generated forgeries

Discriminator Loss:

$$LossD = -E[\log D(x)] - E[\log(1 - D(G(z)))]$$

where D(x) is the discriminator's prediction for real input x, and G(z) is the output of the generator given random noise z.

7.6 Detecting duplicated and deleted frames

Video forgery methods Frame Replication or Removal (copy-pasting frames). Identification can include:

Frame similarity:

Use pixel-wise comparison methods or statistical measures (like Mean Squared Error or Structural Similarity Index) to identify frames within a video stream which are similar, or very similar.

Mean Squared Error (MSE) formula:

$$MSE = (1/n) \Sigma (I_{original}(i) - I_{modified} (i))^2$$

Where $I_{original}(i)$ and $I_{modified}$ are the pixel values of the original and manipulated frames, and n is the number of pixels.

Structural Similarity Index (SSIM):

$$SSIM(x,y) = [(2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2)] / [(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)]$$

Where μ_x and μ_y are the average pixel values, σ_x and σ_y are the variances, and σ_{xy} is the covariance between images x and y.

7.7 Auditory-Visual Synchronization Study

If the video was tampered with, the audio stream will not match the video content. It requires:
Audio-Video offset estimation: Find the audio track with audio-visual frame per second (FPS) as well as visual track which contains lip or motion that fades away when you listen to it.

Cross-correlation techniques can be applied for the mentioned purpose.

Cross-correlation calculation:

$$\mathbf{R_{xy}(t) = \Sigma\ x(n) * y(n + t)}$$

Where ***x(n)*** is the audio signal and ***y(n+t)*** is the video signal at time ***t***.

8. References

[1] B. Balas and C. Tonsager. Face animacy is not all in the eyes: Evidence from contrast chimeras. Perception, 43(5):355–367, 2014.

[2] M. Barni, L. Bondi, N. Bonettini, P. Bestagini, A. Costanzo,

M. Maggini, B. Tondi, and S. Tubaro. Aligned and nonaligned double jpeg detection using convolutional neural networks. Journal of Visual Communication and Image Representation, 49:153–163, 2017. 1

[3] B. Bayar and M. C. Stamm. A deep learning approach to universal image manipulation detection using a new convolutional layer. In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, pages 5–10. ACM, 2016. 1

[4] F. Chollet. Xception: Deep learning with depthwise separable convolutions. 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pages 1800–1807,2017. 5

[5] F. Chollet et al. Keras. https://keras.io, 2015. 5

[6] D. Erhan, Y. Bengio, A. Courville, and P. Vincent. Visualizing higher-layer features of a deep network. University of Montreal, 1341(3):1, 2009. 6

[7] S. Fan, R. Wang, T.-T. Ng, C. Y.-C. Tan, J. S. Herberg, and B. L. Koenig. Human perception of visual realism for photo and computer-generated face images. ACM Transactions on Applied Perception (TAP), 11(2):7, 2014. 3

[8] H. Farid. A Survey Of Image Forgery Detection. IEEE Signal Processing Magazine, 26(2):26–25, 2009. 1

[9] P. Garrido, L. Valgaerts, O. Rehmsen, T. Thormahlen, P. Perez, and C. Theobalt. Automatic face reenactment. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 4217–4224, 2014. 2

[10] S. Ioffe and C. Szegedy. Batch normalization: Accelerating deep network training by reducing internal covariate shift. arXiv preprint arXiv:1502.03167, 2015.

[11] Akanksha Gupta and Dilkeshwar Pandey , Unmasking the Illusion: Deepfake Detection through MesoNet , 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)

video forgery

ORIGINALITY REPORT

11%	8%	8%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.coursehero.com Internet Source	1%
2	Submitted to Hong Kong University of Science and Technology Student Paper	1%
3	Submitted to Higher Education Commission Pakistan Student Paper	1%
4	Submitted to Queen Mary and Westfield College Student Paper	1%
5	ijirt.org Internet Source	1%
6	Submitted to Arab Open University Student Paper	1%
7	dokumen.pub Internet Source	1%
8	Mi Chen, Rafael S. de Souza, Quanfeng Xu, Shiyin Shen et al. "Galmoss: A package for GPU-accelerated galaxy profile fitting", Astronomy and Computing, 2024 Publication	1%
9	Lecture Notes in Computer Science, 2016. Publication	<1%
10	www.mathaware.org Internet Source	<1%

11	V. Sharmila, S. Kannadhasan, A. Rajiv Kannan, P. Sivakumar, V. Vennila. "Challenges in Information, Communication and Computing Technology", CRC Press, 2024 Publication	<1 %
12	Submitted to Indian School of Mines Student Paper	<1 %
13	Submitted to Indiana University Student Paper	<1 %
14	repository.ntu.edu.sg Internet Source	<1 %
15	old.hartland.edu Internet Source	<1 %
16	"Artificial Neural Networks and Machine Learning – ICANN 2024", Springer Science and Business Media LLC, 2024 Publication	<1 %
17	Oluwatobi Adeleke, Sina Karimzadeh, Tien-Chien Jen. "Machine Learning-Based Modelling in Atomic Layer Deposition Processes", CRC Press, 2023 Publication	<1 %
18	actaenergetica.org Internet Source	<1 %
19	ar5iv.org Internet Source	<1 %
20	assets-eu.researchsquare.com Internet Source	<1 %
21	dspace.vut.cz Internet Source	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		