OPEN ACCESS Freely available online

ISSN: 2090-2697
Journal of
Forensic Biomechanics

Short Communication

Detection of Splicing Forgeries through Feature-Based Forensic Analysis

Matthew Cheng*

Department of Forensic Medicine, Fudan University, Shanghai, China

DESCRIPTION

In the world of digital media, the ease of manipulating images and videos has given rise to a significant challenge for forensic investigators-the detection of splicing forgeries. Splicing forgeries involve the manipulation of visual content by merging two or more separate image or video fragments to create a new, deceptive representation. To combat this growing problem, researchers and forensic experts have developed a feature-based forensic procedure that leverages advanced algorithms and techniques to detect splicing forgeries. This article delves into the concept of splicing forgeries and explores the key components of this feature-based forensic procedure [1].

Understanding splicing forgeries

Splicing forgeries are a type of digital manipulation technique where different fragments of visual content are combined to create a misleading or fraudulent representation. These forgeries can be used to alter the context of an image or video, create false evidence, or deceive viewers. Common examples of splicing forgeries include altering the background of a photo, adding or removing objects, or manipulating the appearance of individuals within an image [2].

The feature-based forensic procedure

The feature-based forensic procedure for splicing forgeries detection is based on the principle that when different fragments of an image or video are merged, subtle inconsistencies and artifacts are introduced. These inconsistencies can be identified by analyzing various features of the visual content, such as noise patterns, lighting conditions, edges, and color gradients. The procedure involves several steps, each aimed at extracting and analyzing specific features to uncover signs of splicing forgeries [3].

Pre-processing

The first step involves preparing the image or video for analysis. This includes removing any compression artifacts, resizing the content to a standardized resolution, and converting it to a suitable color space for further processing [4].

Noise analysis

Noise analysis plays a crucial role in identifying splicing forgeries. Different camera sensors and digital devices have unique noise patterns that can be used to determine if multiple fragments in an image have been merged. By examining noise residuals and noise distribution across the image, forensic experts can identify discrepancies that indicate splicing [5].

Illumination inconsistencies

Inconsistent lighting conditions are often present in spliced images or videos. The forensic procedure analyzes illumination features such as shadows, highlights, and overall brightness to identify unnatural variations within the content [6].

Edge and boundary analysis

When fragments are combined, edges and boundaries can exhibit unnatural discontinuities. The procedure identifies edge-based artifacts by examining abrupt changes in gradient, blurriness, mismatched sharpness. By analyzing the spatial relationship between different elements in the image, the forensic experts can pinpoint areas with inconsistent edges [7].

Color and texture analysis

Color and texture analysis is another essential component of the procedure. Splicing forgeries often introduce inconsistencies in color gradients and texture patterns. By comparing color histograms, texture descriptors, and statistical models of different regions, the forensic experts can identify areas that do not conform to the natural characteristics of the scene [8].

Compression analysis

Modern image and video formats employ compression algorithms that introduce specific artifacts. By analyzing compression-related features such as quantization tables, block

Correspondence to: Matthew Cheng, Department of Forensic Medicine, Fudan University, Shanghai, China, E-mail: Matthewheng@gmail.com

Received: 02-May-2023, Manuscript No. JFB-23-21639; **Editor assigned:** 05-May-2023, PreQC No. JFB-23-21639 (PQ); **Reviewed:** 19-May-2023, QC No. JFB-23-21639; **Revised:** 26-May-2023, Manuscript No. JFB-23-21639 (R); **Published:** 02-Jun-2023, DOI: 10.35248/2090-2697.23.14.443

Citation: Cheng M (2023) Detection of Splicing Forgeries through Feature-Based Forensic Analysis. J Forensic Biomech. 14:443.

artifacts, and compression noise, forensic experts can determine if an image or video has been manipulated [9].

Machine learning and pattern recognition

Machine learning algorithms and pattern recognition techniques play a crucial role in automating the detection process. By training models on a vast dataset of authentic and spliced images, these algorithms can learn to identify patterns and anomalies that are indicative of splicing forgeries. This allows for faster and more accurate detection of manipulated content [10].

CONCLUSION

The feature-based forensic procedure for splicing forgeries detection represents a significant advancement in the field of digital forensics. By leveraging advanced algorithms and analyzing various features of the visual content, forensic experts can detect splicing forgeries and expose fraudulent manipulations. As technology continues to advance, it is essential to stay at the forefront of forensic techniques to ensure the integrity and authenticity of digital media. The on-going development and refinement of feature-based procedures will play a crucial role in combating the ever-evolving challenges posed by digital manipulation.

REFERENCES

1. Kaur G, Malhotra S. A hybrid approach for data hiding using cryptography schemes. 2013; 4(8).
2. Paar C, Pelzl J. Understanding cryptography: a textbook for students and practitioners. 2009.
3. Luckett WM. Cellular automata for dynamic S-boxes in cryptography. 2007.
4. Toorani M, Falahati A. A secure variant of the Hill cipher.2009; 313-316.
5. Saeednia S. How to make the hill cipher secure. Cryptologia. 2000; 24(4):353-360.
6. Lin CH, Lee CY, Lee CY. Comments on Saeednia's improved scheme for the Hill cipher. J Chin Inst Eng. 2004;27(5):743-746.
7. Martínez-Ramos L, Mecate-Zambrano M, et al. How to repair the hill cipher. J Zhejiang Univ Sci. 2008; 9(2):211-214.
8. Thilaka B, Rajalakshmi K. An extension of hill cipher using generalised inverses and mth residue modulo n. Cryptologia. 2005; 29(4):367-376.
9. Gupta I, Singh J, Chaudhary R. Cryptanalysis of an extension of the hill cipher. Cryptologia. 2007; 31(3):246-253.
10. Biryukov A. Encyclopedia of cryptography and security. 2011.