TECHNIUM

Technium Vol. 4, No. 8 pp.18-22 (2022)
ISSN: 2668-778X
www.techniumscience.com

A Review for Video Authentication and Integrity

Rahma Nazar Ibrahim [1], Shahd Abdulrhman Hasso [2]

1 Software Engineering Department, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq
roraalhayali2@gmail.com
2 Software Engineering Department,College of Computer Science and MathematicsUniversity of Mosul, Mosul, Iraq
shahd_hasso@uomosul.edu.iq

Abstract: In daily life, digital video authentication is a crucial problem. Digital videos may be recorded or captured by many different devices, and these can all be sent through the internet and other unsecured means. Due to the advancement of video editing tools, there is an issue with the editing or changing of digital video without authorization. There are many different methods and techniques, which are suggested for overcoming these problems. Digital video is the fundamental of surveillance system. However, it is easy to be modified by threats that may decrease drastically the trust of surveillance system. The techniques used for video authentication by various authors are discussed in this study.

Keywords*: Digital Media; Video Integrity; Video Authentication*

I. INTRODUCTION

In the past few years, video authentication has continued to be a key topic that has drawn a lot of interest from researchers. By definition, digital video authentication is the process of evaluating whether or not the video that was captured is real but hasn't been altered. In just a few seconds, information may be sent fast over thousands of kilometers. This will have a significant impact on public growth and development. However, while the considerable advancement in information technology has brought forth a new generation of useful data, it has also added a few new information-related obstacles. [1]

People's lifestyles are altering due to digital media. Digital material is readily available to everyone and may be edited with files from a basic PC or mobile device. Modification is not permitted in surveillance systems that use digital video as their primary source, which significantly lowers the video's dependability [2].

a. Need for video authentication

Visual data can be changed by advanced processing tools without leaving any visual hint. To be hard is to have digital video that has already been transmitted, such as what has already been recorded. Except through the airport competing authentication technologies. [3]

b. Modifying video content

Tampering occurs when malicious changes are made to information that was produced by a person whose video had a specific sequence. This can be done for a variety of purposes, such as to undermine someone's moral character, to insult someone, or to obfuscate the information offered in the video [4].

Different levels of security are required for various video application types. For instance, low security is allowed for video on demand, while strong security is necessary to totally prohibit unauthorized access for military applications or financial data. To meet the needs of real-time applications, computational power means that the encryption or decryption procedure shouldn't add a lot of latency. Video compression is used in order to reduce storage space and bandwidth and ensure that the compression process is as efficient as possible.[4]

As with human authentication by a handwritten signature or letter authentication through a watermark on a letter, the authentication idea is based on identifying details that are used to assure the video integrity. There are two main components: the portion that creates identification information (auth) and the part that verifies identity information (ver) to assure information integrity. The important element is identifying information, often known as the signature, which should be difficult to copy in order to tell the original from copies. When using the authentication idea for video, the identification information should be durable enough to withstand compression, especially for content-based video authentication, and sensitive enough to manipulation that might identify fake videos.[5]

For a human viewer, realistic and carefully made video forgeries may go totally unnoticed, Since subjective examination cannot give sufficient confidence that the contents of a video are an actual and undamaged record of reality, specialized forensic procedures must be used in cases where a video might be used as evidence. The study application known as digital visual media forensics provides these specialist services.[6]

The authentication of multimedia data was first established in 1976 by Diffie and Hellman, but researchers are still quite interested in this area. Fragile watermarking and digital signatures have been employed in video authentication for a while, but both have been shown to have disadvantages.[7]

II. PROBLEM BACKGROUND

Attacks on and detection of video manipulation; When malicious changes are performed to a video, they either target the file's contents (the visual data that each frame of the video provides) or the timing relationship between the frames. [4]

One or more of the following are examples of video tampering [7]:

1. Insert a frame: This involves inserting one or more frames into the frame sequence.
2. Frame deletion: This refers to the removal of one or more frames from the sequence.

3. Frame shuffle: rearranging the frame order
4. Spatial manipulation involves altering the frame's content.

III. RELATED WORK

In this [1], we propose a new video authentication method. PLEXUS is a method for improving digital dependability and sporadic video assaults. There are two steps in this process. Basic actions Steps of authentication and verification In each instance, The two signatures, as well as the signature function, will be created. If the video is authentic, they will be compared and should match.

An improved approach for verifying the integrity of the videos is proposed in [2] using the watermark method. The technique isolates the header and time code hash values from the actual video data in order to distinguish between attacks and natural changes. According to the review research, the integrity check algorithm is superior to current methods that apply the concepts of a digital signature.

In [4] a proposed method for compressed video encryption was made available. Using this proposed algorithm, highly confidential video files might be sent safely so as to be protected from illegal viewing. By applying the compression technique to the video before the encryption, they achieve a balance between security and processing time since the compression method uses less bandwidth and less storage. Since the authors did not utilize steganography, data can be concealed within the movie's encryption frames to boost video security.

In [5], a method of improving digital video authentication in surveillance systems using a three-dimensional histogram of oriented gradient of chosen DCT (discrete cosine transform) coefficients was described. The effectiveness of this strategy depends on the appropriate threshold, which must be high in order to disregard any tampering. The outcomes of the experiment demonstrate that when applying a high threshold, modified footage is disregarded.

A novel method for digital video authentication that focuses on local video statistical data was made forth in [7]. SVM (Support Vector Machine) classifier has not been utilized in this strategy. However, this approach was found to be reliable and effective. The suggested technique was tested on a dataset of films, eight distinct attacks were entirely inserted into each video, and the system was shown to be 96.77 including on overall in categorizing the attacks.

In [8] approach for copy-paste forgery detection. Based on Histogram of Oriented Gradients (HOG) feature matching and video compression qualities. The advantage of utilizing HOG features is that they can withstand a variety of signal processing manipulations. For detecting purposes, frames with a good correlation between duplicated and genuine areas are selected.

An algorithm that aids in determining if the video has been manipulated is presented in [9]. Computing the repeated frames and computing the tampering attack are all the two steps that include the algorithm. In order to detect whether or not the digital video has already been tampered with, local information is discovered and the SVM classifier is effectively used.

In [10] Applying a symmetric encryption algorithm to the video encrypts it. The Least Significant Bits (LSB) method used in steganography hides the signature in the lower bits of picture pixels. According to the results of simulations, this technique shortens the time needed to encrypt videos with the highest security level and privacy

In [11] The correlation between every pair of neighboring frames and their combination with the first frame's location is selected randomly. Before being joined, related transactions are encrypted with the AES method. While preserving high quality optical frames, several attacks between and within frames go uncovered by analysis.

In [12] A. used Discrete Wavelet Transform (DWT) to compress the video as it was being sent or stored over the network. The results acquired decreased the size of the movie and the transmission time. An effective compression strategy may be carried out using the DWT method. High-level security can also be managed with video encryption.

In [13], in real life, steganography is a crucial duty when users wish to keep their data private. Traditional text-and image-based steganography techniques run into problems when they are not widely available. They can only transport tiny files. So the issue is how to obtain enough files to conceal our message. When you have a lot of data to carry, this activity gets quite tiresome. Here, video steganography is required. The capacity issue can be solved by using video as a transmission cover for the secure message. Every video frame has information that may be concealed. This indicates that the video can store a lot of data.

They conceal data within the movie using the steganography technique described in [14]. The Least Significant Bit (LSB) approach was employed, which is thought to be a good method for concealing all of the message's characters inside the video's frame design. These images were chosen at random.

An algorithm focused on two things was suggested by IN [15]. SVM learning comes first, followed by tamper detection and classification using SVM, though because SVM and a video database are used, this suggested technique is computationally expensive and a little bit slow.

A hybrid forensic system was created in [16] for the purpose of detecting frame insertion, removal, and replication. The method detected errors caused by post-production frame tampering in the brightness gradient component of optical flow in order to detect frame insertion and removal. By examining the anomalies in the expected residual patterns of forged films, frame-replication forgeries were discovered and localized.

IV. CONCLUSION

Various video tampering attacks, such as spatial and temporal tampering, are discussed in this work. Many videos forgery detection and authentication procedures and strategies have been addressed in relation to the above studies. Since there are several ways to tamper with videos, there should also be various ways to detect videos. There is no ideal detection technique for every circumstance. Therefore, the best video forgery detection technique depends on a variety of factors, including video forgery techniques, available technology, computational constraints, video quality, and video formats.

ACKNOWLEDGEMENTS

I would like to thank the Software department at the University of Mosul for all the support provided. I am also grateful to Dr. Dujan Basheer Taha for her collaboration during this work.

REFERENCE

[1] ABDULWAHAB, Hala Bahjat; HAMEED, Khaldoun L.; BARNOUTI, Nawaf Hazim. Video Authentication using PLEXUS Method. *(ijacsa) International Journal Of Advanced Computer Science And Applications*, 2018, 9.11.

[2] I. Echizen, S. Singh, T. Yamada, K. Tanimoto, S. Tezuka, and B. Huet, ''Integrity verification system for video content by using digital watermarking,'' in Proc. Int. Conf. Service Syst. Service Manage., vol. 2, Oct. 2006, pp. 1619–1624.

[3] PARMAR, Zarna; UPADHYAY, Saurabh. A review on video/image authentication and temper detection techniques. International Journal of Computer Applications, 2013, 63.10.

[4] KULKARNI, Ajay, et al. Proposed video encryption algorithm v/s other existing algorithms: A comparative study. *arXiv preprint arXiv:1303.3485*, 2013.

[5] Kroputaponchai, Teerasak, and Nikom Suvonvorn. "Video authentication using spatio-temporal signature for surveillance system." In Computer Science and Software Engineering (JCSSE), 2015 12th International Joint Conference on, pp. 24-29. IEEE, 2015.

[6] SINGH, Raahat Devender; AGGARWAL, Naveen. Video content authentication techniques: a comprehensive survey. *Multimedia Systems*, 2018, 24.2: 211-240.

[7] Al-Athamneh, Mohammad, Fatih Kurugollu, Danny Crookes, and M. Farid. "Video authentication based on statistical local information." In Utility and Cloud Computing (UCC), 2016 IEEE/ACM 9th International Conference on, pp. 388-391. IEEE, 2016

[8]. Subramanyam, A. and S. Emmanuel. Video forgery detection using HOG features and compression properties. in Multimedia Signal Processing (MMSP), 2012 IEEE 14th International Workshop on. 2012. IEEE.

[9] Gupta, Ankita, Shilpi Gupta, and Anu Mehra. "Video authentication in digital forensic." In Futuristic Trends on computational analysis and knowledge management (ABLAZE), 2015 International Conference on, pp. 659-663. IEEE, 2015.

[10] MOHSEN, Asmaa Hasan; SHAKER, Shaimaa Hameed. Authentication of Digital Video Encryption. Iraqi Journal of Science, 2016, 2954-2967.

[11] A HASSO, Shahd; B TAHA, Taha. A New Tamper Detection Algorithm For Video. Journal of Engineering Science and Technology (JESTEC), 2020, 15.5: 3375-3387.

[12] Al-Ani, M. S.and Hammouri, T. A. 2011. Video Compression Algorithm Based on Frame Difference Approaches. International Journal on Soft Computing (IJSC), 2(4), pp: 67-79.

[13] KAUR, Jas; KAUR, Jagroop. Hiding Text in Video Using Steganographic Technique-A Review. International Journal of Engineering Sciences, 2016,

[14] SWATHI, A.; JILANI, S. A. K. Video steganography by LSB substitution using different polynomial equations. *International Journal of Computational Engineering Research*, 2012, 2.5: 1620-1623.

[15] S. Upadhyay and S. K. Singh, "Learning based video authentication using statistical local information," Image Information Processing (ICIIP), 2011 International Conference on, Himachal Pradesh, pp. 1-6 , 2011.

[16] Singh, R.D., Aggarwal, N.: Detection of Re-Compression, Transcoding and Frame-Deletion for Digital Video Authentication. In: Proceedings of 3rd International Conference on Recent Advances in Engineering and Computer Sciences. Chandigarh India,

Submitted: 03.07.2022
Revised: 15.08.2022
Accepted: 23.08.2022