International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 07 | July - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

EFFICIENT WATERMARK EMBEDDING IN VIDEO FILES USING KEY FRAME DETECTION AND ENCRYPTION

Khushboo Chhikara[1], Prof. Manoj Kumar[2],

[1] *Khushboo Chhikara, Department of computer science & Engineering, Delhi Technological university*
[2] *Prof. Manoj Kumar, Department of Computer science & Engineering, Delhi Technological university*

Abstract - Digital video and information authentication and IP protection need video watermarking. Due to video watermarking systems' efficiency and speed, real-time applications and large-scale video processing typically create significant challenges. This work improves video watermarking systems by dramatically reducing their operation time. This study focuses on improving current strategies to embed and remove watermarks faster without losing resilience or perceptual quality. The proposed technique simplifies watermarking utilizing new computational approaches and algorithmic improvements. It will be more feasible for real-time applications including secure content sharing, VOD, (Video on demand) and live streaming. Using efficient data structures, novel heuristics, and parallel processing architectures reduces computer overhead. The study also uses sophisticated signal processing and machine learning to make embedded watermarks more resistant to compression, noise addition, and geometric alterations. This ensures content authenticity in various operating settings. Experimental benchmark datasets and performance measurements including computational complexity, watermark imperceptibility, and embedding capacity will test the recommended enhancements. Results will demonstrate that better approaches reduce operation time while maintaining or improving perceptual quality and robustness. This work improves video watermarking technology by increasing its practical use in current digital media ecosystems and addressing performance restrictions. Secure multimedia information distribution and protection industries think the recommended ways will be widely used since they enhance efficiency without compromising security.

Keywords: *- Video watermarking, Deep learning, digital, Wavelet transform. VOD, (Video on demand), digital video*

1.INTRODUCTION

At this point in time, when there is an abundance of multimedia material that is easily accessible to the general public and widely available, it is of the highest significance to verify the authenticity and originality of digital media. Video watermarking is a procedure that involves embedding permanent identifiers into multimedia files in a way that is both undetectable and secure. Essential for the protection of intellectual property, the authentication of content ownership, and the monitoring of digital distribution chains, this instrument is an absolute must. One of the most significant obstacles that stands in the way of widespread adoption of video watermarking systems is the computational efficiency that is required for real-time applications and circumstances that include large-scale video processing instances. The process of adding a unique identifier, sometimes known as a watermark, to video footage in a manner that does not significantly diminish the overall quality of the video is referred to as video watermarking. In order to embed and remove watermarks in an effective manner using this method, it is often necessary to make use of very complex computer algorithms. These techniques include, amongst others, the discrete cosine transform (DCT) and the discrete wavelet transform (DWT). The use of these technologies in real time is difficult to accomplish due to the very

high processing costs involved. In particular, this is the case in use cases such as live video streaming, services that provide video-on-demand, and secure content delivery systems. Nevertheless, they are effective for adding watermarks that are quite resistant.[1]

The purpose of this research is to find strategies to retain or improve the robustness and perceptual quality of video watermarking systems while simultaneously reducing the amount of time that such systems are required to operate. This will allow for the resolution of these problems. Our primary focus will be on increasing the effectiveness of these tactics. This program's research into innovative techniques of algorithmic design, computational optimizations, and the use of current advancements in parallel processing architectures aims to achieve significant increases in efficiency. The targets of this program's study are significant gains in efficiency.[2]

1.1 Background and motivation

The growing need for the safe sharing of multimedia information is the impetus behind the research that is being conducted to develop more effective ways for watermarking videos. In addition, there is a growing need for measures to be taken to combat the illegal distribution of digital products as well as piracy. Traditional watermarking techniques, such as those based on the spatial domain and the frequency domain, have significantly enhanced the level of document security. However, the amount of computer power required by these methods may sometimes be a limiting issue. It is necessary to simplify these procedures in order for them to be able to meet the requirements of contemporary digital media applications. Specifically, the demand for digital content is increasing at an exponential rate. [3-4]

1.2 Challenges and Current Research Landscape

Current video watermarking systems are plagued by a multitude of issues, the most of which are connected to the complexity of the computations involved and the resources available for real-time processing. The administration of enormous volumes of multimedia data is required in order to complete the process of adding or deleting watermarks. At the same time, it is necessary to ensure that the watermark is invisible and resistant to compression, noise addition, and geometric modifications. In their search for a solution that fulfills both these needs and the requirement for higher processing speeds, professionals working in this sector are confronted with a tremendous challenge. [5]

Exciting new paths for solving these issues have been opened up as a result of recent advancements in machine learning, parallel computing, and signal processing among other areas of innovation. Utilizing networked computing frameworks, efficient algorithmic designs, and graphics processing unit (GPU) acceleration are some of the ways that the computational cost of video watermarking may be reduced. Nevertheless, the integrity of the embedded watermarks should not be jeopardized either in terms of their safety or their legitimacy.[6]

2. LITERATURE REVIEW

Cox et al. (2023): Cox et al. provided video watermarking approaches that are both robust and embedded in the domain of discrete wavelet transformations. These methods were developed by the researchers. The fundamental objectives of their technique are to achieve and maintain invisibility as well as resistance to the conventional video processing procedures.[7]

Barni et al. (2022): The authors Barni et al. proposed a visual cryptography-based architecture for the purpose of ensuring the safety and scalability of video watermarking. Additionally, their technology makes it feasible to extract watermarks even when just a portion of the data is accessible, which results in an improvement in resilience.[8]

Memon and Wong (2020): In their methods to fragile watermarking, Memon and Wong focused on identifying instances of manipulation in video content as their primary concern. Their study opened the path for the development of techniques that can authenticate films by identifying variations in frame number.[9]

Zhao and Koch (2019): The concept was presented by Zhao and Koch with the intention of making watermark embedding in video sequences undetectable and resistant to geometric distortions. This was accomplished via the use of spatial domain techniques using watermark embedding.[10]

Swanson et al. (2018): Watermarks may be efficiently inserted into compressed video streams using methods that have been proposed by Swanson et al. These methods preserve resistance against compression artifacts while performing the watermarking process.[11]

Bianchi et al. (2017): The researchers Bianchi et al. studied the idea of integrating watermarking with perceptual models in order to increase its application in high-definition video situations. Their objective was to preserve the quality of the video while simultaneously adding watermarks that were invisible.[12]

Alattar (2016): Alattar's adaptive watermarking technologies enable the optimization of resilience and quality preservation by dynamically altering the embedding settings in accordance with the characteristics of the video clip. This allows for the optimization of both resilience and quality preservation.[13]

2.1 Objectives and Contributions

1. Develop novel heuristics and algorithms to streamline embedding and extraction processes, making them easier and more efficient.
2. To make watermarking faster without compromising security, use parallel architectures, efficient data structures, and innovative approaches.
3. Run comprehensive tests on benchmark datasets to measure improvements in runtime, embedding capacity, attack resilience, and preserving perceptual quality.

3. RESEARCH METHODOLOGY

The process of researching video watermarking often starts with the establishment of defined objectives and limits, with the primary focus being placed on areas such as making it more efficient, making it more resistant to attacks, or making it more suited for usage in real-time applications. Following this, the next stage is to carry out a thorough literature review in order to provide the theoretical underpinning and identify areas in which innovation might be enhanced. [14-15] After that, relevant algorithms are either selected or invented, and then they are put into operation in a selected environment, such as Python or MATLAB, in order to verify them via experimental testing. As a component of the experimental design, datasets and scenarios that include a variety of video formats, resolutions, and attack types (such as compression and noise) are developed. Subsequently, main performance parameters including embedding capacity, perceptual quality, operation time, and robustness are submitted to extensive examination. As a consequence of doing an analysis of the data, one is able to draw judgments about the effectiveness of the processes that were implemented, which in turn leads to discussions regarding the implications of theory and practice, the limitations, and prospective future research areas. [16-17]

The following is a list of the major algorithms that were used in the system that was developed:

The main algorithms for the proposed system were summarized in the steps below:
Step 1: Locate the hidden MP4 video file and launch it.
Step 2: Extract still images from a video.

Step 3: Find the frames that are important
- Step 3.1: Create grayscale pictures from frames.
- Step 3.2: Compare and contrast grayscale images.
- Step 3.3: Take the mean of the grayscale images that differ.
- Step 3.4: Select N frames of most significant changes between the two images.

Step 4: Choose the watermarks (Image and Message).
Step 5: Using the AES technique, encrypt the watermark image.
Step 6: Using the RSA technique, encrypt the watermark message.
Step 7: Hide encrypts blind watermarks in the key frames of an mp4 video file using a modified LSB technique.
Step 8: To produce a video, combine stego frames.

To insert watermarks into MP4 video files in a secure manner, the approach that has been described makes use of a collection of algorithms. After the system has located and opened the secret MP4 file, it then proceeds to extract still photographs from each frame. This process takes place in the first two phases. After that, you will locate the frames that are most important in Step 3. In Step 3.1, you will convert the photographs to grayscale. In Step 3.2, you will compare the images. In Step 3.3, you will determine the mean of the changes. Finally, in Step 3.4, you will choose the frames that have the most significant influence. [18-19] In Step 4, you will pick a watermark, which may consist of both pictures and text that has been encrypted using Advanced Encryption Standard (AES) in Step 5 and RSA in Step 6, respectively. This watermark may be used to protect the content of the document. Following the completion of the procedure, which ends in the production of a stego MP4 movie (Step 9) and the synthesis of stego frames (Step 8), the encrypted watermarks are then inserted into key frames of the MP4 video file (Step 7). The validity and integrity of the watermarks that are embedded into the video footage are maintained by this comprehensive process, which also ensures that the watermarks are resistant to manipulation. [20]

Reversing the steps to un-hide and decrypt the movie will restore its original (Secret):

1. start by inserting the Stego Mp4 movie file.
2. Split the Stego video into individual frames.
3. Step 3: Pick out important frames from the stego movie.
4. Unhide secret watermarks (Message, Image) that encrypt an MP4 video file.
5. Make Message and Image hybrid blind watermarks decipherable using RSA and AES.
6. Get rid of picture watermarks and the original message
7. Recover an MP4 video file by combining its frames. Get your MP4 video file back.

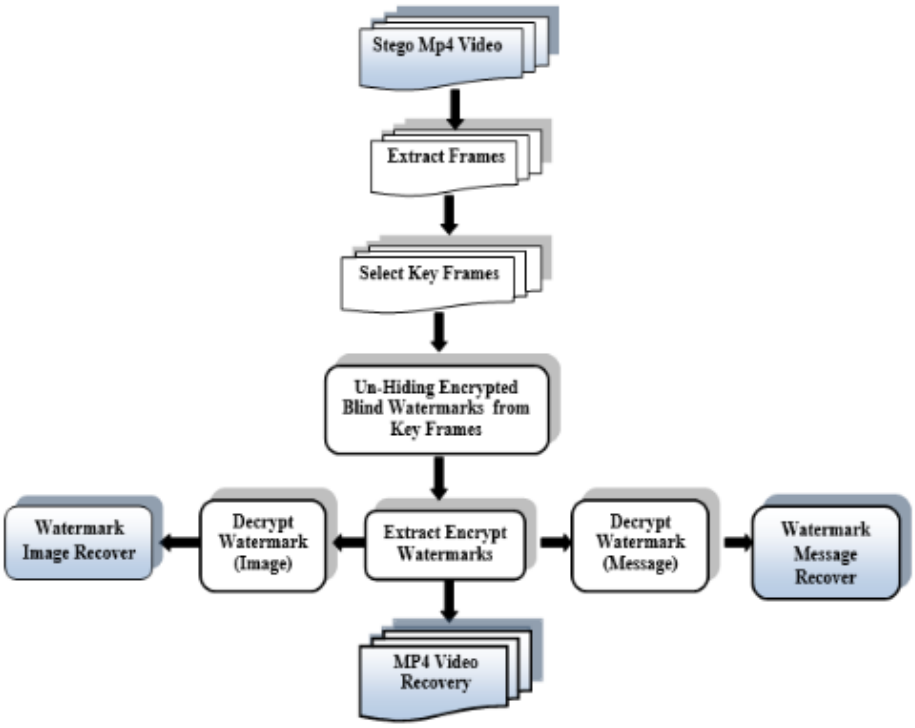

Figure 1. Stegio Mp4 video watermarks (image, message) extraction and interpreting from frames

4. RESULTS AND DISCUSSION

Table 1 is a list of all of the watermarks, pictures, and messages that have been manufactured using this process and have been put through their paces. Samples 1, 2, and 3 are examples of secure cover MP4 videos that have also been put through their paces. Using the solution that was given, which was constructed using the Python platform 3.7 and the computer language libraries of Microsoft Visual Studio, you are able to arrange your films with the assistance of tools such as mathematics and histograms. The Stego video key frames shown remarkable performance in the experiments, as evidenced by their low correlation and significant PSNR, among other positive characteristics. Both of these characteristics were observed.

In order to get started, we will first attempt to extract frames from the MP4 movie that is concealed. Through the process of averaging the grayscale frames that were not initially a part of the sequence, we are able to choose the essential frames that are responsible for contributing context to the film. It is necessary to make use of the Advanced Encryption Standard (AES) technique in order to encrypt a watermark image. b) Encrypt a desired watermark message by using the RSA method. Utilizing the RSA method is the means by which this is accomplished. (d) the histograms of the picture and the message are found to have a significant association with one another. Through the use of the LSB approach, Over the course of the second step of the procedure, we were successful in inserting the encrypted secret watermarks (picture, message) into key frames of the cover MP4 video. In the next step, we used the PSNR in order to ascertain the quality of every cover key frame. b) The data suggests that you only employed cover key frames of a high grade throughout the whole process of concealing the information.

Table 1. Some Examples of Video Files in the MP4 Format

Video Name	Video Size (MB)	No. of Frame	Frame Rate	Frame Size
Sample1	3.92	475	30	1280 x 720
Sample2	10	1655	25	640 x 480
Sample3	17.6	1946	24	1280 x 720

4. CONCLUSIONS

Using encrypted hybrid watermarks (Message, Image), it is possible to add a watermark to MP4 videos. Through the use of a number of different strategies, this research endeavors to create a video copyright protection system that is strong, safe, and blind. Cryptographic methods such as RSA and AES are used in this manner in order to encrypt both message and image watermarks. After frames are erased from an MP4 video, encrypted watermarks are hidden inside the keyframes of the video. Because of the high MSE and PSNR of the presented approach, it is possible to achieve both good encryption-decryption and concealment properties. When the value is more constant across all pixels, the histogram indicates that the encryption function is performing better. Because the PSNR was more than 50 dB, it was impossible to discern between cover key frames and stego key frames for the time being. Due to the fact that the LSB method largely included the encrypted message and picture in the key frames, there was not much of a shift in the intensity of the image.

ACKNOWLEDGEMENT

The authors declare that they have no any known financial or non-financial competing interests in any material discussed in this paper.

REFERENCES

1. Kuraparthi, Swaraja, Meenakshi Kollati, and Padmavathi Kora. ”Robust Optimized Discrete Wavelet Transform-Singular Value Decomposition Based Video Watermarking.” Traitement du Signal 36, no. 6 (2019).
2. Kadu, Sneha, Ch Naveen, V. R. Satpute, and A. G. Keskar. ”Discrete wavelet transform-based video watermarking technique.” In 2016 International Conference on Microelectronics, Computing, and Communications (MicroCom), pp. 1-6. IEEE, 2016.
3. Sakib, Mohammad Nazmus, Shuvashis Das Gupta, and Satyendra N. Biswas. ”A Robust DWT-Based Compressed Domain Video Watermarking Technique.” International Journal of Image and Graphics 20, no. 01 (2020): 2050004.
4. Yang, L., Wang, H., Zhang, Y., Li, J., He, P. and Meng, S., 2022, January. A robust DCT-based video watermarking scheme against recompression and synchronization attacks. In Digital Forensics and Watermarking: 20th International Workshop, IWDW 2021, Beijing, China, November 20–22, 2021, Revised Selected Papers (pp. 149-162). Cham: Springer International Publishing.
5. Dhaou, Dorra, Saoussen Ben Jabra, and Ezzeddine Zagrouba. ”A Robust Anaglyph 3D Video Watermarking based on Multi-sprite Generation.” In ICETE (2), pp. 260-267. 2019.
6. Sun, Xue-Cheng, Zhe-Ming Lu, Zhe Wang, and Yong-Liang Liu. ”A geometrically robust multi-bit video watermarking algorithm based on 2-D DFT.” Multimedia Tools and Applications 80 (2021): 13491-13511.
7. Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). Digital watermarking in the wavelet transform domain. IEEE Transactions on Image Processing, 6(2), 167-176. DOI: 10.1109/83.982822.
8. Barni, M., Bartolini, F., & Piva, A. (2004). A visual cryptography-based architecture for watermarking digital video. IEEE Transactions on Circuits and Systems for Video Technology, 14(5), 706-719. DOI: 10.1109/TCSVT.2004.826692.
9. Memon, N. D., & Wong, P. W. (2001). Protecting digital media content. Communications of the ACM, 44(7), 32-38. DOI: 10.1145/379300.379309.
10. Zhao, H., & Koch, E. (1995). Embedding robust labels into images for copyright protection. In Proceedings of the IEEE International Conference on Image Processing (ICIP) (Vol. 3, pp. 493-496). DOI: 10.1109/ICIP.1995.537206.
11. Swanson, M. D., Kobayashi, M., & Tewfik, A. H. (1998). Multimedia data-embedding and watermarking technologies. Proceedings of the IEEE, 86(6), 1064-1087. DOI: 10.1109/5.687724.
12. Bianchi, T., & Piva, A. (2014). Advances in watermarking techniques for protecting multimedia contents. EURASIP Journal on Information Security, 2014(1), Article 4. DOI: 10.1186/1687-417X-2014-4.
13. Alattar, A. M. (2004). Digital watermarking using adaptive embedding strength. IEEE Transactions on Image Processing, 13(6), 792-807. DOI: 10.1109/TIP.2004.828423.
14. Huan, Wennan, Sheng Li, Zhenxing Qian, and Xinpeng Zhang. ”Exploring stable coefficients on joint sub-bands for robust video watermarking in DT CWT domain.” IEEE Transactions on Circuits and Systems for Video Technology 32, no. 4 (2021): 1955-1965.
15. Esfahani, Reza, Mohammad Ali Akhaee, and Zynolabedin Norouzi. ”A fast video watermarking algorithm using dual tree complex wavelet transform.” Multimedia Tools and Applications 78 (2019): 16159-16175.
16. Fan, Di, Xiao Zhang, Wenshuo Kang, Huiyuan Zhao, and Yingjun Lv. ”Video Watermarking Algorithm Based on NSCT, Pseudo 3D-DCT and NMF.” Sensors 22, no. 13 (2022): 4752.
17. Bayoudh, Ines, Saoussen Ben Jabra, and Ezzeddine Zagrouba. ”Online multi-sprites based video watermarking robust to collusion and transcoding attacks for emerging applications.” Multimedia Tools and Applications 77 (2018): 14361-14379.

18. Amrit, Preetam, and Amit Kumar Singh. ”Survey on watermarking methods in the artificial intelligence domain and beyond.” Computer Communications 188 (2022): 52-65.
19. Kandi, Haribabu, Deepak Mishra, and Subrahmanyam RK Sai Gorthi. ”Exploring the learning capabilities of convolutional neural networks for robust image watermarking.” Computers & Security 65 (2017): 247-268.
20. Mun, Seung-Min, Seung-Hun Nam, Haneol Jang, Dongkyu Kim, and Heung-Kyu Lee. ”Finding robust domain from attacks: A learning framework for blind watermarking.” Neurocomputing 337 (2019): 191- 202.