WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Video Watermarking Scheme Based on Counting Secret Sharing

***Bindeshwar Prasad Sah*[1], *Botta Darshan*[2], *Anesetti GaneshVenkat*[3], *Dr. S. Prasanth Vaidya*[4]**

[1,2,3]Department of CSE, Aditya Engineering College Surampalem
[4]Associate Professor, Aditya Engineering College Surampalem

ABSTRACT

Video watermarking is the process of embedding a unique identifier or signal, known as a watermark, into a video. The watermark is typically invisible to the naked eye and can serve multiple functions including safeguarding copyrights, verifying ownership, and authenticating content. In this project, we implement two watermarking techniques, Least Significant Bit (LSB) and Count-Based Secret Sharing (CBSS), to embed and extract watermarks from videos.

The LSB method refers to the process of substituting the least significant bit of every pixel present in the video frames with a corresponding bit extracted from the watermark. This technique is simple and fast but can be easily detected and removed. CBSS, on the other hand, is a more robust and secure technique that involves dividing the video frames into sampling blocks and generating shares for each block. These shares are then combined to reconstruct the watermark during extraction.

The project includes a Python implementation of the LSB and CBSS techniques and a graphical user interface (GUI) that allows users to select a video file, embed a watermark, and extract a watermark. The GUI also provides options to adjust the embedding strength and enter a password for the watermark, which enhances security. The project also includes a performance evaluation of both techniques, which compares their efficiency, robustness, and security.

In general, this project showcases the implementation of watermarking methods for safeguarding video content and offers a valuable resource for those involved in creating, distributing, and consuming such content.

Keywords: *Watermarking, Digital image processing, LSB(Least Significant Bit), CBSS (Count-based Secret Sharing), Video processing, Authentication, Data hiding, Robustness, Security, and Steganography*.

1. INTRODUCTION

"Video watermarking refers to the method of inserting a distinctive marker or watermark into a video to safeguard its copyright, authenticate its content, and detect any tampering. A range of techniques can be employed for watermarking, including the Least Significant Bit (LSB) and Count-based Secret Sharing (CBSS), which will be utilized in this project."

The LSB technique is a popular and simple method of embedding a watermark into an image or video. In this technique, the least significant bits of the pixel values are replaced with the bits of the watermark, thus making minimal changes to the original image or video.

CBSS is a technique used to split a secret into multiple shares, such that the secret can only be reconstructed if a minimum number of shares are combined. This technique is useful for watermarking because it allows us to split the watermark into multiple shares and embed each share into different parts of the video. The presence of a watermark makes it challenging for an intruder to eliminate it.

Watermark Embedding:

In the process of embedding a watermark, the first step involves converting the watermark into a binary format and split it into equal shares using CBSS. Then, we select random frames in the video and embed each share of the watermark into different parts of the frame using LSB. Finally, we save the watermarked frames back into the video file.

Watermark Extraction:

In the watermark extraction process, we read the watermarked video file and select the same frames used for embedding. Then, we extract the LSBs of each part of the frame and combine them to reconstruct the shares of the watermark. Finally, we combine the shares to reconstruct the original watermark and compare it with the expected watermark to verify the authenticity of the video.

Verification:

To ensure the authenticity of the extracted watermark, we generate a hash of the reconstructed watermark and compare it with the hash of the original watermark. If the hashes match, then we can be confident that the watermark was not tampered with during extraction. We also compute the percentage of matching between the reconstructed hash and the original watermarking ID to indicate the verification strength.

2. LITERATURE REVIEW

Watermarking is a widely used technique to safeguard multimedia content from unauthorized reproduction and distribution. To watermark a video, the LSB technique is a popular choice among the available methods. In this method, the least significant bits of each pixel in the video frames are modified to embed the watermark information. However, this method is vulnerable to attacks and can easily be removed by an attacker.

To overcome the limitations of the LSB technique, a new technique called Count-Based Secret Sharing (CBSS) has been proposed. CBSS is a steganographic method that divides the video frames into blocks and generates random shares for each block. The shares are then distributed across the video frames in a way that makes them difficult to detect or remove. To retrieve the watermark embedded within a video, the shares are combined using a reconstruction algorithm. CBSS is more robust against attacks than the LSB technique.

Several studies have been conducted to improve the performance of CBSS. One study proposed a new method called Extended CBSS (ECBSS), which uses a more sophisticated sharing scheme to improve the robustness of the watermark. Another study proposed a method called Adaptive CBSS (ACBSS), which dynamically adjusts the sharing scheme by analyzing the visual content of the video frames. Apart from CBSS, other techniques such as Discrete Wavelet Transform (DWT) and an approach for video watermarking involve the use of Singular Value Decomposition (SVD) as well. DWT is a method that transforms the video frames into a frequency domain and embeds the watermark in the high-frequency coefficients. SVD is a method that decomposes the video frames into singular values and embeds the watermark in the singular values.

Overall, video watermarking is an important technique for protecting multimedia content from unauthorized duplication and distribution. The LSB technique and CBSS are two commonly used methods for video watermarking. CBSS is a more robust technique than the LSB technique, and several studies have been conducted to improve its performance. Other techniques such as DWT and SVD have also been proposed for video watermarking, and their performance should be further investigated.

3. PROPOSED METHOD

The proposed video watermarking system utilizes a CBSS is a cryptographic technique used to securely share a secret among group of participants it can be used to generate watermarking bits that are embedded in the video file for semi-complete verification. This technique is similar to that used in steganography. To use the system, the user selects a watermarking ID (password) that serves as the target key (TK) for the CBSS system. This is a departure from the original random TK generation method.

The system then generates shares as a watermarking-bits stream through a 1-bit shares generation phase. To insert a watermark, a sequence of bits is added to the video file. This process involves embedding the watermarking bits into the video data to store the watermarking bits. The embedding process includes the conversion of shares, which will be extracted later during the watermarking-bits extraction phase for verification.

During the extraction phase, the CBSS system is utilized to recover the TK shadows from the watermarked video by randomly selecting various video frames that are grouped under a k threshold. The selected pixels of the video are then used to retrieve the TK shadows through the CBSS method. The system cross-checks the TK shadows with the TK (which serves as a watermarking ID) in order to determine the degree of watermarking verification, expressed as a percentage.

Please note that not every combination of TK-shadows shares may result in the correct TK, and therefore, the percentage of verification for watermarking could differ. For more information on the processes of watermarking embedding and extraction, as well as the simulation strategy, please refer to the project documentation.

4. CONCLUSION

To summarize, watermarking is an effective method for safeguarding the copyrights of digital content. In this project, we have explored the process of embedding and extracting a watermark in a video using Python and OpenCV. We have used the LSB method to embed the watermark in the video frames and the CBSS method to retrieve the watermark embedded in the video frames. The implemented system is robust and can resist various attacks, including compression, noise addition, and filtering.

Watermarking is an effective way to protect the intellectual property rights of video content. The LSB watermarking technique used in this project has shown good results in terms of imperceptibility and robustness to various attacks.

The CBSS system has been implemented successfully to remove the watermark embedded in the video. The project has yielded significant findings regarding the video watermarking procedure and the significance of selecting appropriate methods that align with the application's specific requirements.

The watermark embedding and extraction process has been demonstrated using a sample video file. The embedding process involved selecting a password, encoding the password into a binary format, and embedding the password into the video frames using the LSB method.

The extraction process involved reading the video frames, extracting the embedded password, and verifying the password's correctness using the CBSS method. The percentage of verification has been computed, indicating the accuracy of the extraction process.

The outcomes of the project illustrate that the utilization of watermarking is a feasible approach to safeguard digital media from copyright infringement. The implemented system can help protect the owner's rights by identifying and tracing illegal copies of the original media.

5. REFERENCES

Abu-Hashem and Gutub (2022) developed a novel approach for computing hash Hirschberg protein alignment in an efficient manner. The technique utilizes hyper-threading and multi-core sharing technology to improve performance. This research is published in CAAI Transactions on Intelligence Technology.

https://scholar.google.co.in/scholar?q=https://doi.+org/10.1049/cit2.12070&hl=en&as_sdt=0&as_vis=1&oi=scholart

Almazrooie, Samsudin, Gutub, Salleh, Omar, and Hassan (2020) proposed a method for ensuring the integrity of digital Holy Quran verses. This method involves utilizing a cryptographic hash function and compression. The study was published in the Journal of King Saud University - Computer and Information Sciences, volume 32, issue 1, pages 24-34.

https://www.sciencedirect.com/science/article/pii/S1319157817305232?via%3Dihub

Almehmadi and Gutub (2022) propose a new method for watermarking Arabic e-text that supports partial dishonesty, utilizing a counting-based secret sharing approach. This method is discussed in the Arab Journal of Science and Engineering.

https://link.springer.com/article/10.1007/s13369-021-06200-7

Al-Nofaie, Gutub, and Al-Ghamdi (2019) have proposed improvements to Arabic text steganography for personal use by incorporating pseudo-spaces. Their research is currently pending publication in the Journal of King Saud University-Computer and Information Sciences.

https://doi.org/10.1016/j.jksuci.2019.06.010

Tran, T., Luong, H. V., & Nguyen, T. T. (2021). Efficient Robust Video Watermarking Using Dynamic Salient Regions Detection and Selective Embedding. Journal of Information Security and Applications, 62, 102843. https://www.sciencedirect.com/science/article/pii/S221421262100079X?via%3Dihub

"A Robust Watermarking Algorithm for Video Based on Singular Value Decomposition and DNA Encoding" authored by Wu, Y., Gao, Y., and Zou, J. in 2020 and published in the Journal of Ambient Intelligence and Humanized Computing explores the development of a secure and reliable method of watermarking videos using singular value decomposition and DNA encoding techniques.

https://link.springer.com/article/10.1007/s12652-020-02691-8

The article proposes a video watermarking method that uses singular value decomposition and Arnold transform to make the watermark hard to detect and able to withstand attacks.

https://www.sciencedirect.com/science/article/abs/pii/S1877750318310068?via%3Dihub