Cureus Journal of Computer Science

Open Access Original Article

Secure Video Watermarking Embedding and Extraction Process Using Transformation Techniques

Received 11/15/2024
Review began 11/17/2024
Review ended 07/31/2025
Published 08/20/2025

DOI:
https://doi.org/10.7759/s44389-024-01368-z

Shoeb K. Pathan [1] , Meesala S. Kumar [2]

1. Computer Science and Engineering, Sandip Foundation, Sandip University, Nashik, IND 2. Distributed and Networking Systems, Sandip Foundation, Sandip University, Nashik, IND

Corresponding author: Shoeb K. Pathan, shoeb.pathan007@gmail.com

Abstract

In the rapidly evolving digital world, protecting multimedia content is more crucial than ever. Digital watermarking has become a vital technique for securing copyrights, verifying content authenticity, and preventing unauthorized use. This paper introduces a secure watermarking approach based on Discrete Wavelet Transform (DWT), which plays a key role in image decomposition and embedding processes. The method focuses on the segmentation of video content into frames, where DWT is applied to embed watermarks effectively. This approach lays the groundwork for future enhancements, including advanced encryption and compression techniques such as Singular Value Decomposition, Artificial Jellyfish Search Algorithm, and Elliptic-Curve Cryptography, along with H.265 video encoding for compression. The initial implementation of DWT demonstrates its potential in safeguarding digital content by providing a solid foundation for more comprehensive digital watermarking strategies. By integrating DWT with future techniques, the paper aims to address the pressing challenges of content protection, contributing significantly to the field of digital media security in today's digital landscape.

Categories: Image Processing and Analysis, Cryptographic Algorithms, Cryptography
Keywords: digital watermarking, discrete wavelet transform (dwt), multimedia security, singular value decomposition (svd), artificial jellyfish search algorithm (ajs), elliptic-curve cryptography (ecc), h.265 video encoding, image decomposition, secure embedding techniques

Introduction

In the field of information security, ensuring the protection of digital content has become increasingly critical. Digital watermarking techniques offer a way to embed information, such as text or identifiers, directly within digital media like images, videos, or audio files. This process involves modifying the content of the media in such a way that the embedded information remains invisible to the naked eye, preserving the original quality and appearance of the media. For images, this means that alterations to pixel values are made without noticeable visual changes [1]. Watermarks can be categorized as either robust or fragile, depending on the intended application. A robust watermark is designed to withstand various types of media manipulations, such as lossy compression, scaling, and cropping, ensuring that the embedded information remains intact even after such transformations [2]. On the other hand, a fragile watermark is intended to detect tampering; it is designed to break or alter when the media is modified, thus signaling unauthorized changes [3].

Digital watermarking serves different purposes depending on its type. Fragile watermarking is often employed for scenarios where data integrity is crucial, preventing unauthorized copying or alterations [4]. However, challenges remain in optimizing the embedding methods and ensuring data authentication. Robust watermarking, by contrast, focuses on embedding ownership information that can endure even under conditions of deliberate or accidental media modification [5]. This makes robust watermarking particularly valuable for protecting the ownership rights of multimedia content [6]. In an era where multimedia encompasses a broad array of formats - text, audio, graphics, video, and more - effective watermarking is essential for safeguarding the integrity and ownership of digital content [7]. As digital media continues to evolve, the need for sophisticated watermarking techniques that can handle the complexities of modern multimedia applications becomes increasingly apparent [8].

Literature survey

In the domain of multimedia security, the protection of digital content has garnered significant attention due to the increasing risks of unauthorized access and misuse [9]. One of the prominent techniques employed to safeguard such content is digital watermarking, particularly using methods based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) [2]. The combination of these techniques has been widely researched for its ability to embed watermarks within digital media, such as images and videos, by modifying the frequency components of the content in a manner that is imperceptible to the viewer [10]. The former includes algorithms that operate in both the spatial and

transform domains, while the latter is tailored to various video compression standards, such as MPEG (Moving Picture Experts Group)-2, MPEG-4, H.264, and H.265 [4-5]. The process of inserting these watermarks, also known as watermarking, covertly conceals confidential information within host multimedia data. Notably, this procedure transpires at the sender's end, with the reverse process of watermark extraction occurring at the recipient's end. Video watermarking finds applications in broadcast monitoring, copyright protection, and authentication, among others [11,12].

Multiple strategies have been developed by researchers to combat watermarking attacks, which can be broadly categorized into common signal processing attacks and geometric distortions [13]. Geometric transformations modify the spatial arrangement of pixels within an image, making watermark detection challenging and potentially rendering the original watermarking process ineffective [14]. Besides DWT and SVD, more advanced methods like the Undecimated Discrete Wavelet Transform have been introduced to enhance the performance of watermarking [15]. The literature highlights the challenges of watermark extraction, especially under signal degradation or geometric transformations, emphasizing the need for reliable retrieval without compromising media quality [16].

Materials And Methods

The proposed model introduces a novel approach to video security through an adaptive and efficient watermarking embedding process. Central to this framework is the DWT, a well-established method for decomposing video frames into frequency components, enabling precise manipulation of the data. The combination of DWT with SVD ensures robust watermark embedding by allowing the integration of the watermark at a deeper structural level within the video frame, enhancing both invisibility and security [2]. A key innovation in the proposed model is the use of the Artificial Jellyfish Search (AJS) algorithm. Drawing inspiration from the behavior of jellyfish, the AJS algorithm dynamically selects optimal positions within the video subframes for embedding. This approach introduces adaptability to the watermarking process, reducing the risk of the watermark being easily detected or removed by adversaries. The AJS algorithm's exploration and exploitation balance ensure that the embedding locations are not static, making it more resilient against attacks such as frame manipulation or frame averaging [1].

In addition to the AJS algorithm, chaotic maps are employed to optimize the search space further. By leveraging chaotic behavior, these maps ensure the process avoids local optima, facilitating the efficient exploration of potential embedding positions within the video. This integration enhances the watermarking model's robustness by ensuring that the embedding locations are optimally chosen, thereby strengthening the resistance against removal or tampering attempts [15,16]. Another critical component of the proposed model is the incorporation of the Elliptic Curve Model (ECM), a well-regarded cryptographic technique. By utilizing ECM for public key cryptography, the model adds a layer of encryption to the watermarking process. The ECM's streamlined key sizes and efficient cryptographic properties contribute to the overall security of the model, ensuring that the embedded watermark remains secure even if intercepted. This proposed model, which integrates DWT, SVD, the AJS algorithm, chaotic maps, and ECM, creates a comprehensive and secure solution for video watermarking [1]. By focusing on both the robustness of the embedding process and the efficiency of key management, this model achieves a high level of security while maintaining the quality and integrity of the video content. This makes it highly applicable in safeguarding intellectual property and ensuring authenticity in digital video media [2,15].

Mathematical expression

Let O represent the original video, and F_i represent the i^{th} frame of the video, where $i \in \{1, 2, \ldots, N\}$ and N is the total number of frames.

$$O = \{F_1, F_2, \ldots, F_N\} \quad (1)$$

For each frame F_i from Equation (1), apply SVD and DWT.

Let S_i represent the SVD applied to F_i in Equation (2) and W_i the DWT applied to F_i as per Equation (3).

$$F_i = U_i \sum_i V_i T(\text{SVD}) \quad (2)$$

$$W_i = \text{DWT}(F_i) \quad (3)$$

For the secret text image T, apply the same operations:

$$T = U_i \sum_i V_i T \quad (\text{SVD})$$

$$W_T = \mathrm{DWT}(T) \tag{4}$$

Swap the components (e.g., singular values Σi and ΣT) to embed the secret image as per Equation (5).

$$\sum_{i'} = \sum_{i} + k \cdot \sum_{T} \quad (\text{embedding factor } k) \tag{5}$$

The AJS algorithm optimizes the position of embedding the secret image into the video frames. Let P_{opt} represent the optimal position for embedding, where P_{opt} is found by AJS.

$$P_{\text{opt}} = \mathrm{AJS}(F_i, T) \tag{6}$$

The secret grayscale image T is encrypted using ECC mentioned in Equation (7). Let $E(T)$ represent the encrypted image.

$$E(T) = \mathrm{ECC}(T) \tag{7}$$

After encrypting the secret image, embed the resulting bit stream BE into the optimal positions P_{opt} of the video frames shown in Equation (8).

$$F_i' = \mathrm{Embed}(F_i, BE, P_{\text{opt}}) \tag{8}$$

Apply H-265 compression to the watermarked video O', which consists of the modified frames $\{F_1', F_2', \ldots, F_N'\}$.

$$C(O') = \mathrm{H265}(O') \tag{9}$$

Algorithm steps

1. Divide the original video (O) into individual frames.

2. Implement SVD and DWT by swapping components with the secret text image.

3. Utilize the AJS algorithm to identify the best positions for embedding.

4. Encrypt the secret grayscale image using ECC.

5. Insert the bit stream into the optimally chosen values.

6. Apply H-265 compression to the watermarked video.

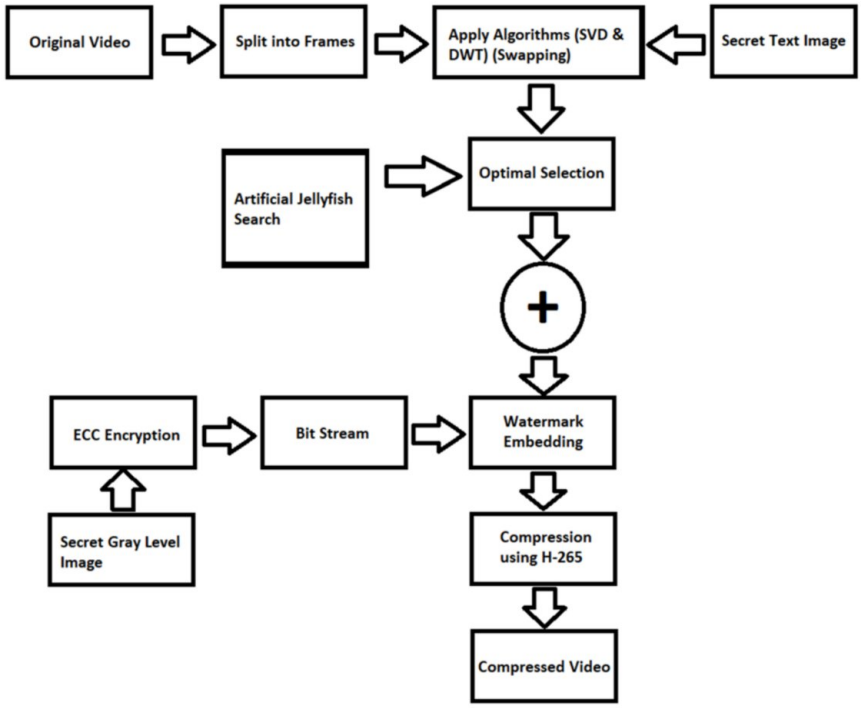

FIGURE 1: Schematic Representation of Proposed Block Diagram

DWT, Discrete Wavelet Transform; ECC, Elliptic Curve Cryptography; SVD, Singular Value Decomposition

One aspect that requires attention is the need for a more detailed explanation of how the ECM technique integrates into the watermarking process. A step-by-step breakdown of the ECC method, how it is applied, and the specific advantages it brings would make the process clearer for readers unfamiliar with cryptography.

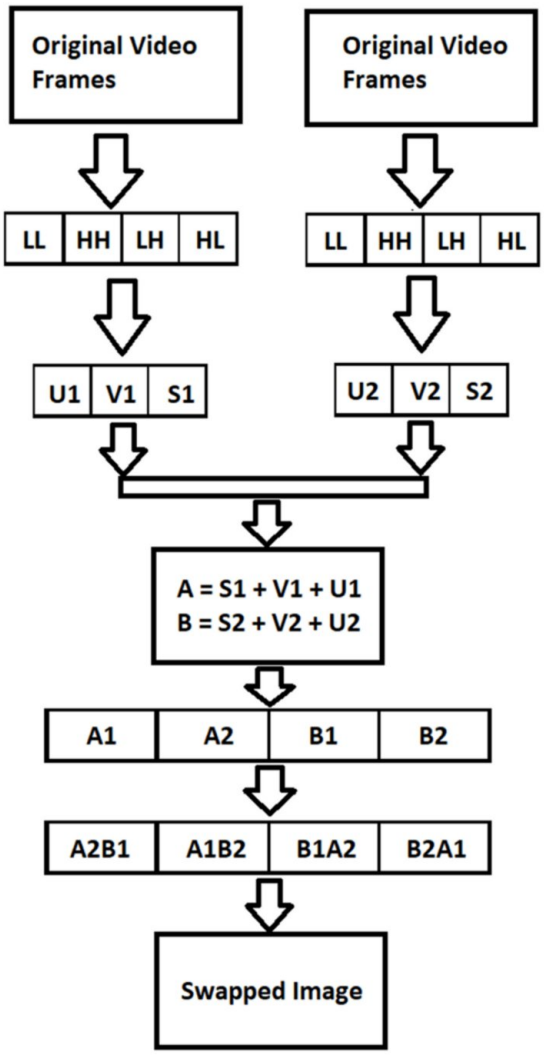

FIGURE 2: Original and Watermark Images Swapping Process

The content includes visual aids (Figures *1* and 2) that assist in explaining the process, but adding more detailed captions and descriptions would further improve the clarity of these diagrams. Additionally, while the use of swapping and watermark embedding is highlighted as a security benefit, a comparison with other techniques in terms of their respective strengths and vulnerabilities could give readers a broader understanding of its security advantages.

In summary, the Secure Video Watermarking Embedding Process discussed here is an impressive attempt to boost video security through a blend of advanced techniques. The combination of DWT, SVD, AJS, and ECC reflects a comprehensive approach to tackling various security concerns. Enhancing the content with more in-depth explanations of certain methods and offering a comparison with alternative approaches could make the process even clearer. Nonetheless, this method significantly contributes to the field of video security and watermarking strategies.

Results

The provided screenshot showcases a "Video Watermarking Module" that has been developed using the .NET Framework. The system used for the implementation is equipped with an Intel Core i5 9th generation processor, 8GB of RAM, and a 256GB SSD, ensuring smooth performance for handling video processing tasks.

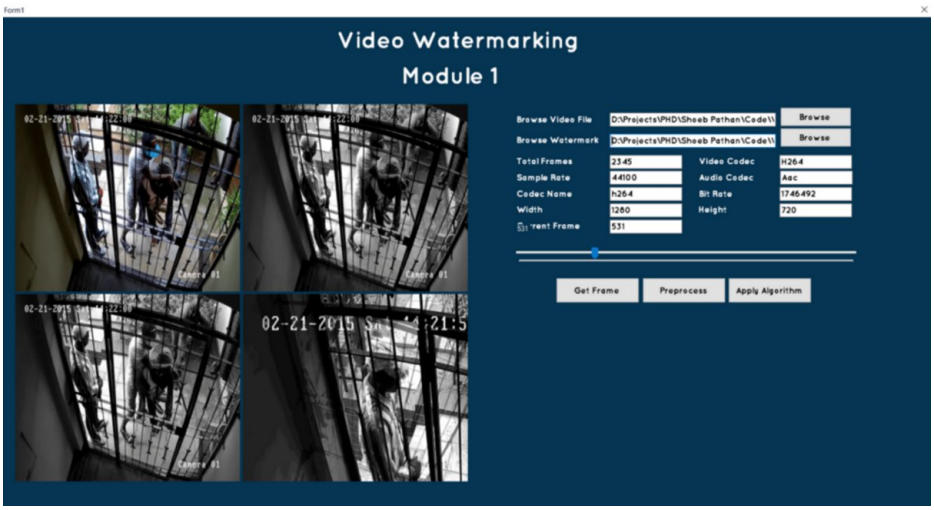

FIGURE 3: Screenshot of Video Watermarking Module 1

The screenshot shown in Figure *3* depicts the user interface of a video watermarking module where the DWT algorithm has been implemented on video frames. The interface allows users to browse both the video file and the watermark image to be embedded. It displays important video information, such as total frames, sample rate, codec, and bit ate.

In Figure *3* on the left side, four extracted frames are shown, where DWT is applied. The purpose of DWT is to decompose these frames into different frequency components, enabling precise watermark embedding. The right side provides controls for selecting frames, pre-processing, and applying the watermarking algorithm. This process enhances security by embedding the watermark in a less perceptible manner while preserving the video's visual quality. Table *1* presents the performance of watermark extraction under various attacks.

Name of attacks	PSNR	CF
Rotational attack	21.47	0.622
Extract watermark without any attack	31.43	0.964
Salt & Pepper noise	24.82	0.559
Gaussian filter attack	29.81	0.953
Gaussian noise	29.15	0.612
Circular filter attack	24.16	0.560
Poisson noise	29.62	0.734
Median filter attack	30.70	0.958
Scaling attack	29.59	0.964
Blur video attack	29.42	0.951

TABLE 1: Performance of Watermark Extraction Under Various Attacks

CF, Correlation Factor; PSNR, Peak Signal-to-Noise Ratio

Discussion

In the current stage of our research, the results are primarily based on metrics derived from the foundational research paper. Key metrics such as Peak Signal-to-Noise Ratio (PSNR), Correlation Factor (CF), and resistance to various types of attacks (including geometric and signal processing attacks) have been evaluated to establish the baseline performance. These metrics provide a critical understanding of how well the watermark is embedded in the media and how resilient it is to both quality degradation and

malicious attacks.

Our proposed model, which integrates the DWT with SVD, AJS algorithm, and chaotic maps, aims to significantly improve these baseline metrics. The incorporation of these advanced techniques ensures that the watermark is embedded at a more structural level within the video frame, offering enhanced imperceptibility, higher PSNR values, and stronger CF outcomes. This deep embedding not only maintains the visual quality of the host video but also ensures that the watermark remains robust, even under aggressive signal distortion.

Moreover, the adaptive nature of the AJS algorithm introduces flexibility in the watermarking process, ensuring that the embedding locations are dynamic rather than fixed, which provides an additional layer of protection. This adaptability is expected to improve resistance against common attacks, such as geometric transformations, frame averaging, and compression-based attacks, which often target static embedding methods. Additionally, the chaotic maps employed in the optimization process help avoid local optima, further enhancing the robustness of the watermark under attack conditions.

By incorporating ECM-based cryptography for secure key management, the proposed model also ensures the confidentiality of the embedded watermark. ECM's efficient cryptographic properties bolster security without significantly increasing computational overhead. This is especially critical in applications where both the integrity and authenticity of the video content must be maintained across various platforms and attack vectors.

Overall, with the combination of these innovative techniques, we anticipate not only higher PSNR and CF values but also a marked improvement in the system's resilience to attacks like compression, noise, and geometric distortions. These improvements are expected to position our proposed watermarking system as a highly secure and efficient solution for safeguarding digital video content in real-world applications, such as copyright protection, content verification, and digital forensics. Future work will involve a detailed quantitative analysis of these metrics to further validate the performance gains introduced by our approach.

Conclusions

In conclusion, this paper offers a detailed analysis of the methodology and security framework introduced by the proposed video watermarking model. By incorporating DWT, SVD, the artificial jellyfish algorithm, and ECC encryption, the model demonstrates a solid approach to securing digital video content. These techniques collectively provide enhanced security and data protection. However, further exploration of ECC's integration and experimental validation would provide greater insights into its practical effectiveness.

As a contribution, the introduction of a new and efficient algorithm for watermark extraction from digital content would represent a significant advancement in the field. Such an algorithm would further strengthen the domain of digital watermarking, adding valuable knowledge to existing research.

Additional Information

Author Contributions

All authors have reviewed the final version to be published and agreed to be accountable for all aspects of the work.

Concept and design: Shoeb K. Pathan

Acquisition, analysis, or interpretation of data: Shoeb K. Pathan, Meesala S. Kumar

Drafting of the manuscript: Shoeb K. Pathan

Critical review of the manuscript for important intellectual content: Shoeb K. Pathan, Meesala S. Kumar

Supervision: Meesala S. Kumar

Disclosures

Human subjects: All authors have confirmed that this study did not involve human participants or tissue. **Animal subjects:** All authors have confirmed that this study did not involve animal subjects or tissue. **Conflicts of interest:** In compliance with the ICMJE uniform disclosure form, all authors declare the following: **Payment/services info:** All authors have declared that no financial support was received from any organization for the submitted work. **Financial relationships:** All authors have declared that they

have no financial relationships at present or within the previous three years with any organizations that might have an interest in the submitted work. **Other relationships:** All authors have declared that there are no other relationships or activities that could appear to have influenced the submitted work.

References

1. Murthyraju K, Subbarao MV: Using artificial jellyfish algorithm with transformation technique for secure video watermarking embedding process. 2022 International Conference on Computing, Communication and Power Technology (IC3P), Visakhapatnam, India. 2022, 204-208. 10.1109/IC3P52835.2022.00050
2. Faragallah OS: Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain. AEU - International Journal of Electronics and Communications. 2013, 67:189-196. 10.1016/j.aeue.2012.07.010
3. Asikuzzaman M, Pickering MR: An overview of digital video watermarking. IEEE Transactions on Circuits and Systems for Video Technology. 2018, 28:2131-2153. 10.1109/tcsvt.2017.2712162
4. Mawande S, Dakhore H: Video watermarking using DWT-DCT- SVD algorithms. 2017 International Conference on Computing Methodologies and Communication (ICCMC), Erode, India. 2017, 1161-1164. 10.1109/ICCMC.2017.8282656
5. Yu X, Wang C, Zhou X: A survey on robust video watermarking algorithms for copyright protection. Applied Sciences. 2018, 8:1891. 10.3390/app8101891
6. Kuraparthi S, Kollati M, Kora P: Robust optimized discrete wavelet transform-singular value decomposition based video watermarking. Traitement du Signal. 2019, 36:565-573. 10.18280/ts.360612
7. Fung CWH, Godoy W Jr: A new approach of DWT-SVD video watermarking. 2011 Third International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, Malaysia. 2011, 233-236. 10.1109/CIMSim.2011.48
8. Jafari Barani M, Ayubi P, Yousefi Valandar M, Yosefnezhad Irani B: A blind video watermarking algorithm robust to lossy video compression attacks based on generalized Newton complex map and contourlet transform. Multimedia Tools and Applications. 2019, 79:2127-2159. 10.1007/s11042-019-08225-5
9. Prasetyo H, Hsia CH, Liu CH: Vulnerability attacks of SVD-based video watermarking scheme in an IoT environment. IEEE Access. 2020, 8:69919-69936. 10.1109/access.2020.2984180
10. Rahim N, Rathi R, Meesala SK: Blind Image deblurring using Bayesian approach on parallel architecture. International Journal of Computer Applications. 2012, 42:19-23.
11. Mohammed AA, Ali NA: Robust video watermarking scheme using high efficiency video coding attack. Multimedia Tools and Applications. 2018, 77:2791-2806. 10.1007/s11042-017-4427-1
12. Ganic E, Eskicioglu AM: Robust DWT-SVD domain image watermarking: embedding data in all frequencies. MM&Sec '04: Proceedings of the 2004 workshop on Multimedia and Security. 2004, 166-174. 10.1145/1022431.1022461
13. Yin C, Li L, Lv A, Qu L: Color image watermarking algorithm based on DWT-SVD. 2007 IEEE International Conference on Automation and Logistics, Jinan. 2007, 2607-2611. 10.1109/ICAL.2007.4339020
14. Ghosh D, Ramakrishna K: Watermarking compressed video stream over Internet. 9th Asia-Pacific Conference on Communications (IEEE Cat. No.03EX732), Penang, Malaysia. 2003, 2:711-715. 10.1109/APCC.2003.1274450
15. Xue J, Li Q, Li Z: A novel digital video watermarking algorithm. Procedia Engineering. 2011, 24:90-94. 10.1016/j.proeng.2011.11.2607
16. Esen E, Alatan AA: Robust video data hiding using forbidden zone data hiding and selective embedding. IEEE Transactions on Circuits and Systems for Video Technology. 2011, 21:1130-1138. 10.1109/tcsvt.2011.2134770