International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-11, Issue-01, Apr 2025

Review on Secure Video Watermarking Embedding Process Using Artificial Jellyfish Algorithm with Transformation Technique

Shoyeb Karim Pathan[1], Meesala Sudhir Kumar[2]

[1]Student, School of Computer Science & Engineering Department, India.

[2]Professor, School of Computer Science & Engineering Department India.

[1]shoyebpathan604@gmail.com, [1]Orcid Id: 0009-0002-1390-540X

Abstract. The ever-evolving digital landscape has given rise to multifaceted challenges, with digital watermarking emerging as a promising solution. Beyond safeguarding copyrights, digital watermarking finds diverse applications in content authentication, distribution tracing, and tamper recovery. Given the prevalence of digital photo and video sharing, vulnerabilities to unauthorized use are rampant. This chapter introduces an innovative and secure watermarking approach employing Discrete Wavelet Transforms (DWT) and Singular Value Decomposition (SVD), facilitating image decomposition and exchange. To optimize the effectiveness of DWT and SVD, an Artificial Jellyfish Search Algorithm (AJS) intelligently selects coefficients.

The proposed method operates through sequential steps: segmentation of original videos into frames, application of the watermarking process, and encryption via Elliptic-Curve Cryptography (ECC). This model pioneers two central concepts: substitution of text images with original ones and embedding grayscale images within swapped counterparts. Notably, the watermarked image is subsequently compressed using the H.265 video encoding algorithm, significantly reducing video size and facilitating efficient transmission.

By integrating these techniques, the chapter contributes to enhancing the safeguarding and protection of digital content the face of potential infringements. The utilization of DWT, SVD, AJS, ECC, and H.265 encoding underscores a comprehensive and forward-looking approach to digital watermarking, poised to address intricate challenges in contemporary digital communication and content protection.

Keywords: Digital watermarking, Discrete Wavelet Transforms (DWT), Singular Value Decomposition (SVD), Artificial Jellyfish Search Algorithm (AJS), Elliptic-Curve Cryptography (ECC), H.265 video encoding algorithm

I. INTRODUCTION

In the realm of information security, the imperative to safeguard data and implement appropriate practices is paramount. Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images, this means that the modifications of the pixel values have to be invisible. Furthermore, the watermark must be either robust or fragile, depending on the application. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as lossy compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others. In some cases, the watermark may need to be fragile. "Fragile" means that the watermark should not resist tampering, or would resist only up to a certain, predetermined extent

The example below illustrates how digital watermarking can hide information in a totally invisible way. The original image is on the left; the watermarked image is on the right and contains the name of the author.

Digital watermarks can be largely divided into fragile watermarking and robust watermarking. Fragile watermarking is mainly used for protecting data that cannot be copied, but some problems remain to be solved such as methods for data build-in and authentication, and the types of data to be

 DOI : 10.35291/2454-9150.2025.0103

inserted for data authentication. The protection of a fragile watermark can be guaranteed by maintaining security either by the insertion method or Data-Hiding Method using Digital Watermark in the Public Multimedia Network inserted data. Robust watermarking emphasizes the robustness of the watermark information built into the digital image. Thus, the extraction of ownership information should be possible even from intentional or unintentional image transformation and lossy compression [5, 6]. As such, robust watermarking is mainly used for the ownership protection of multimedia contents.

Multimedia uses various media formats (such as text, sound, graphics, animation, film, interactive) in the collection and processing of information to educate or entertain the user of these. The use of electronic devices to store and experience visual content also applies to multimedia. Multimedia is comparable, but larger, to conventional mixed media art. “Rich media” means immersive multimedia.

II. LITERATURE SURVEY

An on-going concern revolves around the illicit acquisition and utilization of information and information systems using DWT-based SVD video watermarking method, the video frames are transformed with the DWT using two resolution levels. The high frequency band HH and the middle frequency bands LH and HL are SVD transformed and the watermark is hidden in them. The proposed DWT-based SVD video watermarking method is characterized by two improvements: (1) a cascade of two powerful mathematical transforms; the Discrete Wavelet Transform (DWT)-based SVD using additive method, and (2) an error correction code is applied and embeds the watermark with spatial and temporal redundancy [2]. Addressing this issue, digital watermark technology has emerged as a pioneering approach to fortify the ownership of multimedia assets. This technique entails the permanent embedding of watermarks within multimedia files, ensuring robustness, imperceptibility, and security.

The watermark embedding techniques were classified based on the domain in which they embedded the watermark, including compressed, spatial and transform. Each technique was discussed in detail and some existing works related to them were then reviewed. [3]. These watermarks can encompass copyright material, ownership details, or authentication sequences. The text summarizes robust video watermarking algorithms designed for copyright protection, categorizing them into two primary types: original video-based watermarking algorithms and compressed video-based watermarking algorithms. The former is further divided into algorithms operating in the spatial domain and those in the transform domain. Meanwhile, the latter category is segmented based on the compression standards they utilize, specifically MPEG-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 [10].

While the fundamentals of image watermarking are transferable to video sequences the coordinates of Best Dwt blocks were optimized with the help of ABC with optimized Transparency and Robustness. The watermark is inserted in best dwt blocks which again helped the scheme in achieving high robustness by preserving the video quality intact [7], video watermarking demands additional attributes: low complexity, constant bit rate, and domain processing within compressed formats. Video watermarking finds applications in Broadcast Monitoring, Copyright Protection, and Authentication, among others.

Multiple strategies have been developed by researchers to combat watermarking attacks, which can be broadly categorized into common signal processing attacks and geometric distortions [8]. However, addressing geometric distortions is complex due to synchronization issues and the difficulty of detecting watermarks within distorted media. Such challenges necessitate ongoing research. Geometric transformations alter the spatial relationships between pixels in an image, rendering watermark detection arduous and, in some cases, rendering the initial watermarking effort futile. the SVD-based video watermarking scheme overcomes the FPP occurring in the former existing scheme. [9].

This review chapter surveys the landscape of watermarking techniques against the backdrop of multimedia security. It explores the efficacy of various strategies against signal processing and geometric attacks, underscoring the importance of handling geometric distortions and their implications for watermark identification. Through an examination of established techniques and ongoing research, this chapter sheds light on the current state of video watermarking security, paving the way for future advancements in safeguarding multimedia content.

Cons:

The chapter introduces multiple techniques, including Discrete Wavelet Transforms (DWT), Singular Value Decomposition (SVD), Artificial Jellyfish Search Algorithm (AJS), and Elliptic-Curve Cryptography (ECC). The complexity introduced by combining these techniques may make it challenging to implement and replicate the proposed model.

Absence of Extraction Details: The chapter [1] does not mention how watermarks are extracted from watermarked images or videos. Without this information, it is unclear how the embedded information is retrieved.

Lack of Discussion on Detection and Decoding: In digital watermarking, the extraction process typically involves detecting and decoding the watermark from the watermarked

 DOI : 10.35291/2454-9150.2025.0103

content. The chapter [1] does not provide any insights into the methods, algorithms, or techniques used for this crucial step.

No Mention of Robustness or Error Correction: An important aspect of watermark extraction is ensuring robustness against common signal processing operations and potential errors in the watermarked content. The chapter does not address whether the proposed model incorporates error correction techniques or how it handles signal processing operations.

Missing Evaluation of Extraction Quality: There is no indication in the chapter [1] that the quality of watermark extraction is evaluated or discussed. Evaluating extraction quality is essential to assess how well the watermark survives various transformations and attacks.

The chapter [5] does not indicate any novel contributions or innovative approaches in the field of video watermarking. It suggests a review of existing algorithms without highlighting any new techniques or advancements.

In addition to these technical advancements, the chapter underscores the significance of watermarking in addressing copyright protection concerns and preserving the integrity of digital content. By embedding watermarks containing copyright information, ownership details, or authentication sequences, content providers can assert ownership rights and deter unauthorized use or distribution of their multimedia assets.[6]

Furthermore, the chapter highlights the evolving landscape of watermarking techniques, categorizing them based on embedding domains and discussing their applicability in various contexts such as broadcast monitoring, copyright protection, and authentication. Through a comprehensive survey of existing methods, the chapter provides insights into the current state of video watermarking security and identifies areas for future research and innovation.

Overall, the proposed DWT-based SVD video watermarking method represents a significant advancement in multimedia security, offering a robust solution to combat illicit acquisition and unauthorized utilization of digital content. By addressing key challenges such as imperceptibility, robustness, and security, the method contributes to the ongoing efforts to safeguard intellectual property rights in the digital era.

One notable contribution to this domain is an improved video watermarking scheme based on the undecimated discrete wavelet transform (UDWT). This scheme divides the frames of the cover video into 8 × 8 blocks, with two AC coefficients selected in each block for watermark insertion. Leveraging the properties of UDWT across four frequency bands, the scheme capitalizes on the redundancy inherent in this transform to achieve a high watermarking capacity. Furthermore, the inherent masking properties of the human visual system, coupled with UDWT, contribute to the obliviousness of the watermarking scheme, thereby enhancing its security. [17]

Experimental evaluations of the proposed video watermarking scheme demonstrate its ability to fulfill all four key requirements of watermarking: security, obliviousness, robustness, and capacity. These findings underscore the effectiveness of UDWT-based watermarking in addressing critical concerns related to intellectual property rights and ownership assertion in digital video content. [17]

Keywords: digital watermarking, multimedia security, signal processing attacks, geometric distortions, video watermarking.

III. PROPOSED SYSTEM ARCHITECTURE

The proposed Secure Video Watermarking Embedding Process outlined in this content is a noteworthy endeavour in the field of video security enhancement. This review aims to dissect and evaluate the various components and algorithms introduced in this process.

The integration of the AJS algorithm underscores the multidisciplinary nature of video watermarking research, drawing inspiration from diverse fields such as biology and mathematics to enhance security measures. By mimicking the exploration patterns of jellyfish, the algorithm introduces a dynamic and adaptive element to the embedding process, optimizing the selection of embedding positions while mitigating the risk of detection by potential adversaries.

Moreover, the utilization of chaotic maps for solution optimization highlights the importance of leveraging advanced mathematical concepts to address complex optimization challenges. Chaotic maps offer a robust framework for exploring solution spaces efficiently, ensuring that the embedding process converges to optimal positions within the video frames. This approach not only enhances the security of the watermarking process but also contributes to its resilience against potential attacks.

In essence, the incorporation of the AJS algorithm and chaotic maps in the Secure Video Watermarking Embedding Process represents a significant advancement in the field of video security. By combining innovative algorithms with established techniques such as DWT and SVD, the proposed process demonstrates a holistic approach to addressing security concerns in digital video content. Through meticulous design and integration of diverse methodologies, the process achieves a balance between complexity, efficiency, and robustness, paving the way for enhanced protection of intellectual property rights in multimedia assets.

The foundation of the process revolves around the integration of different techniques to ensure robust and reliable security for video content. The process begins by segmenting the original video into subframes, a fundamental step that

 DOI : 10.35291/2454-9150.2025.0103

lays the groundwork for subsequent operations. The combination of Discrete Wavelet Transforms (DWT) and Singular Value Decomposition (SVD) techniques to manipulate the frames introduces a layer of complexity that contributes to the overall security scheme.

One of the innovative features is the application of the Artificial Jellyfish Search Algorithm (AJS) for selecting specific positions within the video frames for embedding secret grey images. This algorithm, inspired by jellyfish behaviour, adds an interesting biological touch to the technical processes. The employment of chaotic maps for optimizing solution distribution in the search area shows the meticulous approach taken to achieve convergence and prevent local minimum traps.

$$A\rightarrow i+1 = yA\rightarrow i(1 - Ai), 0 \leq A\rightarrow 0 \leq 1$$

The integration of the Elliptic Curve Model (ECM) technique, known for its significance in cryptography, is a substantial highlight. The usage of ECM for public key cryptography is a clever choice, as it harnesses the inherent security properties of elliptic curves to enhance the watermarking process's robustness. The streamlined key size and storage requirements are undoubtedly appealing attributes of ECC.

Algorithm

Input: Original Video - O

Split O into Frames

Apply SVD and DWT (Swapping) with Secret Text Image

Perform Artificial JellyFish Search for Optimal Selection

Perform ECC Encryption on Secret Gray level Image

Embed Bit Stream on the Optimal selected values

Compress using H-265

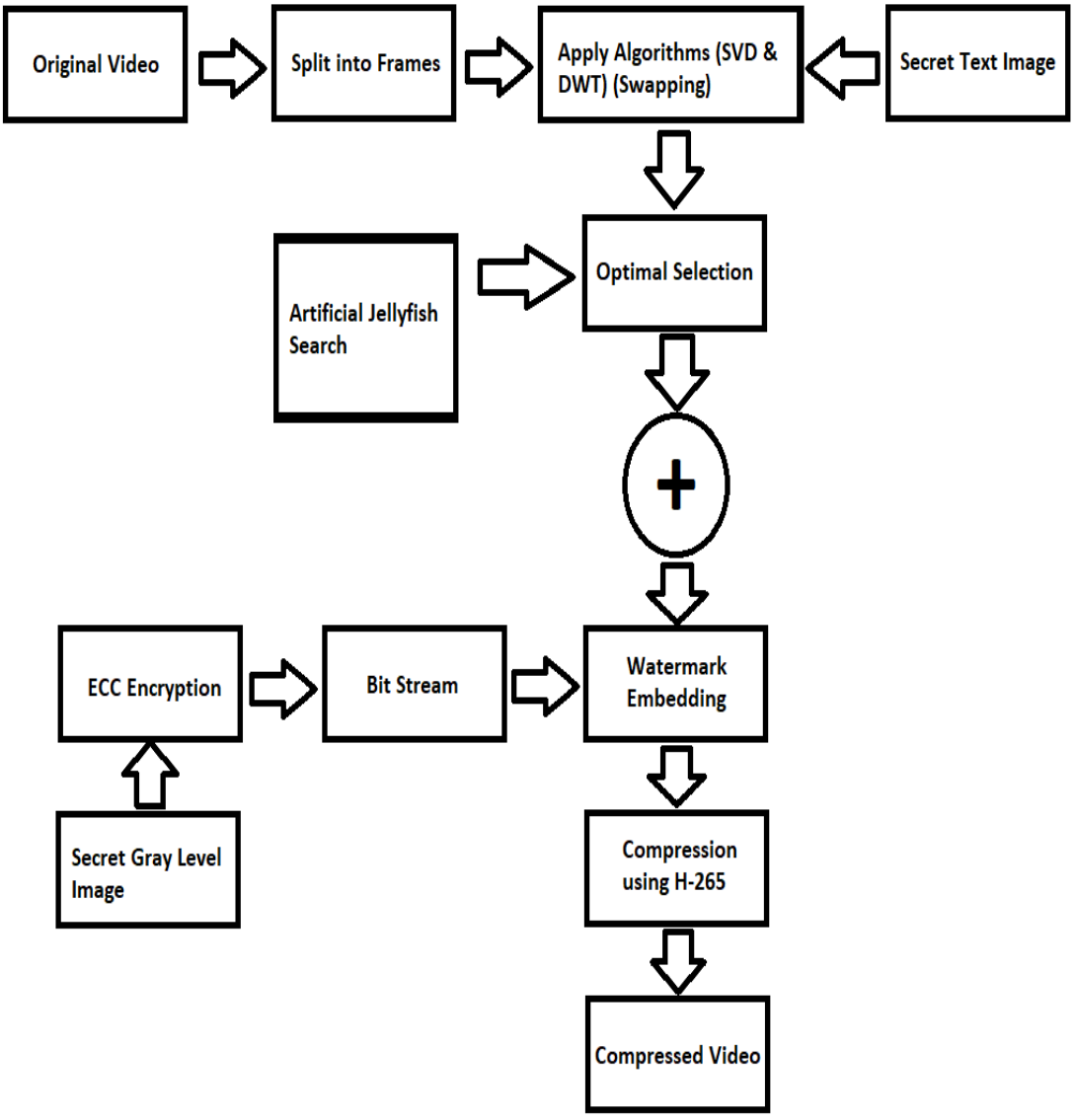

Fig. 1. Schematic representation of proposed block diagram

However, a point to consider is the need for a more comprehensive explanation of how the ECM technique is linked to the watermarking process. A step-by-step illustration of the ECC process, its integration, and the benefits it provides

 DOI : 10.35291/2454-9150.2025.0103

could offer more clarity to readers who may not be familiar with cryptographic concepts.

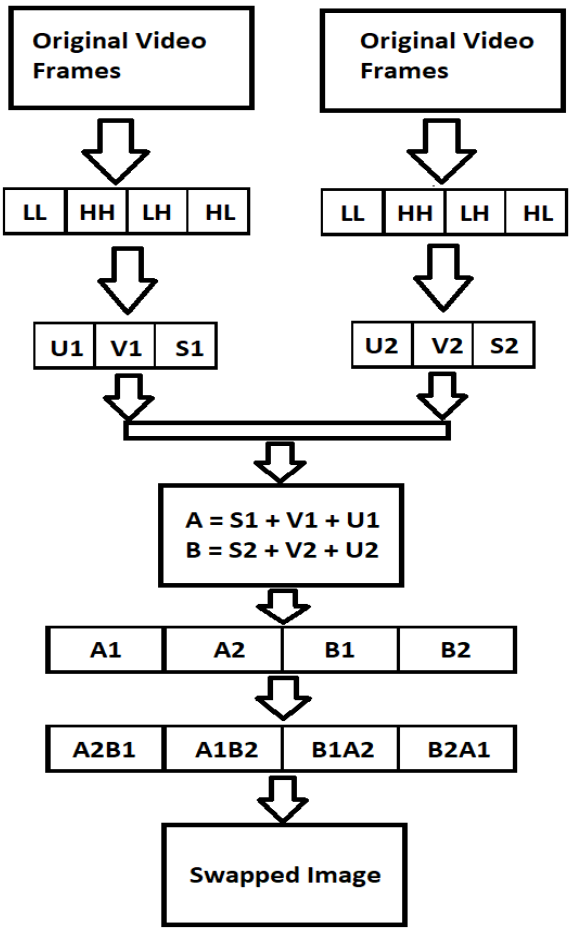

Fig. 2. Original and watermark images swapping process

$$y[n] = (x * y)[n] = \sum_{k=-\infty}^{\infty} x[k]g[n-k]$$

The content provides graphical representations (Figure 1 and Figure 2) that enhance the understanding of the process, but additional captions and explanations would further enhance the clarity of these illustrations. Furthermore, while the process's use of swapping and watermark embedding is emphasized as a security advantage, a comparative analysis against other methods in terms of their security strengths and weaknesses could provide a more comprehensive perspective.

In conclusion, the Secure Video Watermarking Embedding Process presented here demonstrates a commendable effort to enhance video security using a combination of innovative techniques. The integration of DWT, SVD, AJS, and ECC underscores a holistic approach to address different aspects of security. The content could be further improved by providing more comprehensive explanations of certain concepts and techniques while offering comparative insights into the process's security effectiveness. Overall, this process is a valuable contribution to the realm of video security and watermarking techniques.

$$T: \begin{cases} K^n \to K^m \\ x \mapsto M_x \end{cases}$$

Fig. 3 Video Frame

IV. RESULTS AND DISCUSSION:

The presented section provides a thorough examination of an innovative digital image watermarking technique. The authors opted for MATLAB 2018 as their implementation platform, executed on a Windows computer equipped with an Intel Core i5 processor and 4 GB of RAM. This comprehensive review aims to delve into the experimentation, performance analysis, and results interpretation of the approach.

The choice of utilizing MATLAB 2018 for implementation offers a solid foundation for this study. The capability of MATLAB to handle intricate algorithms and its prominence in the field of image processing assure a robust platform for experimentation. Mentioning the hardware specifications provides essential context for understanding the resources used, contributing to the reproducibility and comparability of the experiment.

An aspect that significantly enriches the review is the use of an existing dataset from the web. This practice ensures consistency and comparability with future research, and the dataset's image size (255x255 pixels) provides a clear indication of the scale of the experiment.

Table 1. Performance at different gain factors at different sub-bands(1)

GF	HL band		HH band		HH band		LH band	
	PSNR	NAE	PSNR	NAE	PSNR	NAE	PSNR	NAE
0.05	41.2321	0.9244	41.2455	0.9246	41.2415	0.9493	41.2455	0.9293
0.1	40.7322	0.9248	40.6447	0.925	40.7415	0.9343	40.7447	0.9245
0.005	41.6821	0.9353	41.8947	0.9255	41.6915	0.9248	40.6947	0.9249
0.01	41.6321	0.9293	41.6454	0.9295	41.6415	0.9253	40.6454	0.9254
0.001	41.7222	0.9343	41.7346	0.9345	41.7315	0.9244	41.7346	0.9244

The section's highlight lies in the detailed performance analysis. By employing a range of standard metrics such as Average Difference (AD), Mean Square Error (MSE), Peak

 DOI : 10.35291/2454-9150.2025.0103

Signal to Noise Ratio (PSNR), Normalized Absolute Error (NAE), Normalized Correlation Coefficient (NCC), Compression, Minimum Difference (MD), and Structural Content (SC), the authors offer a comprehensive evaluation of their technique's performance. Each metric's brief explanation adds clarity to the review.

Tables I, II provide valuable insights into the existing technique's performance under varying conditions. Table I highlights the influence of gain factors on PSNR and NAE, showing a sensitivity to the factor's values. Table II adds depth by assessing the technique's resilience to different attacks.

Table 2. Calculate CF, PSNR Values for attacked frames of video(1)

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

To further enhance the review, it could benefit from explanations of the metrics chosen and their relevance to image watermarking assessment. Additionally, incorporating graphs or figures to visualize performance trends would provide a more intuitive understanding of the results.

In conclusion, the section effectively presents a comprehensive evaluation of the digital image watermarking technique. By utilizing MATLAB 2018, specifying hardware details, and employing an existing dataset, the authors establish a strong foundation for their experiment. The thorough performance analysis and the array of metrics utilized showcase the technique's effectiveness under various conditions. The review could be further enriched with visual aids and more detailed explanations of the chosen evaluation metrics. Overall, the section serves as a valuable contribution to the realm of image watermarking techniques.

V. CONCLUSION

This review seeks to elucidate the methodology, security measures, and overall contributions of the proposed model.

In conclusion, the chapter presents a comprehensive approach to video watermarking through the integration of DWT, SVD, artificial jellyfish algorithm, and ECC encryption. The combination of these techniques showcases a robust methodology with the potential for enhancing security and data integrity. However, to enhance the chapter's impact, further elaboration on ECC's implementation and potential experimental validation could provide a more comprehensive perspective on the model's effectiveness in real-world scenarios.

As a contribution, we can introduce a novel and robust algorithm for the extraction of watermarked data from digital content. We can propose an algorithm that represents a significant advancement in the field of digital watermarking and contributes to the existing body of knowledge.

REFERENCES

[1] KommisettiMurthyraju, M.Venkata Subbarao "Using Artificial Jellyfish Algorithm with Transformation Technique for Secure Video Watermarking Embedding Process." 2022 International Conference on Computing, Communication and Power Technology (IC3P)

[2] Faragallah, Osama S. "Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain." AEU- International Journal of Electronics and Communications 67, no. 3 (2013): 189-196.

[3] Asikuzzaman M, Pickering MR. “An overview of digital video watermarking.” IEEE Transactions on Circuits and Systems for Video Technology. 2017 Jun 5;28(9):2131-53.

[4] Mawande S, Dakhore H. “Video watermarking using DWT-DCT- SVD algorithms.” In 2017 International Conference on Computing Methodologies and Communication (ICCMC) 2017 Jul 18 (pp. 1161- 1164). IEEE.

[5] Yu X, Wang C, Zhou X. “A survey on robust video watermarking algorithms for copyright protection”. Applied Sciences. 2018 Oct;8(10):1891.

[6] Kuraparthi S, Kollati M, Kora P. “Robust Optimized Discrete Wavelet Transform-Singular Value Decomposition Based Video Watermarking”. Traitement du Signal. 2019 Dec 1;36(6).

[7] Fung CW, Godoy Jr W. “A new approach of DWT-SVD video watermarking”. In2011 Third International Conference on Computational Intelligence, Modelling & Simulation 2011 Sep 20 (pp. 233-236). IEEE.

[8] Barani MJ, Ayubi P, Valandar MY, Irani BY. “A blind video watermarking algorithm robust to lossy video compression attacks based on generalized Newton complex map and contourlet transform”. Multimedia Tools and Applications. 2020 Jan;79(3):2127-59.

[9] Prasetyo H, Hsia CH, Liu CH. “Vulnerability attacks of SVD-based video watermarking scheme in an IoT environment”. IEEE Access. 2020 Mar 30;8:69919-36.

[10] Naazish Rahim,Rakesh Rathi, Sudhir Kumar Meesala. “Blind Image Deblurring using Bayesian Approach on Parallel Architecture.” International

 DOI : 10.35291/2454-9150.2025.0103

Journal of Computer Applications (0975 – 8887) - Volume 42– No.14, March 2012

[11] Mohammed AA, Ali NA. "Robust video watermarking scheme using high efficiency video coding attack". Multimedia Tools and Applications. 2018 Jan;77(2):2791-806.

[12] E. Ganic, A. M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies", in Proceedings of the 2004 workshop on Multimedia and Security, pp. 166-174, 2004.

[13] Cheng-qun Yin, Li Li, An-qiangLv and Li Qu, "Color Image Watermarking Algorithm Based on DWT-SVD", Proc. of IEEE Int. Conf. on Automation and Logistics, pp. 2607-2611, 2007.

[14] K. Ramakrishna, D. Ghosh. "Oblivious Watermarking Of Digital Video Using Inter-Frame Similarities," Proc. IEEE Int. Conf, 2000.

[15] XueJunxiao, Li Qingbin, Li Zhiyong. "A Novel Digital Watermarking Algorithm," Elsevier Proc. of Int. Conference on Advances in Engineering, pp. 90-94, 2011.

[16] ErsinEsen and A. Aydin Alatan. "Robust Video Data Hiding Using Forbidden Zone Data Hiding and Selective Embedding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 8, 2011.

 DOI : 10.35291/2454-9150.2025.0103