Digital Video Watermarking Framework: A Python-Based Approach

Dr.V Prasannajaneya
Dept. ECE IARE
Hyderabad,India
Prasanna.vajrala@ gmail.com

L.Amulya
Dept. ECE IARE
Hyderabad,India
amulyalingala0204
@gmail.com

S.Jagruthi *Dept. ECE IARE*
Hyderabad,India
Jagruthisonti2004
@gmail.com

J.Meghanath
Dept. ECE IARE
Hyderabad,India
j.meghanathpavansai
@gmail.com

***Abstract*—Digital video watermarking has become increasingly important in safeguarding the intellectual property rights, ensuring authenticity, and tracking the distribution of digital video content. This overview explores the techniques, challenges, and applications of digital video watermarking. Various embedding methods, including spatial domain, transform domain, and spread spectrum techniques, are discussed, alongside the challenges of robustness and imperceptibility. The applications of digital video watermarking in copyright protection, content authentication, broadcast monitoring, and forensic analysis are also examined. Understanding the fundamentals of digital video watermarking is crucial in today's digital age for content creators, distributors, and consumers alike.**

***Index Terms*—Digital video watermarking, imperceptibility, embedding techniques, copyright protection, authentication , robustness.**

I. Introduction

In today's digital landscape , where the proliferation of digital video content is ubiquitous , ensuring the protection , authentication and integrity of such content has become paramount. Digital video watermarking has emerged as a key technology in addressing these concerns.A full watermarking process should ideally consist of three critical operations, namely, watermark embedding, watermark extraction, and watermark detection[1].It normally embeds invisible copyright watermarks into the host data and does an extra encryption. These invisible copyright watermarks are certification, symbols, digital signatures, and so on[2].The suitability of a digital watermarking algorithm in copyright protection determines many factors, one being more important of its robustness to various attacks.[3] With the tool of digital water marking, a video can have richer information to tell whether the content of the product has been changed or not . Digital watermarking requires different strategies to achieve reasonable robustness[4] The task of balancing robustness, imperceptibility, and capacity is very delicate in designing good watermarking systems. This technology is found to be applied in the area of copyright protection, content authenticity verification, broadcast monitoring, and forensic analysis. This allows content producers to protect their copyrights and track any unauthorized use or sharing of their videos. In the early days, encryption and control access techniques were employed to protect the ownership of media. They do not, however, protect against unauthorized copying after the media have been successfully transmitted and decrypted.[5]

Transform domain techniques, on the other hand, apply mathematical transforms such as Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) to the video frames before embedding the watermark[6-7].Spread spectrum techniques spread the watermark signal across the entire frequency spectrum of the video, making it robust against attacks.Digital video watermarking technology faces many challenges, setting harsh conditions against the most frequent video modifications such as compression, resizing, and transcoding, not to mention any kind of edition of the embedded watermark. Spatial domain techniques directly modify the pixel values of the video frames to embed the watermark.Frequency Domain watermarking ,most of watermarking methods the watermark will be inserted into frequency domain instead of the spatial domain for the robustness of the watermarking[9] Here we are using Python programming language in order to ease the process.Since it is Easy to learn and it is an Open source and can be used for Image processing and graphic design applications.Python provides a Extensive standard libraries including OpenCV, Pillow, and scikit-image, that offer ready-made functions for image and video processing tasks.

the general architecture of a watermarking process looks like that: As shown in figure 1, signature is made of two main steps: embedding and detection. Watermarking is advantageous in that it provides far greater protection to Ownership, integrity, authenticity, and rights of authorship, which Thus can become difficult to achieve otherwise.

A. Video Watermarking

After embedding a watermark into a host video, it may be threatened several categories of attack, whereas the watermark extraction is implemented at the decoder from the attacked version of the watermarked video. Therefore some aspects like invisibility of the watermark, capacity, blind detection, resistance to various attacks, and the security of the watermark must be desirable while disposing the framework. design of a watermarking algorithm ownership as in figure.

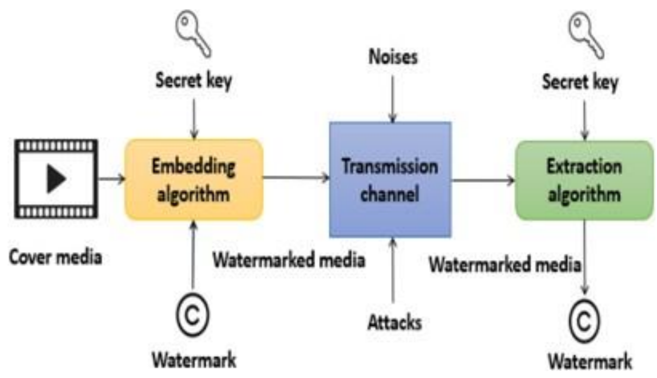

Fig. 1. General procedure of a watermarking.

However, the focus of this paper is invisible watermarking which is more challenging since the watermark must be invisible to the human visual system (HVS) not to leave any degradation upon the video's visual quality.[2] Although the field has developed over time, the grayscale versions of RIS have not been put to much use. Currently, it has expanded to color versions.

Each video sequence color frame includes three components of each color space: red (R), green (G) and blue (B) and is referred to as the RGB color space. The computation can also be done alternatively for the luminance (Y) and chrominance (U and V) components in YUV domain. As perceived by human eyes, the Y channel is the general intensity and includes about a frame, and the U and V channels carry the color information.

II. Literature survey

Based on the current state-of-the-art deep-learning model applied in video watermarking schemes, this paper offered a deep survey. In an attempt to introduce video watermarking and deep learning. Because of neural network algorithms being applied, it enhanced the paradigms of key watermarking tools such as capacity, robustness, and invisibility reaching impossible levels when using only traditional methods of watermarking.[1] Based on the domain of the original image, the above mentioned watermark embedding methods were classified into compressed domain, uncompressed spatial and transform. In the subsequent sections, each of the methods is a expounded. and then some previous related existing literature, which have been said here too on them were also put forward. As part of contribution to the pioneering studies on domain watermarking techniques such as geometiric-invariant watermarking technique, other related investigations examined. An overview of the general image-based representation of 3D videos is presented which includes stereoscopic DIBR and The details of Multi-view and some of its related work were presented. [2] To surmount the drawbacks of a digital video watermarking algorithm, this paper presented a novel robust video watermarking scheme based on a combined technique of discrete cosine transform and discrete wavelet transforms. This proposed scheme is easy to be implemented since it uses random frames with no special requirement for video frames[3]. Video watermarking is one of the most interesting technologies in the process of digital television development. will always be digital watermarking that is based on the Scalable Part of H.264 over a large range of bit-rates including in MPEG-4-Scalable Video Code (SVC). Unfortunately, the such algorithms of watermarking which are used for H.264/SVC framework cannot meet this requirement of copyright protection. This paper extended the existed framework for invisible watermark- before adopting the Discrete Cosine Transform with a scalable algorithm which can apply the multi-resolution property of a watermarking algorithm of the H.264/SVC.[4] An innovative structure of the proposed method is the DWT-based blind digital video with the scrambled watermark and error control scheme for copyright protection of digital watermarked images. correcting code. This scheme incorporates various segments of one watermark into different scenes of a video under the wavelet domain. It enhances the strength of the scheme since the error some of them are refining the watermark correcting code improves the correcting. code is synchronized and it is watermarked in an audio channel. This video Here the used watermarking algorithm is able to withstand frame attacks of the high level. decreasing, averagely or statistically analyzed in a way that they were not problems that has solved effectively in the past. [5] Discrete wavelet transform, Discrete cosine transform, bacterial foraging optimization (BFO) and Particle swarm optimization (PSO) techniques are more successful and reliable. It confirms and goes further the empirical application of the mization and analyzes their performance with intent to embed the watermark in the medical image. PSNR NCC, normalized cross correlation) a two dimensional correlation peak signal signal to noise ratio, PSNR (peak signal to noise ratio) a value. The correlation, represented by the symbol R, and the image fidelity, represented by the symbol IF, has been determined in order to prove correlation between the applied algorithms' efficiency. comparative aspect of such algorithms' performance. The In other words, a high PSNR and an NCC must be achieved to accomplish very good embedding. of message.[6]

The watermarked images denoising effect that a Fully Convolutional Neural Network (FCNN) has, as a denoising attack. The deep architecture aids in an improved training process and enhances the performance in terms of removing the noise but still keeping the detailed structure of the image.[7]

The watermark encryption and decryption method will help to reduce to copy any video content which is sensitive. This script helps client too effectively to encode, decode or reset to unique configuration by choosing any video from nearby system. To install a secret watermark to advanced media is a definitive objective of watermarking framework.

Advanced watermarking innovation is an arising field in PC science, cryptology, signal handling and interchanges. We have examined the calculations for watermarking of picture as a feature of the task. The watermarking research is more invig-

Fig. 2. Watermarking trade-off properties

orating as it needs aggregate ideas from every one of the fields alongside Human Psychovisual examination, Multimedia and Computer Graphics. The watermark might be of noticeable or imperceptible sort and each has its own applications[8]

Recent attention in watermarking, mainly through the incorporation of deep learning principles, has been targeted at video content with the embedding of signatures. The method has several important advantages over the existing methods in watermarking since it provides a great accuracy and better results in comparison with most of the existing works in the approach where superior learning capabilities are established. This paper presented a comprehensive overview of the recent achievements in video watermarking based on deep learning. The reviews are categorized based on the network architecture used; therefore, it represents a summary of the state of the art in the field. This paper concludes by considering potential future avenues of research on deep learning-based video watermarking Two methods were adopted to embed the watermark into video. The first way was DCT-based and the second one based on the SVD-based algorithm for video to transform it into frequency domain. For both techniques, the embedding process of the watermark was carried out after the original video was divided into a set of frames, and one frame was divided into a block of 8 x 8, and the DCT and SVD is performed on each block. [9]

III. Methodology

A. Techniques used

RDWT is an abbreviation for Redundant Discrete Wavelet Transform. It’s a variation of the conventional DWT (Discrete Wavelet Transform) used in digital signal processing like digital video watermarking.

Here are some key points to note about RDWT in digital video watermarking: 1.Redundancy: Unlike DWT, which is redundant in nature as it does not down-sample a signal, RDWT results into more coefficients but with the same resolution at all decomposition levels. 2.Shift Invariance: The shift-invariant feature of RDWT makes it more resistant to geometrical attacks such as cropping, translation and rotation. This property is very important for watermarking since the latter helps in retaining the watermark even after such alterations. The Wavelet Transform used is Haar Wavelets.It is an well-known wavelet for signal processing and especially applicable to digital video watermarking with RDWT. It is a type of wavelets, which has the simplest rectangular shape. It’s Simplicity ,The Haar wavelet is the simplest orthogonal wavelet, which models for a pair of basic functions.A scaling function (tents or intervals) known as father-wavelets and another one called mother-waveletes.Haar wavelets are easy to compute because they have piecewise constant basis functions Piece-wise Constant The Resolution of the Haar wavelet transforms this signal into two parts at each level - the average (also approximation) and detail.

B. Workflow for Embedding Process

The steps are as follows

A. Frame extraction: It involves taking out the frames from a video sequence.

B. Apply RDWT to each frame, generating many sub-band coefficients.

C. After the step of creating wavelet coefficients, insert a watermark to put robustness in water mark we embed it into high frequency sub-bands by taking LH,HL and HH.

D. Then applying inverse RDWT to produce reconstructed watermarked frames.

E. If we compile all of the watermarked frames back together, we will have the video sequence reconstructed.

we implemented Redundant Discrete Wavelet Transform using the Haar wavelet. The process involves:

- Frame Decomposition: We apply Haar wavelet transform on each video frame which de-composes it into different sub bands (LL, LH HL, HH)
- Redundant Transform: In contrast to standard DWT, the RDWT does not involve down-sampling; therefore each sub-band has equal size as original frame which guarantees redundancy.Watermark Embedding will be added to corresponding sub-bands, which are LH channel, HL channel and HH channels for balancing time by considering robustness while keeping invisibility.
- Inverse Transform: Reconstruct the watermarked frames by applying inverse Haar wavelet transform.Make sure to choose Extract Frames which extract frames out of the original video sequence.Haar wavelet transform is applied individually to each frame thereby resulting in four sub-bands.If necessary, repeat the procedure a few times to achieve multi-level decomposition.
- Watermark Insertion is done by selecting sub-bands (mainly LH, HL, HH) for watermark embedding.The watermark is then embedded by modifying the coefficients of selected sub-bands.
- Then, apply the inverse Haar wavelet transform 3 to reconstruct the watermarked frames.Rebuilding the video involves putting together the watermarked frames to form a sequence of the original video.

The Haar wavelet model is useful for RDWT-based digital video watermarking because it simplicity and efficiency. This presented a more direct manner to extract and embed video frames which also secures robustness of the watermark in embedding process, yet it has not caused much destruction on original quality.

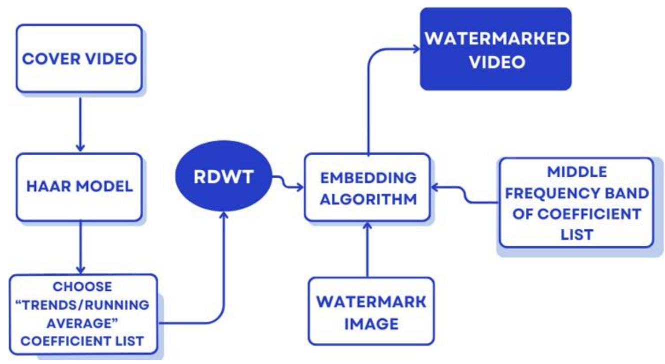

Fig. 3. Flowchart for Embedding of watermark

C. *Workflow for Extraction Process*

The flowchart of a process for extracting a watermark from a video. The first step is to use a Haar model to extract the watermark from the cover video. Haar features are elementary building blocks for object detection. In this case, the Haar model is likely used to detect the specific watermark within the video.The next step involves choosing between "Trends" or "Running Average" and then using a coefficient list. It's possible this step involves filtering the extracted watermark to remove noise or other unwanted signals.

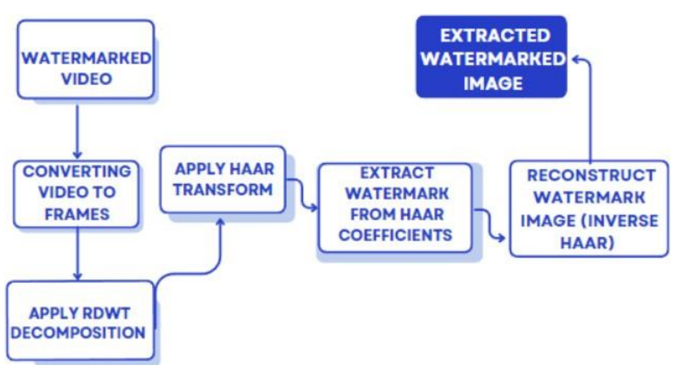

Fig. 4. Flowchart for extraction of watermark

The final step is RDWT (Redundant Discrete Wavelet Transform) which is used to extract the middle frequency band of the coefficient list. This might be where the watermark information is encoded.ln conclusion, this block diagram appears to show a process for extracting a watermark from a video using a Haar model, filtering, and then isolating the watermark information in a specific frequency band.

D. *Measurements for Analysis*

To evaluate the strength of a watermarking algorithm in terms of robustness and invisibility, the following are the metrics used to test the ability of the algorithm.

1) Invisibility evaluation metrics: The term being used is Peak Signal to Noise Ratio (PSNR) This is the amount of signal power to the disturbing noise power that degrades representation quality. As many of the signals are exhibited an enormous dynamic range, or the ratio between the largest and smallest possible of a variable quantity the PSNR is usually expressed in decibel scale logarithm.Therefore, it becomes imperative to develop numerical methodologies to quantify impacts that image enhancement algorithms have on image quality.

$$PSNR = 10log10(255^2/MSE) \quad (1)$$

The term SSIM comes from Structural Similarity Index and that is what it is – an image quality measure. In connection with this the SSIM index must be made with reference to the reference image in relation to the current image. The reference image is often needs to of perfect quality. This quantitative measure employs Structural similarity (SSIM), Contrasts and the Structural information between the two images, to arrive the at the SSIM value.The brightness of the two signals average value which represents the two images signals is Luminance. It is determined in accordance with the standard density to keep pace with the champion basin.It denotes the SSIM of two images as follows where

μ_x and μ_y represent the means of the two images, and $\gamma^2_x \gamma^2_y$ represent their variances

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + k_1)(2\sigma_x\sigma_y + k_2)}{(\mu_x^2 + \mu_y^2 + k_1)(\sigma_x^2\sigma_y^2 + k_2)}$$

There are constants k1 and k2, which exist to avoid a 0/0 calculation. In the default, k1 =0.01 and k2 =0.03.

2) Robustness assessment metrics

$$NC(X,Y) = \frac{1}{WH}\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}\delta(X_{i,j},Y_{i,j}),$$

$$\delta(X,Y) = \begin{cases} 1, & \text{if } X = Y \\ 0, & \text{otherwise} \end{cases}$$

Normalized Correlation (NC) is a score for two signals that measures their similarity in the form of a relative displacement function. NC has values in the interval [0,1], such that value, which represents higher image similarity. NC between the original image A and the extracted image B is given by the equation below: The robustness of the proposed method is verified if the NC is approximately equal to 1.

IV. Python based implementation

Cover video is loaded using the OpenCV library in Python, which deals with computer vision. Then the secret message is

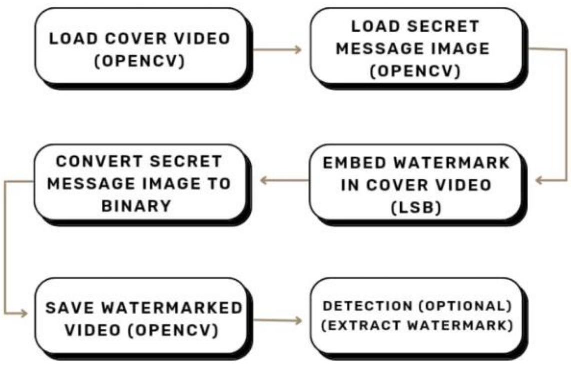

Fig. 5. Implementation using python-Embedding

loaded using OpenCV.This converts the secret message into a type of binary, which is in the sequence of 0s and 1s. The watermark is embedded into the cover video using the Least Significant Bit (LSB) substitution method. The method involved was altering least significant bits of frames of the cover video to hide the watermark.The watermarked video is saved using OpenCV.

Detection is Optional it detects and recovers the watermark If needed, it can retrieve and detect the watermark from the watermarked video itself. It reads the watermarked video frame by frame, extracts the watermark from each frame, and saves the extracted watermark.

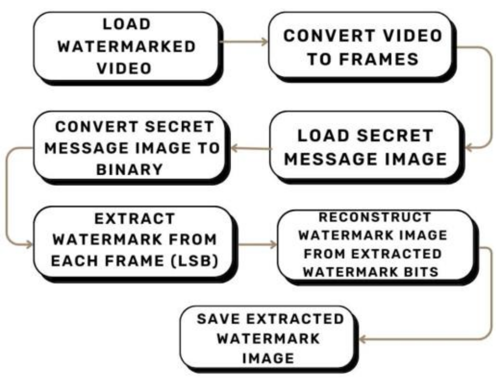

Fig. 6. Implementation using python-Extraction

This flowchart shows how the our code extracts a watermark from a watermarked video based on the method of Least Significant Bit (LSB) extraction. The watermarked video and the secret message image are to be initialized; the secret message will be passed as an image and is to be converted into a binary secret message; there will be extraction of a watermark from the number of frames of the video by comparing the least significant bits of each pixel to the binary secret message; and finally, the watermark bits are reconstructed to an image and saved.

The code uses OpenCV for video and image processing and NumPy for binary operations. For simplicity, assume that the size of the secret message containing an image is less than the size of the cover video frame, and only a very elementary LSB extraction method is used.

V. RESULTS AND DISCUSSIONS

The performance of digital video watermarking code in Python for embedding and extracting watermarks is optimized through the use of its powerful libraries and efficient handling of computational tasks. Libraries like OpenCV facilitate rapid video processing, while NumPy and PyWavelets streamline numerical computations and wavelet transforms.
These libraries enable the efficient embedding of watermarks into video frames and the swift extraction of these watermarks when needed. We have observed an increase in the robustness of the watermarked video as well as the increase in PSNR,SSIM,NC values as calculated in the output of the code.

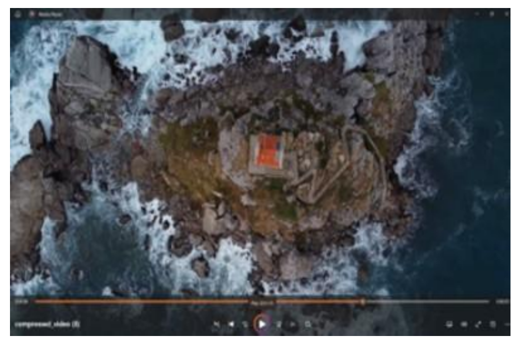

Fig. 7. Cover Video

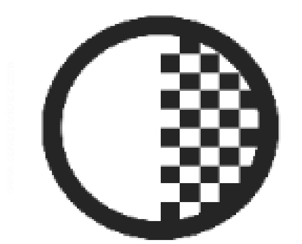

Fig. 8. watermark image

SSIM values of both the videos remain closely constant showing the structural similarity remains same even if the video is compressed,whereas the PSNR value gets better for the compressed video with an adjusted bitrate to the original watermarked video.

The NC values are calculated using the original watermark and the extracted watermark. For minor changes and to get a clear watermark we can enhance and denoise the extracted watermark and measure the NC value for them as well

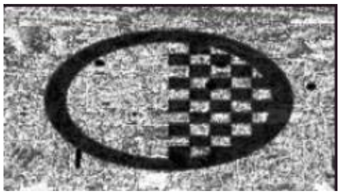

Fig. 9. extracted watermark image

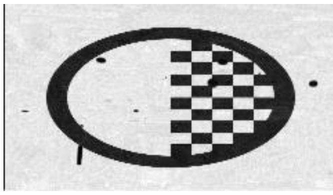

Fig. 10. extracted watermark image after enhancement

Video format	SSIM	PSNR
Watermarked video	0.91	28.5
Compressed video	0.92	31.0

TABLE I
PSNR AND SSIM VALUES OF WATERMARKED AND COMPRESSED WATERMARKED VIDEO

Value	Extracted	Enhanced	Denoised
NC	0.86	0.92	0.93

TABLE II
NC VALUES OF EXTRACTED ,ENHANCED AND DENOISED WATERMARK

VI. CONCLUSION AND FUTURE WORK

A. Summary of Findings

The combination of simplicity, efficiency, and robustness makes the use of Haar transformation and Python in digital video watermarking a good idea. Haar transform is very fast in computations hence can be used in real time applications or systems while Python has simple syntax that is easy to understand especially when used with libraries such as OpenCV and NumPy that help to further improve how code works. It's also resilient to most common attacks such as compression and noise therefore ensuring the durability of watermarks. Additionally, the presence of large supportive community and resources for Python facilitate development and troubleshooting processes. The Haar transform integrated with Python's extensible ecosystem compared to other types of transformation delivers a viable solution which is cheap, cross-platform based and adjustable hence being ideal for watermarking videos. Digital video watermarking using the Redundant Discrete Wavelet Transform (RDWT) provides enhanced robustness and imperceptibility compared to traditional transform techniques. RDWT's shift-invariance property allows for better preservation of watermark information even after various video processing operations, such as compression and scaling. This technique mitigates the artifacts commonly introduced by other methods, ensuring that the watermark remains invisible to viewers while being resilient against attacks. Additionally, RDWT maintains the spatial resolution of the video, making it ideal for high-quality applications. Its integration with Python's powerful libraries and extensive community support further simplifies implementation, enabling the development of sophisticated and reliable watermarking solutions.

B. Addressing Challenges and Future Recommendations

In the future, machine learning approaches for adaptive watermarking which increase robustness against attacks should be leveraged for digital video watermarking using Python and RDWT with the Haar transform. Investigating GPU acceleration and parallel processing can greatly boost real-time application performance. Improving RDWT's integration with further advanced transforms could result in increased resilience and imperceptibility. The watermarking process can also be made more efficient by concentrating on maximizing code efficiency and minimizing computational overhead. Updating frequently and taking advantage of Python's developing environment will provide cutting-edge digital video watermarking solutions.

While RDWT with Haar transform offers a solid foundation for digital video watermarking using Python, future advancements can push its capabilities further. Consider exploring techniques like SVD for embedding to enhance robustness against attacks. The system can be improved by adapting watermark strength to video content and implementing robust authentication methods. Additionally, research into blind watermark extraction (not requiring the original video) and integration with deep learning for watermark generation can improve practicality and robustness.

REFERENCES

[1] Mansour, S., Jabra, S. B., and Zagrouba, E. (2023). A comprehensive review of video watermarking technique in deep learning environments. https://doi.org/10.1109/cw58918.2023.00020

[2] Asikuzzaman, M., and Pickering, M. R. (2017). An Overview of Digital Video Watermarking. IEEE Transactions on Circuits and Systems for Video Technology https://doi.org/10.1109/TCSVT.2017.2712162

[3] Jie, Sang and Qi, Liu and Chun-Lin, Song. (2020). Robust video watermarking using a hybrid DCT-DWT approach. Journal of Electronic Science and Technology. 18. 100052. 10.1016/j.jnlest.2020.100052.

[4] Sun, Yanfei and Wang, Junyu and Huang, Haozhi and Chen, Qing. (2020). Research on scalable video watermarking algorithm based on H.264 compressed domain. Optik. 227. 165911. 10.1016/j.ijleo.2020.165911.

[5] Chan, Pat and Lyu, Michael. (2003). A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code. 202-213. 10.1007/978-3-540-39927-8.

[6] Bharati, Subrato and Rahman, Mohammad and Podder, Prajoy. (2019). Analysis of DWT, DCT, BFO and PBFO Algorithm for the Purpose of Medical Image Watermarking. 10.1109/CIET.2018.8660796.

[7] Hatoum, Makram and Couchot, Jean-Franc¸ois and Couturier, Raphae¨l and Darazi, Rony. (2021). Using Deep learning for image watermarking attack. Signal Processing Image Communication. 90. 116019. 10.1016/j.image.2020.116019.

[8] Abhishek Bajaj. (2022) Implementation Of Video Digital Watermarking Based on Python

[9] Fathe, Eman and Salih, Meaad. (2020). Digital Video Watermarking Methods using DCT and SVD.

[10] The implementation of the proposed method is available at: Click here