SYSTEMATIC REVIEW AND SIMULATIVE COMPARISON OF VIDEO WATERMARKING SCHEMES

HAWEEZ SHOWKAT\textsuperscript{1}, ROHUN NISA\textsuperscript{2} , Dr. ASIFA BABA\textsuperscript{3}

\textsuperscript{1,2,3} Islamic University Of Science and Technology, J&K, India

E-mail: haweezsk@gmail.com \textsuperscript{1}, rohunnisa@islamicuniversity.edu.in \textsuperscript{2}, asifababa@gmail.com \textsuperscript{3}

ABSTRACT

These days, one of the most sought-after data security study areas is watermarking. Innumerable techniques have been developed to achieve better results in terms of robustness and perceptual quality which are generally in a tradeoff mode. In order to get insight into current trends in the watermarking area, a non-exhaustive assessment of research publications was done in order to weigh the advantages and disadvantages of each one. This paper's primary contribution is a comparison of simulation results for video watermarking using SVD, DWT-SVD, LWT-SVD, RWDT-SVD, and SVD-APDBCT, which provides an understanding of different assessment parameters. Watermarked videos with various noise attack variations have been subjected to simulations, and comparison analysis for fidelity and resilience in terms of PSNR and CC is obtained.

Keywords: SVD, DWT, RDWT, LWT, APDBCT.

1. INTRODUCTION

In the present scenario of high technology where new methods of information broadcasting and communication have come into existence, it’s a challenge to secure the information transferred through an open communication channel. Along with the new ways of communication, new techniques of modification of data due to which spreading rumors and wrong information has become a norm. Illegally downloading videos has become a big problem for copyright owners, as high speed internet has aided the process. Watermarking came as a solution to these problems, where an invisible information is embedded in the frames of video, which can be extracted by the owner at the time of extraction so as to authenticate the ownership disputes. The watermark can be extracted on the receiver side only by the dedicated detector so as to uphold the rights of IPR (intellectual property rights) holders. The main aim of this paper is to analyze some basic watermarking techniques which will give researchers an insight of which scheme has advantage over the other.

1.1 Watermarking schemes should have the following attributes.

a) Robustness: It gauges the watermarking scheme's potential to become redundant in the face of both deliberate and unintentional attacks. Once the watermark has been removed, it ought to be able to verify the intellectual property rights holders' ownership.

b) Perceptual quality: The degree of distortion a watermark adds to the cover signal is another name for it. In this day and age of HD TVs, we cannot afford to compromise on visual quality any longer. Consequently, the watermark must be as subtle as possible in terms of fidelity to maintain the video's commercial worth.

c) Time consumption: Increasing complexity in video watermarking directly extends processing time, posing a challenge for real-time applications like live videos. High time consumption compromises the feasibility of timely watermarking, essential for seamless integration in dynamic scenarios.

d) Data Payload: Capacity, in the context of watermarking, gauges the information storage potential within a cover signal. It quantifies the bits of the watermark embedded in the image, aiming for sufficiency to convey the uniqueness of the extracted watermark. The optimal balance ensures effective representation and retrieval of the embedded information.

e) Trustworthiness: Certainly, the primary objective of watermarking is to establish ownership verification for the authorized party. The underlying scheme must guarantee that unauthorized entities are unable to generate counterfeit watermarks during the extraction
process, ensuring the integrity and authenticity of the ownership verification mechanism [57].

The surge in video transactions has brought forth a proliferation of security challenges. Illicit distribution, facilitated by the ease of uploading and downloading, poses a threat to video content. Watermarking emerges as a crucial solution, safeguarding intellectual property rights and mitigating unauthorized copying. Another issue arises during video transmission, where tampering distorts content, spreading misinformation. Watermarking addresses this by enabling tamper detection, embedding watermarks in video frames not only enhances security but also increases data hiding capacity. This allows for the transmission of additional information within the same bandwidth without compromising perceptual quality, addressing both social and technical challenges in the evolving landscape of video transactions.

1.3 Watermarking Classified According To Domains:

Watermarking, a crucial aspect of securing digital content, offers diverse approaches categorized into spatial and frequency domains.

1.3.1 Spatial domain: In the spatial domain, the Least Significant Bit (LSB) method is prominent, leveraging the property of LSB to be inconspicuous to the human eye. This technique involves substituting the LSB of each pixel with the Most Significant Bit (MSB) of the corresponding watermark pixel, constituting a straightforward watermarking process. However, it is susceptible to pixel-to-pixel attacks, potentially enabling the removal of the watermark.

1.3.2 The basic mathematical tools used in frequency domain watermarking are as follows:

a) DCT: The Discrete Cosine Transform (DCT) is a frequency-based image transformation, expressing images in terms of sines and cosines. Developed to address vulnerabilities in Least Significant Bit (LSB) techniques, it enhances robustness in watermarking applications. Offering efficient energy compaction, it is particularly effective for highly correlated image data[58]. However, its computational complexity and time-consuming nature pose challenges. DCT’s susceptibility to geometric attacks, such as rotations or scalings, is a notable limitation. It is further categorized into Global and Block-based watermarking methods. Global methods apply the watermark uniformly to the entire image, while Block-based methods partition the image for localized application, offering a flexible approach to address specific regions and enhance resistance against attacks. Despite computational complexities, DCT remains a crucial tool in image processing for its ability to balance compression efficiency and robustness in watermarking[32].

b) APDBT: When the image is compressed utilizing the DCT with a Window that has low bit rates, some of its negative characteristics are left unaddressed [65] like block artifacts. The application of the APDCBT (all phase discrete cosine biorthogonal transform) transform solves this problem since, in comparison to the standard DCT, it performs well at both high and low frequencies. Due to its effectiveness, the APDCBT has been extensively utilized in both general image processing and specific watermarking applications. The APDCBT transform performs exceptionally well in low-frequency aggregation and high-frequency attenuation when compared to the traditional DCT transform [67].

c) DFT: In the context of image processing, the Discrete Fourier Transform (DFT) utilizes complex-valued coefficients, offering insights into phase and magnitude [19]. Optimal embedding results are observed in mid frequencies, with central coefficients representing low frequencies showing the strongest performance. Notably, DFT boasts advantages in rotational, scaling, and translational invariance, outperforming techniques like Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) in geometric attacks such as cropping, rotation, and scaling. However, a significant drawback is the loss of all time-related information with DFT, limiting its applicability in scenarios where time dynamics are crucial for analysis or interpretation. Despite this limitation, DFT’s resilience against geometric attacks makes it valuable in various image processing applications.

d) DWT: The Discrete Wavelet Transform (DWT) provides a comprehensive representation by analyzing both spatial and temporal domains of
an image [36]. It partitions the image into four blocks - LL, LH, HL, and HH. LL carries maximum image information, while LH, HL, and HH capture vertical, horizontal, and diagonal details, respectively. This hierarchical decomposition, with potentially multiple levels, is achieved through high band filters, including Haar, Daubechies orthogonal filters, and bi-orthogonal filters. DWT’s multi-level approach aligns with the human visual system, offering a nuanced understanding [28]. Notably, DWT addresses blocking effects/artifacts associated with block-based schemes, a significant improvement over embedding techniques. However, this advancement comes at the cost of increased computational complexity compared to techniques like Discrete Cosine Transform (DCT). Despite this, DWT’s ability to capture diverse image details positions it as a valuable tool in image processing.

e) LWT: Similar to DWT, the Lifting Wavelet Transform (LWT) divides an image into four bands, consisting of one detailed and three approximation coefficients. In contrast to DWT, LWT is reversible. LWT’s three fundamental processes—split, predict, and update—contribute to its superior image quality restoration after embedding. On the other hand, DWT excels in robustness against specific attacks such as JPEG compression and low-pass filtering. The choice between DWT and LWT often depends on the specific requirements of the application, with DWT offering reversibility and robustness, while LWT stands out in terms of image quality restoration.

f) RDWT: The Reversible Discrete Wavelet Transform (RDWT) distinguishes itself by eliminating up-sampling and down-sampling coefficients, preventing a reduction in image size. This modification enhances payload capacity and addresses the shift invariance issue present in the traditional Discrete Wavelet Transform (DWT). RDWT demonstrates robustness against various attacks, including geometric and non-geometric noise attacks, with exceptions for cropping and rotation [53]. Comparative studies have shown RDWT’s superiority over the Discrete Cosine Transform (DCT) by avoiding blocking artifacts at image boundaries. Additionally, RDWT outperforms the conventional DWT in terms of image quality [54], making it a promising choice for applications where maintaining image fidelity and robustness against specific attacks are crucial considerations.

g) IWT: The Integer Lifting Wavelet Transform (ILWT) is a variant of the Lifting Wavelet Transform (LWT) that uniquely maps input data to integers, ensuring a lossless reverse process. Renowned for superior computational efficiency compared to LWT, ILWT is both reversible and characterized by minimal quantization errors [55]. Diverging from the traditional linear approach, ILWT introduces split and merge steps instead of up-sampling and down-sampling, marking it as a nonlinear transform. This nonlinearity, coupled with reduced computational costs, positions ILWT as an advantageous choice for real-time video processing applications where preserving information integrity, minimizing errors, and optimizing computational resources are crucial considerations. Its ability to maintain data fidelity while enhancing computational efficacy makes ILWT a valuable tool in various signal processing scenarios [56].

h) SVD: The Singular Value Decomposition (SVD) exhibits remarkable stability in its singular values, ensuring minimal impact on image quality even after embedding. The descending arrangement of the S matrix implies that alterations to smaller values have limited influence on image quality [54]. Notably, SVD's non-fixed orthogonal basis distinguishes it from techniques like Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT), contributing to its enhanced robustness. SVD's inherent difficulty in removing watermarks enhances its security. Additionally, the singular values carry significant energy from the image, making them an efficient payload for watermarking applications. In summary, SVD's stability, robustness, and payload capacity contribute to its effectiveness in watermarking and image processing scenarios [57].

1.4 Classification according to the information required during the extraction process:

a) Non-Blind: Requires the original cover image, the complete watermark image, and a secret key for successful extraction. This method is explicit and demands all components during the process.
b) **Semi-Blind:** Involves extracting information with only a section of the watermark image and the secret key. This approach provides a balance between information security and partial disclosure during the extraction process.

c) **Blind:** Achieves extraction solely based on the secret key without requiring the original cover image or the complete watermark. This method emphasizes minimal information disclosure during the extraction phase, offering a high level of privacy and security.

2. **Literature survey**

In this section some of the best research papers have been discussed to give a broad insight of watermarking techniques.

A resilient least significant bit (LSB) watermarking approach tuned for structural similarity was proposed by Dehkordi A. et al. in [16]. An adaptive method embeds the watermark into the host image. Every block in the host image has undergone embedding until a certain threshold for structural similarity is reached. After a number of attacks on the embedding technique, simulation results showed that the watermarked sequence could be retrieved with an optimal level of accuracy. The drawback of this suggested strategy was that pixel-by-pixel attacks could easily remove the watermark.

A unique Discrete Fourier Transform (DFT) watermarking system with perceptually-optimal visibility versus robustness was proposed by Urvoy M. et al. in [19]. The watermark in this suggested system is a square patch of coefficients that resembles noise, and it is embedded in the Fourier domain using a substitution method. The information is stored in the phase component, whereas the amplitude component modifies the watermark's strength. The aforementioned methodology demonstrated resilience against multiple attacks, including pixel-to-pixel attacks. However, due to the utilization of DFT, the method encountered symmetry constraints.

In order to prevent illegal copying or verify the media's provenance, C. Hsu et al. [18] suggested using watermarking to encrypt secret information into the signals. The suggested approach makes use of prediction kinds of MPEG bit streams with varying residual masks to insert watermarks into both intraframe and non-intraframe content. According to the testing results, the suggested watermarking technique produces an essentially imperceptible difference between the original frames and the watermarked frames, which facilitates MPEG compression and robust cropping.

For the protection of digital media, Divjot et al. in [1] presented a strong watermarking technique. To extract high frequency bands from video frames, this approach applies the Discrete Wavelet transform. The watermark is embedded in each frame by applying Singular Value Decomposition to these bands and utilizing their unique values. Video frames and watermarked video are extracted during embedding by applying an inverse discrete wavelet transform. Blur and Gaussian noise attacks, among other types of attacks, are among the several attacks that the author has tested the suggested scheme against in watermarked video.

The watermarked image is divided up into four sub-band wavelets at the receiving end of the DWT transmission. To obtain singular values, the SVD block is treated with the wavelet coefficient applied to it for the purpose of extracting. The suggested approach uses a scale coefficient of 0.02 to extract the watermark. The computation of PSNR and CC is used to evaluate the strategy. The PSNR obtained in the presence of Gaussian noise with a variance of 0.01 is 33.2908 dB. This approach has the advantage of taking into account a variety of noise attack types, which increases system reliability. The PSNR and correlation coefficient increase noticeably with each noise attack. Furthermore, the issue of false alarms has not been resolved.

Hemdan et al. [2] introduced a hybrid image watermarking approach utilizing Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The fusion of multiple watermarks is executed through the DWT wavelet fusion algorithm, enhancing data hiding capacity. The cover image and watermark undergo frequency domain conversion and are divided into four sub-bands using DWT. SVD is then applied to extract singular values from the frequency bands, embedding the fused watermark utilizing scaling coefficients. In the extraction phase, an anti-fusion process is applied to recover individual embedded watermarks. The proposed scheme demonstrates a PSNR of 20.69 for the cover image under Gaussian noise with a variance of 0.01. It outperforms traditional watermarking techniques in terms of robustness and perceptual quality, with the SVD-transformed image exhibiting high stability in
singuar values. The use of multiple watermarks enhances data hiding capacity and system security, although the scheme does not consider the computational time in the watermarking process, and the impact of various noise attacks is relatively less in this paper as many of them are not considered.

Schemes utilizing Singular Value Decomposition (SVD) for image watermarking have gained popularity for balancing robustness and imperceptibility. Nonetheless, the primary drawback lies in the false positive problem (FPP) associated with SVD-based watermarking schemes.

Tabasco et al. [20] proposed a 3-Level DWT (Discrete wavelet transform) based digital video watermarking scheme. The video is converted into identical frames by comparing the pixels of each frame. Blue channel is obtained and it is converted into 3 level frequency domain using DWT. The watermark is converted into a binary signal and then embed into the middle and high frequency coefficients of the frames. The embedding takes place in a sequence, high frequency coefficients are embedded first preceding the lower frequency coefficients, which increase the invisibility of the watermark. 3-Level IDWT is applied to generate watermarked video. Blue channel is used for embedding purpose, which is least sensitive to human visual system, so as to increase the robustness. Original video is not required at the time extraction of watermark. The proposed scheme performs well in terms of Gaussian noise, Salt & pepper noise adding, frame dropping and frame adding noise attacks.

The major limitation of this work is that the embedding time required is too much . Robustness is limited for a certain range of noise factor

Zhang et al. [13] introduced a state-of-the-art digital watermarking technique incorporating adaptive elements and utilizing Radial Basis Function (RBF) neural networks. The methodology commences with the conversion of the cover image into the frequency domain through the Discrete Cosine Transform (DCT). The watermark, structured as a visually identifiable binary image, undergoes encryption employing a chaos series. Utilizing a secret key, the encrypted watermark is mapped and segmented into 8x8 blocks, subsequently being embedded into the mid-frequency components of the cover image using block-based DCT. The three-layered RBF-trained model plays a pivotal role in determining the strength of the watermark, aiming for maximum potency with minimal perceptibility. The nonlinear radial basis function acts as the activation function in this intricate process. Notably, RBF not only amplifies the Peak Signal-to-Noise Ratio (PSNR) but also enhances watermark robustness, surpassing the capabilities of Artificial Neural Networks (ANN) in terms of simplicity, improved approximation, and swifter learning algorithms.

Despite the computational complexity associated with DCT, the proposed scheme exhibits heightened robustness when contrasted with Least Significant Bit (LSB) techniques. However, it does reveal limitations when confronted with geometric attacks. The proposed approach showcases a comprehensive advancement in digital watermarking, striking a balance between complexity, robustness, and perceptual quality

S. B. Fatima et al. in [5] introduces a novel watermarking scheme using Lifting Wavelet Transform in which a grey scale image is converted into frequency domain using Lifting Wavelet Transform. The high frequency band of an image has been utilized to embed the watermark. In this proposed scheme the high frequency bands of grey scale cover image is embedded with the watermark image. The process of embedding is utilized in order to modify the singular values of HH band of cover image by the singular values of the watermarked image. Subsequently, the signature is generated using orthogonal values which are later on embedded in 4th level of low bands frequency bands of the cover image.

During extraction phase the signature is extracted from 4th level of low frequency bands which is later on compared with the signature extracted during embedding process. If the two signatures match with each other the algorithm proceeds with watermark extraction, to remove false positive detection. Reverse process is performed in order to obtain the watermark from the cover image.

Advantage of this scheme is that false positive rate is taken into consideration. The proposed technique proved to be efficient in terms of memory and time consumption as LWT is better than DWT. However SVD when used on whole image requires lots of memory. Only Jpeg compression noise attacks have been taken into consideration.

Praful et al. [9] proposed an innovative watermarking scheme utilizing Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD). The cover image undergoes decomposition into four frequency sub-bands using DWT. An
Inverse Discrete Wavelet Transform (IDWT) is then applied specifically to the high-frequency coefficients. Singular values are subsequently evaluated for the high-frequency image. Through the incorporation of the watermark and scaling coefficients, these singular values undergo modification, resulting in the creation of the modified high-frequency image. Further, DWT is applied to obtain high-frequency coefficients, followed by the application of IDWT to generate the final watermarked image. The use of SVD contributes to robustness, particularly in geometric attacks, as embedding occurs in high-frequency bands, minimizing perceptual quality impact. Despite the advantages, the scheme introduces increased memory and time requirements due to the application of DWT. Specifically, utilizing SVD on the entire image demands substantial memory resources. The method capitalizes on SVD's stability, preserving perceptual quality when embedding in singular values. However, the trade-off involves heightened computational demands associated with the DWT process, warranting consideration for practical implementation and system constraints. The proposed scheme represents a balanced approach, leveraging the strengths of both DWT and SVD while acknowledging the associated resource implications.

In the image watermarking scheme proposed by Kashyap et al. [21], a 3-level Discrete Wavelet Transform (DWT) is employed on a grayscale cover image to extract lower frequency bands. The watermark image is then embedded within these lower-frequency bands using the Alpha Bending technique, which is also utilized for the extraction of the watermark. While the approach capitalizes on the frequency localization capabilities of DWT, offering potential advantages in robustness, it is not without challenges. One notable drawback of this technique is the substantial demand for time and memory during processing. The computational requirements may limit its applicability in real-time systems or environments with resource constraints. Additionally, the use of DWT introduces aliasing problems, a phenomenon where high-frequency components are erroneously represented as lower frequencies, potentially leading to artifacts in the watermarked image. The smoothness inherent in DWT may impact image details, affecting the perceptual quality. Addressing these issues is crucial for the practical implementation of the proposed scheme, emphasizing the need for a balance between watermark robustness and computational efficiency in image watermarking applications.

Li D et al. [24] introduced a watermarking scheme leveraging Convolutional Neural Networks (CNN) for embedding watermarks in images, specifically designed for smart city applications. The approach integrates Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for embedding and extraction processes. While CNN enhances robustness, offering effectiveness in smart city contexts, it comes with certain challenges. The utilization of DWT, despite its effectiveness in frequency analysis, imposes significant memory requirements, potentially limiting its applicability in resource-constrained environments. Moreover, CNN's reliance on extensive datasets for training poses a notable drawback. Achieving a balance between the benefits of DWT, SVD, and CNN, and addressing associated memory and data challenges, is critical for the successful deployment of this watermarking scheme in practical smart city applications.

An RDWT, SVD based watermarking technique is presented in [50]. Every 4*4 block in the image has its HVS entropy computed for it. In order to decrease distortion and increase imperceptibly, watermarks are embedded in the least distortion places found by the HVS entropy. On bands that do not overlap, RDWT is used. To obtain the singular and orthogonal 4*4 matrices, SVD is performed to the LL bands. To prevent false errors, the watermark is placed in the U2,1 and U3,1 matrices. The watermark is 32 by 32 in size. The ideal threshold for embedding is 0.15. To boost security, watermark encryption and decryption are done via Arnold scrambling. The system grows more intricate as more mathematical techniques are employed.

In [49], the author presents an innovative watermarking scheme that incorporates Discrete Wavelet Transform (DWT), Hessenberg Decomposition (HD), Singular Value Decomposition (SVD), and the Fruit Fly Optimization Algorithm (FOA). The cover image undergoes R-level DWT to decompose it into frequency domain components. HD matrix is then employed to decompose the square matrix obtained from R-level DWT, extracting precise components of the host image. SVD is used to obtain singular
values from the DWT-transformed images of the watermark and cover image, which are combined using scaling coefficients. The FOA is introduced in the embedding process to determine adaptive optimal scaling coefficients for each watermark, inspired by the flashing behavior of fruit flies. The scheme exhibits increased robustness as HD provides precise components of the host image. Although the implementation of FOA is straightforward with good optimization ability, the scheme becomes more complex. Notably, the system hasn't been tested for variants of salt and pepper noise, and the limitations of DWT, including reduced image size and shifting variance property, persist in this approach.

In [54] A semi blind watermarking technique has been introduced by the author, by applying the IWT on both cover and watermark images. The IWT transformed images are then applied with the SVD technique in order to get the frequency domain representation of both cover and watermark images. Singular values of watermark is embedded in singular values of cover watermark using optimized scaling coefficients. Further the optimization of scaling factor is used by employing an efficient ABC algorithm, in order to enhance the quality of watermark. False alarm problem has been addressed by using U and V matrices, to obtain the signature, using hash transform and XOR. This signature is later on embedded in HH band of the watermarked image. Advantage of this scheme is that the proposed technique takes into consideration the false alarm problem. IWT is better than DWT in terms of time consumption and memory requirements. ABC algorithm is used for optimization of scaling coefficient for efficient watermarking. However, as many methods are used, so system becomes complex, and time consumption is more.

In [54], the author introduces a semi-blind watermarking technique that involves applying the Integer Wavelet Transform (IWT) to both the cover and watermark images. The transformed images through IWT are then subjected to the Singular Value Decomposition (SVD) technique to obtain the frequency domain representation for both the cover and watermark images. The embedding of singular values of the watermark into the singular values of the cover is achieved using optimized scaling coefficients. To enhance watermark quality, an efficient Artificial Bee Colony (ABC) algorithm is employed for scaling factor optimization. Addressing the false alarm problem is done by utilizing U and V matrices to obtain the signature through hash transform and XOR, which is subsequently embedded in the HH band of the watermarked image. Notably, the scheme's advantage lies in its consideration of the false alarm problem, while the use of IWT proves advantageous in terms of reduced time consumption and memory requirements compared to Discrete Wavelet Transform (DWT). However, the inclusion of multiple methods contributes to increased system complexity and prolonged time consumption.

In [57], a scheme based on Singular Value Decomposition (SVD) is presented, aiming to address ownership disputes and enhance robustness in watermarking. The image undergoes transformation into three matrices, comprising two orthogonal matrices and one singular matrix. The watermark is then incorporated into the singular values using a scaling coefficient. This approach distinguishes itself from methods like Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT) that offer fixed orthogonal bases, as SVD provides non-fixed orthogonal bases. Notably, this method resolves the challenge of determining the optimal strength for embedding the watermark to achieve the most favorable outcomes. The introduction of SVD also facilitates the optimization of scaling coefficients. However, a potential concern arises with the false positive problem, wherein an intruder may generate their own watermark in the absence of the original watermark. This issue can be mitigated by implementing hybrid SVD algorithms, presenting an opportunity for further improvement in the robustness and security of the watermarking technique.

In [56], a video watermarking method is presented, employing Integer Wavelet Transform (IWT) and Arnold scrambling. Frames are extracted from the cover video, and with the application of IWT using a spline of 5/3, these frames are decomposed into four sub-images. The watermark undergoes initial scrambling through Arnold scrambling, followed by the application of Discrete Wavelet Transform (DWT) to obtain frequency sub-bands. The high-frequency band of the watermark is then embedded into the low-frequency band of the cover frames, utilizing a scaling coefficient of 0.03 and a specified threshold. The advantage of employing IWT lies in its low computational time, enabling the processing of videos in real-time scenarios. This scheme offers a novel approach to video...
watermarking, incorporating both IWT and Arnold scrambling to enhance security and robustness in the embedding process

In [48], a blind watermarking method has been presented, utilizing Redundant Discrete Wavelet Transform (RDWT), Improved Grey Wolf Optimizer (IGWO), and Principal Component Analysis (PCA). RDWT is applied to the cover image to obtain the coefficients in four frequency bands. The watermark undergoes binarization, is divided into blocks, and the principal coefficients are obtained through covariance calculation, reshaped according to the blocks. Inverse RDWT is then applied to generate the watermarked image. The frequency domain is optimized using the IGWO algorithm to obtain both the watermarked image and watermark. The scheme showcases enhanced performance with a newly optimized bandwidth detector. Various noise attacks are simulated to evaluate the scheme, employing metrics such as normalized correlation coefficient (NCC), peak signal-to-noise ratio (PSNR), structural similarity (SSIM) index, and mean square error (MSE). As down sampling step of DWT is removed in RDWT the scheme becomes less prone to noise attacks, which leads to increase in robustness. IGWO detector increases the time consumption efficiency and robustness of the scheme.

A zero-watermarking system with excellent efficiency was presented by Gao et al. [62] in 2021. It works in the polar complex exponential transform domain and uses Deep Convolutional Neural Network (DCNN) and Self Organizing Map (SOM) technology. This novel method represents a major breakthrough in video zero-watermarking, with the goal of improving system resilience and guaranteeing watermarked content's adequate equalization and distinguishability. The suggested system demonstrates a comprehensive integration of artificial intelligence approaches by merging the spatial organization skills of SOM and the feature extraction capabilities of DCNN. The focus on the polar complex exponential transform domain points to a calculated decision to maximize the transformation process, which could enhance the system's overall security against intrusions and preserve the integrity of the video information with zero watermarks.

In 2022, Gutub [63] proposed using a counting-based secret sharing technique to enable ownership watermarking in the presence of interfering multimedia video file fragments.

Ayubi et al. [64] created the two-dimensional secure video watermarking in 2021. It has proven possible to perform standard analysis of a dynamical system to show that chaos exists.

In [55] Chaotic multiple scaling factors (CMSF) are used to help a hybrid technique that combines SVD and IWT-based schemes for image watermarking. The process of watermark embedding involves applying 1level IWT to the cover image. The 1 level IWT's LL band is extracted, and the resulting coefficients are subjected to SVD. Using MD5 hash algorithms, the 128 bit secret key is obtained by summing the HH, HL, and LH bands and the mean of the watermark's modified histogram bins. The logistic G map is used to generate chaotic scaling factors. Because it requires less computing power than optimization techniques, it is superior. Lower bands are embedded with the watermark using SVD and created scaling factors. The watermark is transformed into a chaotic map, adding an additional layer of system protection. The secret key has been created to address false positive errors and boost payload capacity. The scheme's benefit is that it boosts security by transforming the watermark into a chaotic matrix. The issue of false alarms is resolved by creating a chaotic secret key. Compared to other optimization methods, chaotic logistic G map optimization offers superior computing efficiency. An additional benefit is an increase in payload. One of the scheme's drawbacks is that a lot of mathematical techniques were utilized in its execution.

A sine-cosine optimized neural network was proposed by Ingaleshwar et al. [61] in 2023, introducing a new method for video watermarking. This method, which takes advantage of the interplay between the optimization potential of the sine cosine algorithm and the concepts of neural networks, is a noteworthy scientific breakthrough. Ensuring the quality of the video footage while maintaining the smooth integration of secret data is the main objective of this approach. The researchers hope to achieve a compromise between preserving the video's integrity and guaranteeing reliable data embedding by integrating the sine cosine optimization into the neural network protocol. In light of the significance of maintaining the visual integrity of the video and recommending a more subtle and comprehensive approach to video watermarking,
In [60] author introduces an embedding scheme which utilizes reversible watermarking to solve the problem of information loss. The bit values are embedded on the pretext of odd-even embedding. The calculation of modulation index is done and stored in watermarked object.PR sequence is added into modulation information, so as to make the scheme more secure. The said algorithm finds its application in measurement data and 3D objects having coordinates, as they are suitable for objects represented by floating type or fixed point numbers.

Disadvantage of the scheme is not evaluated for video processing the scheme, however is evaluated only for geometric and guassian noise attacks.

In [25] the author uses lifting wavelet transform (LWT) and support vector machine (SVM) for watermarking implementation. 3 level LWT is implemented on the image, which gives 64 sub bands. Each of the sub band is evaluated for visibility and robustness of the watermark, so as to select 9 sub bands for embedding purpose. These sub bands are randomized by secret key1. The sub bands are again divided into 2*2 overlapping blocks, which are again randomized using secret key2. The average difference is calculated between the largest coefficients. The watermark is converted into 1 dimensional binary watermark. The largest coefficient of the block is modified in accordance of watermark to be embedded. The key 2 and key 3 are used to obtain back the sub band coefficients.

ILWT is implemented on the obtain sub bands to get the watermarked image. The extraction of watermark is done using SVM classifier. The scheme has been tested using 300 images and 50 watermark images. The scheme outperforms many other proposed schemes in existing literature in terms of imperceptibility. The comparison of ANN, SVM and kNN has been performed which shows that SVM model with RBF gives better results. The use of SVM instead of SVD makes the system blind. ANOVA and IFS used reduces the computational complexity as it needs not to be performed each time as compared to PCA.

However the system becomes complex and time consuming, so it’s difficult to apply them in real time processing videos.

In [65] the robustness of APDCBT in the watermark embedding system is compared to DCT. By raising the level of LSB resetting, APDCBT outperformed DCT in terms of average normalized cross-correlation. Even after removing half of the watermarked image's components, the watermark was still evident. The suggested approach and the DCT method were compared in terms of average normalized cross-correlation of all images under JPEG compression, Gaussian noise, histogram equalization, and contrast adjustment attacks. However noise attacks like salt and pepper and geometric noise attacks are not evaluated.

The paper[71] explores Intellectual Property Rights (IPR) protection challenges posed by Generative Adversarial Networks (GANs) in generating images and models. Evaluating existing copyright protection measures, the study employs adversarial attacks, watermarking, and attribution analysis across various GAN architectures. Findings reveal satisfactory IPR protection for GANs' input images, model watermarking, and attribution networks. Notably, attention is drawn to the insufficient protection of training sets, necessitating future research. Experimental results show the effectiveness of adversarial attacks on preventing copyright violations and improved watermarking for generation models. Spectral analysis aids in attributing fake images to their source models. Despite advancements, challenges persist in protecting training sets, urging further attention.

The study contributes to understanding GANs' IPR protection effectiveness, urging the development of comprehensive evaluation metrics and ethical generative AI adoption. Ongoing research aims to integrate diverse IPR protection domains for a unified assessment approach.

The paper [72] combines DNA sequences, cellular automata (CA), and chaotic systems to provide a strong digital video watermarking technique for copyright protection. Singular value decomposition (SVD) and contourlet transform (CT) are used in the technique, along with their insertion into low-frequency subbands. Different CA rules can be implemented in parallel using DNA-based one-dimensional chaotic automata. The method has great resilience against a variety of threats and is blind, with its evaluation based on statistical metrics such as PSNR, NCC, and BER. It presents fundamental ideas in Molecular Biology, Cellular Automata, Transform Domain (CT, SVD), Chaos Theory, and more. Practical for copyright protection systems, the suggested approach includes novelties such as a new chaotic map, CT and SVD combination with chaos-based security, and error correction based on watermark repetition.
The outcomes indicate that it is successful. The results suggest its effectiveness compared to other methods in the research literature.

For multimedia information security, Sharma et al. (2021) proposed the Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD) approach [68]. This paper describes a strong color imagery WM in the transform area that is AI-based. In addition to extra optimization factors, video data will be employed as the scheme's input. Using a chaotic map, the watermark is scrambled. The embedding process uses diagonal matrices. To add an additional layer of protection, a secret key is also used during embedding. Using the ABC optimization technique, the scaling coefficient is optimized. Aerial and general medical photos are used to calculate PSNR, SSIM, and NC. Additionally, a range of noise attacks, such as geometric, filtering, and salt-and-pepper noise attacks, are carried out to assess performance in terms of robustness and perceptual quality.

The paper [74] introduces an image watermarking technique utilizing the least significant bit (LSB) and Canny edge detection. The method employs Canny edge detection to identify suitable locations for watermark embedding by dividing the image into blocks, calculating gradients, and applying convolution masks. The LSB is then utilized for embedding the watermark in areas identified by the edge detection process. The proposed approach incorporates an additional layer of security by scrambling the watermark signal using a chaotic substitution box. The study emphasizes robustness and imperceptibility, benefiting from the computational efficiency of LSB. Rigorous testing against various attacks demonstrates the method's resilience. The research contributes a straightforward yet effective image watermarking method, addressing copyright protection and content authentication challenges in the digital domain. Comparative evaluations indicate superior results in terms of SSIM and PSNR compared to existing approaches, emphasizing the method's effectiveness.

The disadvantage lies in the simplicity of the least significant bit (LSB) embedding, which, while computationally efficient, compromises security and capacity, making the process susceptible to advanced attacks and limiting its applicability in scenarios requiring high payload or increased resistance to sophisticated threats.

With the purpose of addressing copyright protection and content authentication difficulties in digital media, the suggested image watermarking system [75] integrates discrete wavelet transform (DWT) with singular value decomposition (SVD). To create a grayscale watermark image, the same procedures are applied to a grayscale cover image first, followed by eigendecomposition on the high-high components. The diagonal component is securely sent once the watermark's singular values are scaled and integrated with the DWT coefficients of the original image. The watermarked image and the diagonal component are used to extract the watermark at the receiving end. Excellent imperceptibility, security, and resilience against a range of threats are demonstrated by the simulation findings. While acknowledging several limitations, such as its moderate resilience to salt and pepper attacks, the research also makes recommendations for future research approaches, including the incorporation of binary watermarks and the concealment of multiple watermarks for greater flexibility.

The presented dual watermarking scheme in [73] introduces an innovative approach with applications in identity protection, media integrity maintenance, and copyright protection across electronic and printed media. Leveraging the owner's signature and fingerprint as watermarks, the scheme ensures ownership verification and media validity. Initially implemented on continuous-tone/greyscale images and later extended to multitone images, achieved through advanced halftoning-based printing, the proposed embedding exhibits robustness and imperceptibility. Experimental evaluations demonstrate outstanding results from both objective and subjective perspectives. In the context of increasing cybersecurity threats, particularly identity-related attacks, the dual watermarking scheme provides a comprehensive solution, excelling in imperceptibility, robustness, and security. The method's adaptability across diverse media types reaffirms its effectiveness in mitigating identity theft risks.

The paper [70] introduces a novel approach called All-Stage Discrete Cosine Biorthogonal Transformation (APDCBT) for digital image processing, specifically for watermark insertion. APDCBT is employed to address issues in Discrete Cosine Transformation (DCT), particularly in low bit-rate scenarios. The method selects image regions based on homogeneity criteria and embeds watermarks in Medium Frequency (MF) bands of APDCBT in pixel blocks. Experimental results
demonstrate APDCBT's superiority over traditional DCT in watermarking, particularly against LSB reset attacks. The proposed method proves effective in copyright protection by concealing watermarks in homogenous image areas. The paper outlines the embedding and extraction processes, using selected blocks and APDCBT transformations. Experimental results, including MSE and PSNR analysis, validate the method's performance on various images. Additionally, robustness against LSB reset attacks and comparison with DCT under different attacks highlight the effectiveness of APDCBT in resisting watermark removal attempts.

3. Simulation Results:
Various common watermarking schemes have been compared in this section to get an insight of which scheme performs better in terms of robustness and fidelity. Videos are converted into frequency domain using various mathematical tools such as DWT, LWT, RDWT and APDCBT. Then SVD is applied so as to embed the watermark in the obtained singular values. Various variants of noise attacks have been evaluated to get a better insight of the various basic schemes in practice. With the help of these results, researchers can choose the scheme according to their requirement for various watermarking practices. The steps for simulation are as follows:

3.1 In the proposed video watermarking embedding process:

1. Initially, frames are extracted from the cover video.
2. These frames undergo a conversion into grayscale images.
3. Each frame and watermark then undergo a specific mathematical transformation (such as Discrete Wavelet Transform (DWT), Lifting Wavelet Transform (LWT), Redundant Discrete Wavelet Transform (RDWT), or All Phase Discrete Cosine Biorthogonal Transform (APDCBT)) to obtain their respective frequency band coefficients.
4. The high-frequency band of each transformed frame and watermark is extracted, and Singular Value Decomposition (SVD) is applied to extract the singular values.
5. Subsequently, the watermark is embedded into the singular values of the cover frames using a scaling coefficient (set at 0.05).
6. The inverse of the chosen frequency domain tool (Inverse DWT (IDWT), Inverse LWT (ILWT), Inverse RDWT (IRDWT), or Inverse APDCBT (IAPDCBT)) is applied using the new high-frequency band coefficients.
7. The frames are then utilized to reconstruct the cover video, which is sent to the receiving end of the watermarking process.

3.2 In the extraction phase:

1. Frames are extracted from the received video.
2. These frames are then converted into grayscale images.
3. The images undergo transformation into the frequency domain using a specific technique (such as Discrete Wavelet Transform (DWT), Lifting Wavelet Transform (LWT), Redundant Discrete Wavelet Transform (RDWT), or all phase discrete cosine biorthogonal transform (APDCBT)) to acquire high-frequency band coefficients.
4. Singular Value Decomposition (SVD) is applied to obtain the singular values, facilitating the extraction of the watermark, which is subsequently assessed for Peak Signal-to-Noise Ratio (PSNR) and Cross-Correlation (CC).

Table 1 offers a comprehensive summary of correlation coefficients linked to various fundamental schemes in the literature. Simultaneously, Figure 1 visually illustrates the interpretation of these coefficients through a graphical representation. Parallely, Table 2 presents PSNR values for each scheme, incorporating different variants of noise attacks in simulations. Figure 2 further enhances comprehension by graphically interpreting the data from Table 2, striving to provide a comprehensive understanding of the diverse facets associated with watermarking schemes. This collective presentation facilitates an in-depth analysis, enabling a nuanced exploration of the intricacies embedded in the information provided.
Table 1. Comparison of correlation coefficient for robustness

<table>
<thead>
<tr>
<th>NOISE ATTACK</th>
<th>Only SVD</th>
<th>DWT SVD</th>
<th>LWT SVD</th>
<th>RDWT SVD</th>
<th>APDCBT SVD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  NO NOISE</td>
<td>.9247</td>
<td>.9992</td>
<td>.9992</td>
<td>.9992</td>
<td>.9454</td>
</tr>
<tr>
<td>2  GUASSIAN(.005)</td>
<td>.5510</td>
<td>.9981</td>
<td>.9988</td>
<td>.9957</td>
<td>.9454</td>
</tr>
<tr>
<td>3  GUASSIAN(.01)</td>
<td>.5485</td>
<td>.9981</td>
<td>.9988</td>
<td>.9956</td>
<td>.9454</td>
</tr>
<tr>
<td>4  GUASSIAN(.02)</td>
<td>.5633</td>
<td>.9981</td>
<td>.9987</td>
<td>.9955</td>
<td>.9454</td>
</tr>
<tr>
<td>5  SPECKLE NOISE(.005)</td>
<td>.4856</td>
<td>.9982</td>
<td>.9982</td>
<td>.9970</td>
<td>.9454</td>
</tr>
<tr>
<td>6  SPECKLE NOISE(.01)</td>
<td>.5014</td>
<td>.9981</td>
<td>.9988</td>
<td>.9961</td>
<td>.9454</td>
</tr>
<tr>
<td>7  SPECKLE NOISE(.02)</td>
<td>.5293</td>
<td>.9981</td>
<td>.9988</td>
<td>.9958</td>
<td>.9454</td>
</tr>
<tr>
<td>8  SALTAND PEPPER(.005)</td>
<td>.4869</td>
<td>.9982</td>
<td>.9988</td>
<td>.9961</td>
<td>.9454</td>
</tr>
<tr>
<td>9  SALTAND PEPPER(.01)</td>
<td>.5061</td>
<td>.9981</td>
<td>.9988</td>
<td>.9958</td>
<td>.9454</td>
</tr>
<tr>
<td>10 SALTAND PEPPER(.02)</td>
<td>.5337</td>
<td>.9982</td>
<td>.9988</td>
<td>.9956</td>
<td>.9454</td>
</tr>
<tr>
<td>11 POISSON NOISE</td>
<td>.4876</td>
<td>.9992</td>
<td>.9992</td>
<td>.9965</td>
<td>.9454</td>
</tr>
<tr>
<td>12 ROTATION(15°)</td>
<td>.9361</td>
<td>.9985</td>
<td>.9988</td>
<td>.9983</td>
<td>.9454</td>
</tr>
<tr>
<td>13 ROTATION(30°)</td>
<td>.9261</td>
<td>.9985</td>
<td>.9988</td>
<td>.9981</td>
<td>.9454</td>
</tr>
<tr>
<td>14 ROTATION(45°)</td>
<td>.9387</td>
<td>.9986</td>
<td>.9988</td>
<td>.9982</td>
<td>.9454</td>
</tr>
<tr>
<td>15 CROPPING(1/2)</td>
<td>.7547</td>
<td>.9990</td>
<td>.9990</td>
<td>.9992</td>
<td>.9454</td>
</tr>
<tr>
<td>16 CROPPING(2/3)</td>
<td>.3869</td>
<td>.9992</td>
<td>.9989</td>
<td>.9992</td>
<td>.9454</td>
</tr>
<tr>
<td>17 MEDIAN FILTER(3*3)</td>
<td>-</td>
<td>.9992</td>
<td>.9982</td>
<td>.9991</td>
<td>.9454</td>
</tr>
<tr>
<td>18 MEDIAN FILTER(5*5)</td>
<td>-</td>
<td>.9992</td>
<td>.9989</td>
<td>.9991</td>
<td>.9454</td>
</tr>
</tbody>
</table>

Fig 1. Comparison graph of correlation coefficient for robustness
The correlation coefficient provides information on the system's robustness. Regarding CC in hybrid models, the LWT/SVD, DWT/SVD, and RDWT/SVD schemes yield remarkable outcomes, with values exceeding .99. After incorporation of different noise attacks, LWT SVD performs better with the exception of median filtering. DWT/SVD and RDWT/SVD appear to be performing better in that segment.

Perceptual quality in terms of PSNR, is a crucial factor when it comes to HD TV and the pixel gradients in medical videos. With PSNRs of 76.0416 (db) and 75.8419 (db), SVD and APDCBT/SVD perform exceptionally well. While APDCBT/SVD does perform better than all other methods after noise attacks are incorporated.
### 4. SUMMARY OF VARIOUS WORK DONE IN LITERATURE:

<table>
<thead>
<tr>
<th>Tools used</th>
<th>Noises evaluated</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
</table>
| [16] LSB                | Motion blurr, JPEG compression, low pass filtering, cropping, Guassian noise, salt pepper noise | ● Easy implementation  
                              ● Less time consuming  | ● Prone to pixel to pixel attacks  |
| [19] DFT, HVS           | Cropping, scaling, rotation, shearing, sharpening, filtering | ● Rotational, shift  
                              ● Translational invariance so prone to geometric attacks  | ● The information that varies in accordance to time is lost.  
                              ● Scheme experienced symmetry constrains  |
| [57] SVD                | White noise, Guassian, JPEG compression, cropping scaling, smoothing, rotation  | ● Increase in stability  | ● False positive error is not addressed.  
                              ● SVD has more memory requirements  |
| [50] RDWT, SVD, Arnold Scrambling, HVS block entropy | Guassian noise, low pass filter, sharpening, median filter, salt pepper noise, speckle noise, histogram equalization, JPEG compression, Guassian noise, cropping, rescaling, Guassian noise, poisson noise | ● A.S provides extra security  
                              ● HVS, SVD helps to increase the perceptual quality of the image  
                              ● RDWT is robust against certain noise attacks  | ● System becomes very complex and time consuming as many tools are incorporated in the scheme.  
                              ● A.S has low period, which make easy for an attacker to decrypt  |
| [59] PRsequence         | Guassain, cropping, rotation translation  | ● Capacity is increased.  
                              ● Applicability for 3 d objects was introduced.  | ● The scheme was not evaluated for videos  
                              ● Very less variants of noise were evaluated  |
| [54] IWT, SVD, ABC      | Salt and pepper, rotation, cropping, scaling, gamma correction, median filter, avg filter, histogram equalization, wiener filter JPEG compression, contrast adjustment sharpening | ● False alarm problem is addressed  
                              ● IWT helps to remove round off errors reduces computational cost.  
                              ● IWT reduces computational cost.  
                              ● ABC used for optimization makes the system more robust  | ● SVD applied on whole image has huge memory requirements.  |
<table>
<thead>
<tr>
<th></th>
<th>Video watermarking was considered</th>
<th>SVM makes the system blind</th>
<th>_data hiding capacity has been increased by use of dual watermark</th>
<th>Image has smoothening and aliasing effects due to DWT</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1]</td>
<td>Increased of PSNR and CC as compared to existing schemes</td>
<td>SVM provides good smoothing</td>
<td>shift sensitivity, poor directionality, lack of phase information</td>
<td>Not many noises have been considered</td>
</tr>
<tr>
<td>[25]</td>
<td>SVM provides good energy compaction.</td>
<td>ANOVA and IFS used reduces the computational complexity.</td>
<td>SVD - based schemes have big memory requirements.</td>
<td>SVD - based schemes have big memory requirements.</td>
</tr>
<tr>
<td>[2]</td>
<td>SVM provides good energy compaction.</td>
<td>ANOVA and IFS used reduces the computational complexity.</td>
<td>SVD provides good stability</td>
<td>Image has</td>
</tr>
<tr>
<td>[5]</td>
<td>LWT,SVD</td>
<td>JPEG compression</td>
<td>• Robustness is increased by smoothening and aliasing effects due to DWT.</td>
<td>• LWT has advantages in terms of time consumption and memory requirements.</td>
</tr>
<tr>
<td>[9]</td>
<td>DWT,SVD</td>
<td>Rotation, median filter, guassian noise, histogram equalization, salt and pepper noise</td>
<td>• The system is robust against geometric noise attacks.</td>
<td>• SVD provides good results of PSNR.</td>
</tr>
<tr>
<td>[13]</td>
<td>DCT,RBF</td>
<td>guassian noise, histogram equalization, JPEG compression, low pass filtering, median filtering, scaling, cropping</td>
<td>• RBF have simple structures of network.</td>
<td>• They can do better approximation.</td>
</tr>
<tr>
<td>[49]</td>
<td>DWT,HD,FOA,SVD</td>
<td>Wiener filter, Median filter, Gaussian low-pass filter, Average filter, Gaussian noise, Salt &amp; peppers noise, Speckle noise, Cropping attack, JPEG compression, Re-scaling, HE attack, Motion blur, Sharpening, Rotation</td>
<td>• FOA is simple and optimization ability is good.</td>
<td>• SVD provides good stability to the image while embedding.</td>
</tr>
<tr>
<td>[48]</td>
<td>RDWT, IGWO,PCA</td>
<td>Rotation, scaling, re-sizing, flipping, compression, histogram equalization, median filtering, motion blur, sharpening.</td>
<td>• RDWT makes the scheme becomes less prone to noise attacks.</td>
<td>• PCA involves information loss of some important image features.</td>
</tr>
<tr>
<td>Method</td>
<td>Noise Attacks</td>
<td>Watermarking Features</td>
<td>Robustness</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>IGWO detector</td>
<td>Increases time consumption efficiency and robustness of the scheme.</td>
<td>Increase efficiency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCA</td>
<td>Tends to reduce processing time</td>
<td>Increase efficiency</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[20] 3 level DWT</td>
<td>Gaussian noise, Salt &amp; pepper noise adding, frame dropping and frame adding noise attacks.</td>
<td>Blue channel is used for embedding purpose, which is least sensitive to human visual system, so as to increase the robustness</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Original video is not required at the time extraction of watermark</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[60] DWT-DCT</td>
<td>Salt and Pepper Noise, Compression, Histogram Equalization, Averaging filter, Median Filter Attack, Gaussian Noise, Gaussian filter, Cropping</td>
<td>Mapping-based watermarking provides a better visual acceptable quality</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lacks robustness for numerous noise attacks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[61] SCBSA</td>
<td>Gaussian noise, Impulse noise, Salt and Pepper noise</td>
<td>It maximizes correlation coefficients</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not perform well in noise attacks like crop, rotating attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[62] CNN-SOM</td>
<td>Salt &amp; pepper noise, PN, Speckle noise, Average filter, Medium filter, Gaussian filter, Histogram Equalization, JPEG compression</td>
<td>Boosts the robustness against inter-frame assaults</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>For video watermarking desynchronization on assaults, it does not perform well.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[63] Counting-based method</td>
<td>-</td>
<td>Establishes the rightful owner of copyright evidence.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time consumption to embed and extract is high</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[64] IWT, CT, DWT-SVD</td>
<td>Salt &amp; Pepper, Gaussian Noise Attack, Jpeg Compression, Median Filter, Average Filter, Wiener Filter, Low pass Filter, Histogram Equalization, Sharpening, Gamma Correction, blurring</td>
<td>A superior visual quality based on certain criteria</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Detecting the rotational attack</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Doesn’t take FPP risk into account</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. CONCLUSION

When it comes to research, video watermarking has received less attention than image watermarking. Numerous issues are linked to it, leading to a great deal of unresolved issues in this specific field. Since time is a crucial component of live video processing, there is a lot of room for improvement in this area by simultaneously raising PSNR and CC and reducing the amount of time needed for extraction and embedding.

This study compares many spatio-frequency domain invisible watermarking techniques, giving a deep understanding of their respective advantages while incorporating a range of noise attacks. Researchers can use these findings to determine which technique is best to apply in a certain study domain, and then use that information to create their own robust hybrid schemes in conjugation of various techniques. A variety of noise attacks, including guassian, salt-and-pepper, and speckle noise with varying noise densities, have been taken into consideration by the simulation for video watermarking. To enhance comprehension of video watermarking under diverse noise attack variations, geometrical and filtering noise attacks have also been examined. We conclude from this research that there are a lot of unsolved issues in the field of video watermarking, and that this simulative comparison may help us understand workable solutions in this area.

REFERENCES:


[60] Hazim, Hussein Tuama, Nawar Alseeawi, and Haider TH ALRikabi. "A Novel Method of


