J. Electrical Systems 20-10s (2024):1284-1294

Swati Patel*

Khushali Raval[2]

Pragneshkumar Gautambhai Patel[3]

ZishanHaider YasinAli Noorani[4]

Aniruddhsinh Dodiya[5]

Pradeep Gamit[6]

Perspective on a Hybrid Digital Watermarking Scheme for Securing Multimedia

Journal of Electrical Systems

Abstract: - Technology dominates today's world, providing widespread, affordable internet access, leading to the rampant illegal sharing of digital media. Pirated versions of digital content are easily distributed globally through social media and mobile apps, violating copyrights and harming content owners' financial and intellectual property rights. The unauthorized copying, manipulation, and redistribution of digital media exacerbate piracy issues, necessitating robust authentication and copyright protection measures. Digital watermarking offers an effective solution to combat piracy by embedding additional information into digital content, ensuring authenticity and copyright ownership. Watermarking can be performed in the spatial or transfer domain. This paper outlines the lifecycle of a watermarking system, provides an overview of video watermarking techniques and their applications, and classifies these techniques based on human perception, detection methods, resistance to attacks, media type, and embedding techniques. It also discusses each approach's methods, uses, challenges, and key characteristics, presenting analytical findings from the past 15 years of literature. Finally, it discusses this study's remaining questions and suggests potential future research directions.

Keywords: IMAGE PROCESSING, DIGITAL VIDEO WATERMARKING, DWT, DCT, SVD

1. Introduction

In today's world, almost everyone has access to affordable high-speed internet through their smartphones, enabling seamless transmission of text, data, images, and videos. However, this convenience exposes users to the risk of personal information misuse[1]. Digital content can be easily copied and altered, leading to piracy and negatively impacting content owners' financial and intellectual property rights[2]. Watermarking helps mitigate these issues by embedding the owner's identity or logo into their work, securing it from unauthorized use. This method involves hiding information within digital data[3]. Digital watermarking marks data without damaging it, emphasizes copyright presence to deter misuse and simplifies proving ownership in cases of unauthorized use. The security field, including watermarking, cryptography, and steganography, has gained significant attention for copyright protection and content authentication. Digital watermarking has become a popular strategy to prevent unauthorized duplication of digital files. Sensitive data is embedded into media and extracted using appropriate algorithms[4]. The key aspects of video watermarking are payload capacity,

* Assistant Professor, Information Technology Department, L.D.College of Engineering, Ahmedabad

swatijpatel@ldce.ac.in

[2]Assistant Professor, Information Technology Department, Vishwakarma Government Engineering College,Chandkheda,Ahmedabad

khushali_raval@vgecg.ac.in

[3]Assistant Professor, Computer Engineering Department, L.D.College of Engineering, Ahmedabad

pragneshpatel@ldce.ac.in

[4]Assistant Professor, Computer Engineering Department, L.D.College of Engineering, Ahmedabad

zishannoorani@ldce.ac.in

[5]Assistant Professor, Computer Engineering Department, Government Engineering College Modasa

aniruddhsinh.dodiya@gecmodasa.ac.in

[6]Assistant Professor, Computer Engineering Department, Government Engineering College Modasa

pradeep.gamit@gecmodasa.ac.in

resilience, and imperceptibility, as shown in Figure 1.

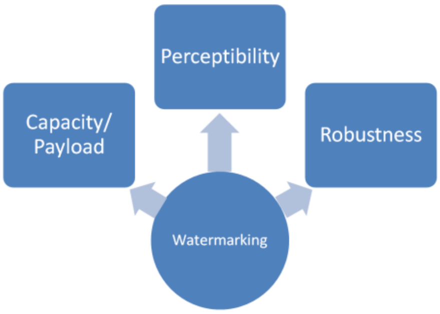


Fig 1: Requirements of Digital Watermarking Techniques

Imperceptibility refers to the similarity between the original and watermarked digital media, ensuring the watermark is not visually noticeable. While slight degradation may be acceptable in some cases, the quality of digital media should remain high. Payload or capacity is the amount of information embedded in the watermarked media. Despite the public watermarking method, removing the watermark should be impossible, and it must resist various attacks. These three characteristics—imperceptibility, payload, and resistance—are interconnected, with improvements in one potentially affecting the others.

Researchers have proposed numerous watermarking approaches for multimedia data security over the past few decades. Spatial domain solutions, used for authenticating digital videos and photos for copyright purposes, are less resistant to attacks. To address this, transform domain strategies using techniques like Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD) have been developed. These methods are generally reliable for protecting multimedia data from copyright violations[5]. Video watermarking presents more significant challenges than image watermarking due to the scattered data across frames and the uneven distribution of moving and stationary areas. Processing an entire video sequence, especially at a frame rate of at least 24 frames per second for high-definition video, is impractical. Therefore, extracting keyframes—representative frames that can be used to recognize the whole video sequence—is advisable[6]. Keyframes offer a quicker view of video content and reduce the computational complexity of video analysis and retrieval applications, ensuring the video can be reproduced using these frames[7].

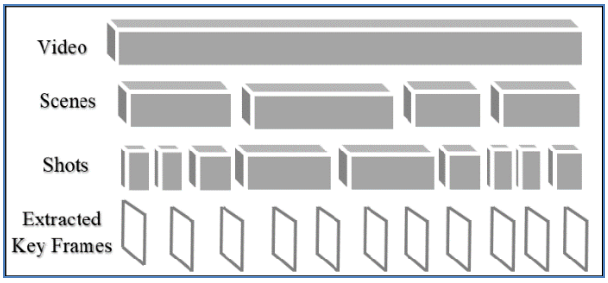


Fig 2: Structural-hierarchy-of-a-video [8]

Video consists of a vast amount of data, much redundant or insignificant. As shown in Figure 2, video has a complex structure comprising scenes, shots, and frames[9]. A scene groups shots into a semantic unit; a shot is a sequence of frames from a single camera action, and a shot boundary marks the transition between shots[10]. Keyframes represent a visual summary and essential information about the video sequence[11], containing high-priority entities and events without repetition and redundancy[12]. Video processing, crucial in applications like watermarking, involves scene segmentation, shot boundary detection, and keyframe extraction. Keyframes effectively summarize the entire video clip, containing the most salient features[7]. Three properties are considered when selecting keyframes: continuity, priority, and repetition. Continuity ensures the video is as uninterrupted as possible. Priority involves including high-priority items based on the application's needs. Repetition avoids representing the same events repeatedly. Incorporating these properties can be challenging[13].

2. Digital Watermarking System

A watermarking system's life cycle is divided into three sections, as shown in Figure 3:

1. Embedding/Insertion of a Watermark

2. Attacking

3. Extraction and Detection of Watermarks

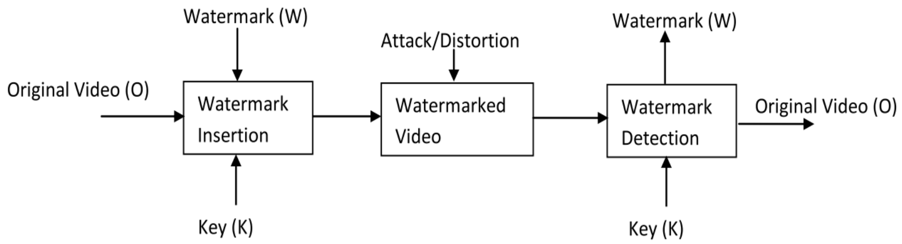


Figure 3: A video watermarking system's block diagram[14]

An algorithm accepts the host and the data to be embedded and produces a watermarked signal in embedding. The watermarked digital signal is then saved or transferred across the channel to another person; any change is referred to as an attack. Third parties may try to modify the digital watermark to erase it. The watermark is extracted from the assaulted signal during extraction. The watermark remains and can be recovered, provided the signal was not altered during transmission. Watermark can be embedded and extracted in a variety of methods, as seen in Figure 4:

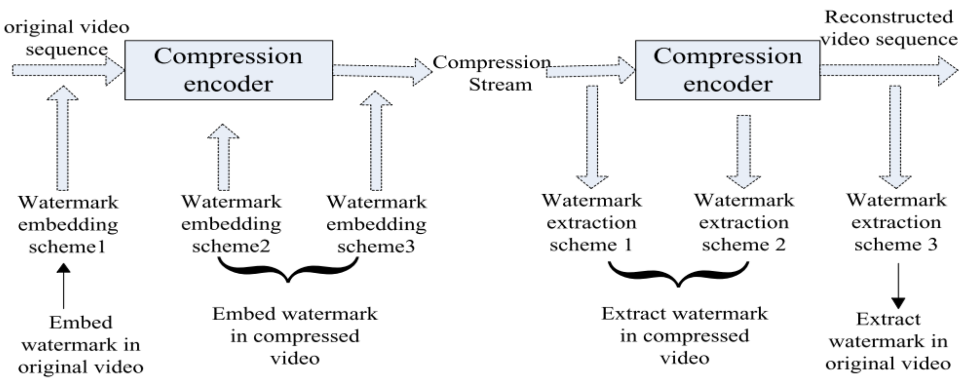


Figure 4: Three ways of watermark embedding [15]

The first category of watermarking methods (Scheme 1) processes the original video data without encoding it. This method is simple but allows the watermark to be removed during compression and increases the bit rate of the video stream[14]. In the second category (Scheme 2), watermarking is paired with video compression standards like MPEG-2, MPEG-4, AVC, and HEVC. This method does not increase the bit rate and uses a built-in video watermarking algorithm. The third category (Scheme 3) involves embedding a watermark in a compressed video, adding complexity to the process.

3. Applications of Digital Watermarking

Researchers in the early 1990s suggested digital watermarking for picture tagging, counterfeit protection, copyright enforcement, and controlled access to image data. By the early 2000s, video watermarking expanded to include copyright protection, authentication, tamper-proofing, broadcast monitoring, fingerprinting, media forensics, medical applications, copy control, picture authentication, and ownership communication[16][3]. The following subsections discuss the most widely used applications.

3.1 Copyright Protection: Watermarks can include copyright information in the host video as proof of ownership during decoding.

3.2 Authentication: A watermark verifies content validity, detecting tampering by changes in pixel values of embedded data[16].

3.3 Tamper-proofing: Watermarks in host videos detect content changes crucial in medical imaging and military surveillance. Fragile watermarks identify minor tampering and highlight altered areas[17].

3.4 Broadcast Monitoring: This system ensures video content, like commercials, is broadcast as contracted. Digital watermarking provides reliable active monitoring, while passive monitoring requires extensive storage.

3.5 Fingerprinting: Unique watermarks in each customer copy help track illicit copies, enabling content owners to identify the source of copyright infringements.

3.6 Media Forensics: Forensic watermarks enhance the ability to detect unauthorized use and enforce contractual usage agreements.

3.7 Content Filtering: Watermarks restrict access to inappropriate content, triggering actions during decoding to block prohibited material.

3.8 Medical Application: Embedding patient names on X-rays, reports, and MRIs ensures confidentiality and prevents report misinterpretation.

3.9 Copy or Playback Control: Watermarks prevent unauthorized copying or playback, with devices designed to detect and block watermarked content during these actions[18].

3.10 Data Hiding: Digital watermarking conceals data, making it undetectable to unauthorized individuals.

4. Watermarking Techniques

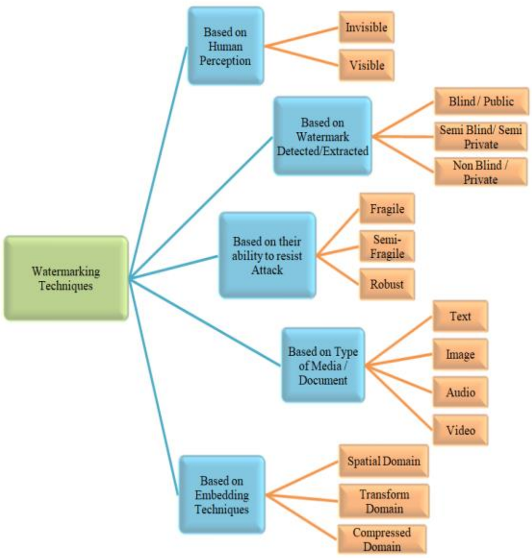


Figure 5: Classification of Watermarking Techniques

4.1 Based on Human Perception:

4.1.1 Invisible

4.1.2 Visible

Watermarking procedures are of two types: visible and invisible. A visible watermark is apparent on digital data, while an invisible watermark is embedded within the data but not visible. The properties of watermarking are tailored to the specific application of the system[19].

Figure 6: (a) Image with visible watermark, (b) Image with invisible watermark [3]

A visible watermark allows the visitor to see the author's logo or identification, but spreading it across the image degrades quality, making it unsuitable for medical purposes. Invisible watermarks are not noticeable to the spectator and do not significantly alter the appearance of the original object. They offer copyright protection and content authentication, being more resistant to signal processing threats and suitable for nearly any application.

4.2 Based on the Watermark Detected / Extracted.

4.2.1 Blind / Public

4.2.2 Semi Blind / Semi-Private

4.2.3 Non-Blind/Private

In a blind technique, the information contained in a watermarked image can be discovered without using the cover picture or the original watermark. This method only requires the watermarked image for extraction, making the original image unnecessary[20]. It is highly resistant to various types of attacks. In a semi-blind technique, specific featured information is needed to extract embedded data from a watermarked image. In a non-blind approach, the original picture is required to detect encoded data within the watermarked image[21].

Extraction (Blind) [K, WC] = W'

Extraction (Semi−Blind)[K,W,WC] = W'

Extraction (Non−Blind) [K, C, W, WC] = W'

Where, K = Key used for embedding, C=Original Cover Image, W=Watermark Image, WC=Watermarked Image, W'=Extracted Watermark

4.3 Based on Their Ability To Resist Attack

4.3.1 Fragile

4.3.2 Semi-Fragile

4.3.3 Robust

With a minor change to the watermarked data, fragile watermarks can be easily destroyed. Watermarks in Semi-Fragile can be broken if a change to the watermarked data reaches a certain threshold. This can be used to ensure data integrity and security. A strong watermark is difficult to remove. Copyright protection can be ensured using this method[22].

4.4 Based on the Type Of Document/Media

4.4.1 Text

4.4.2 Image

4.4.3 Audio

4.4.4 Video

Text watermarking embeds data into documents like DOC and PDF to identify copyright ownership[16]. Image watermarking inserts data or messages into images, utilizing either spatial or transform domain techniques.

Spatial domain operates directly on pixels, while transform domain modifies transformation coefficients[23]. Audio watermarking embeds watermarks in the time or frequency domain without altering the audibility of the original audio file. It addresses copyright issues prevalent in audio applications by proving ownership of audio data[16]. Video watermarking introduces additional data, or watermarks, into the host video stream. This method prevents unauthorized distribution of stolen digital videos over the internet and other communication channels[23].

4.5 Based on Embedding Techniques

The watermark can be immediately embedded in an image or translated into a different domain before embedding in the host data. According to the domain in which a watermark can be implanted, watermarking techniques can be classed as spatial or transform domain watermarking [3]. Apart from that, a watermark might be included in the compressed and encrypted domain.

4.5.1 Spatial domain watermarking

In Spatial Domain watermarking, watermark bits are directly added to the pixel values of the cover picture by altering the grey-level values to match those of the watermark image. This approach is widely used in video watermarking due to its simplicity, speed, and low implementation costs. However, it has drawbacks such as limited information-hiding capacity, vulnerability to cropping, and challenges in achieving robustness [24].To enhance robustness in the spatial domain, the watermark can be embedded multiple times in the host video. While this improves survivability against attacks, it also reduces quality (imperceptibility) due to redundant watermark data[24].

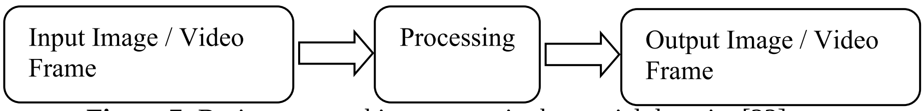


Figure 7: Basic watermarking process in the spatial domain. [23]

Table 1: Characteristics and drawbacks of spatial domain technique:[25] [26] [27]

	Characteristics		Drawbacks
1	It's quite easy to learn and put into practice.	1	Less embedding capacity
2	Only resistant to a few typical attacks such as median filtering, cropping, rotation, and so on.	2	The intermediate party can easily alter the watermark
3	Computational complexity is very less as Watermark is added in the pixel domain.	3	Almost in all spatial domain techniques, the original image is altered during the embedding phase.
4	During watermarking, no transformation is applied to host data.	4	Image processing operations like lossy image compression can destroy the watermark.
5	Watermark can be extracted by correlating the expected pattern with the received signal.	5	Do not allow subsequent processing to increase the robustness

4.5.2 Transform domain watermarking

In Frequency Domain watermarking, the host video frame undergoes transformation into the frequency domain before watermark embedding, followed by inverse transformation. Techniques such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD) are utilized for these transformations, each offering distinct features for video frame representation. This method is known for its resistance to attacks, stability, and higher imperceptibility compared to the spatial domain. However, it imposes a higher processing burden[24]. Despite their advantages in processing speed, these techniques often struggle to automatically balance resilience and imperceptibility in watermarking applications[28].

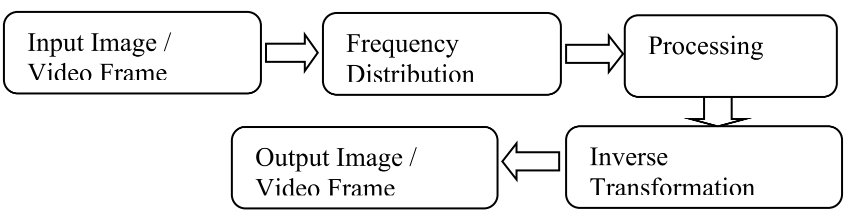
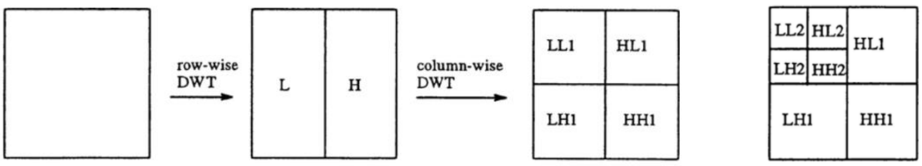


Figure 8: Basic watermarking process in the Frequency domain. [23]

I. Discrete wavelet transform (DWT):

In Discrete Wavelet Transform (DWT), video frame pixels are transformed into wavelets for compression and coding. The frame is divided into four bands: lower resolution approximation (LL), vertical (LH), horizontal (HL), and diagonal (HH), representing low and high-frequency components[29]. Embedding the watermark in the LL subband retains image quality since human vision is less sensitive to changes in this low-frequency region[30]. However, embedding in higher-frequency subbands increases watermark robustness at the cost of visual integrity, as measured by PSNR. The DWT method enhances watermarking's visibility in high-frequency areas, making it challenging to embed in the DWT-converted high-frequency band with large amplitude coefficients.



(a) (b)

Figure 9: (a) First level of decomposition (b) Second level of decomposition

II. Discrete cosine transform (DCT):

DCT (Discrete Cosine Transform) is widely used for its efficient energy compression capabilities and is integral to major compression formats[3]. It decomposes images into frequency coefficients—low, high, and mid-band—allowing for various applications in watermarking[5]. Two types of DCT-based watermarking exist: global, which applies DCT to the entire frame, and block-based, which processes non-overlapping blocks individually[3][31]. The mid-frequency band is commonly chosen for embedding watermarks due to its perceptual characteristics, while alterations in the low-frequency band and DC component significantly affect human perception of image quality and are susceptible to attacks[32]. DCT's effectiveness in watermarking stems from its concentration of signal energy in low frequencies and the vulnerability of high-frequency components to compression and noise[30]. DCT operations can be performed in 1D, 2D, or 3D dimensions; 2D DCT is typically used for image and frame transformations into cosine series[31].

1D-DCT is given as:

$$f(i) = F(u) \quad ...(1)$$

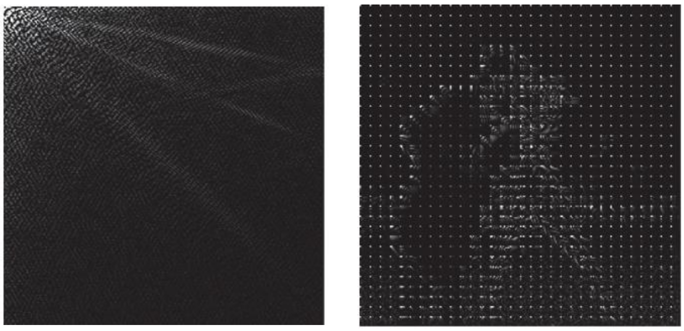
2D-DCT is given as:

$$F(u,v) = \alpha(u)\alpha(v) \sum_{i=0}^{M-1} \sum_{j=0}^{M-1} f(i,j) cos\left[\frac{(2i+1)u\pi}{2M}\right] cos\left[\frac{(2i+1)v\pi}{2M}\right]$$

..(2)

Where u,v = 0,1,2,...M-1, M is size of sequence; f(i,j) is image in spatial domain and F(u,v) is in frequency domain

$$\alpha(u) = \left(\frac{1}{\sqrt{M}} \ if \ u = 0\right) or \ (\sqrt{\frac{2}{M}} \ if \ u \neq 0)$$



(a) (b)

Figure 10: (a) The whole frame (Global) (b) Block-wise process [5]

III. Singular value decomposition (SVD):

ingular Value Decomposition (SVD) is utilized in image compression, concealment, and watermarking due to its mathematical formula $f = U * S * V^T$. It decomposes an image or video frame into three matrices: U and V are orthogonal matrices, and S is a diagonal matrix containing singular values. SVD's benefits include signal size reduction and robustness against attacks, making it suitable for watermarking applications where watermarking alters U, V, or S matrices. Its stability in maintaining singular values under slight frame disturbances is key to its effectiveness in watermarking[30].

$$f = \mathrm{USV}^T$$

…(3)

Where U and V are orthogonal (or unitary) matrices and S is a diagonal matrix, with the diagonal elements in the descending order of S being called the singular values of the frame (f) and V^T *is the transpose of a MxM matrix containing the orthonormal eigenvectors*.

Watermarking strategies based on SVD embed the watermark by changing U, V, or S. Due to the strong stability of the singular values, SVD techniques are commonly used in video watermarking. This means that when a little perturbation is applied to a frame, these values do not fluctuate much. Although this characteristic of the SVD provides robustness to attacks, a limitation is that performing it on an image is computationally expensive[33]

4.5.3 Compressed domain watermarking

In the realm of video watermarking, compression standards like MPEG-2, MPEG-4, H.264/AVC, and H.265/HEVC play crucial roles, particularly in the compressed domain where techniques such as DCT are commonly applied. Among these standards, H.265/HEVC stands out as the most recent and advanced, surpassing its predecessors in efficiency and capability.

I. **MPEG-2:** Developed jointly by ITU-T and ISO/IEC JTC, MPEG-2/H.262 became widely adopted for digital television and DVD video discs after its completion in 1994[11].

II. **MPEG-4:** Known for its object-based multimedia coding aimed at low data rates (<1 Mbps), MPEG-4 encodes visual information as objects, including natural video, synthetic video, and still textures. It supports various coding tools, interlaced and progressive video encoding, and scalability in time and space[13].

III. **H.264/AVC:** Advanced Video Coding (AVC)/H.264 is a significant video coding standard developed between 1999 and 2003, with subsequent extensions until 2009. It precedes HEVC and offers substantial improvements in compression efficiency[4].

IV. **H.265/HEVC:** High-Efficiency Video Coding (HEVC) is the latest standard jointly developed by ITU-T VCEG and ISO/IEC MPEG. It represents a significant leap in video compression technology, offering superior efficiency compared to H.264/AVC. HEVC achieves this through more complex encoding methods, as detailed in the comparative table below[4][34].

5. Challenges of Efficient Digital Watermarking

Various attributes such as cost, speed, security and many more can be used to describe the efficacy of digital watermarking procedures. It is possible to focus on varied types of attacks after embedding a watermark in the host video. At the decoder end, the watermark is retrieved from the attacked version of the watermarked video[20][17][35].

Figure 11: Challenges of Watermarking

5.1 Imperceptibility: Watermarked data should remain visually indistinguishable from the original signal to the human eye, a critical aspect of watermarking. Imperceptibility concerns primarily invisible watermarking, where the embedded data is not discernible by viewers.

5.2 Payload / Capacity: The payload denotes the amount of watermark data embedded in the cover video. An effective watermarking system balances payload and imperceptibility, ensuring it can convey sufficient data while preserving video quality.

5.3 Blind Detection: Watermark detection can be blind or non-blind. Blind detection methods do not require original data at the receiver's end, making them suitable for video watermarking, where managing large amounts of content is impractical.

5.4 Robustness: A watermarking scheme's robustness refers to its ability to remain detectable even after the watermarked video undergoes various distortions or attacks.

5.5 Security of Watermark: Similar to encryption, the security of watermarking methods ensures that unauthorized removal or alteration of the watermark is difficult without access to a specific key or method.

5.6 Reliability: Watermark reliability ensures that the embedded data remains intact and identifiable, even in the face of unintended alterations or damage.

5.7 Speed: Efficient watermarking techniques embed and extract watermarks quickly and effectively, crucial for real-time applications and large-scale deployments.

5.8 Cost of Operation: The operational complexity of a watermarking algorithm directly impacts its cost in terms of computational resources and time required for embedding and extraction. Minimizing complexity helps maintain operational efficiency and affordability.

These points succinctly cover the essential aspects of video watermarking, focusing on imperceptibility, payload, detection methods, robustness, security, reliability, speed, and operational costs[3].

6. Discussion on Open Issues and Future Work

The design of digital image and video watermarking algorithms must consider several key factors. This study surveys various image and video watermarking methods, highlighting significant research over the past 15 years. While progress has been made in developing diverse watermarking techniques, achieving invisible and robust watermarking remains challenging. Methods such as DCT and DWT-based watermarking enhance robustness for medical data security while maintaining authentication. SVD and entropy-based image watermarking demonstrate good imperceptibility and robustness but vary in terms of time and security parameters. DCT, DWT, and SVD-based blind image watermarking continue to seek optimal balance among robustness, imperceptibility, and embedding capacity. Encryption-based schemes exhibit robustness against compression but are vulnerable to geometric attacks with limited capacity. Spatial domain-based approaches are simpler and more computationally efficient but perform poorly against attacks. Current literature primarily focuses on limited data blocks or images, making them susceptible to various attacks. A proposed approach emphasizes watermarking entire video

s, especially keyframes, to enhance system security. For digital video security, a hybrid watermarking system combining DWT, DCT, and SVD is recommended. DWT captures image variations across scales and aids information localization, DCT handles finite data sequences, and SVD preserves geometric details.

References

[1] Y. Sun, J. Wang, H. Huang, and Q. Chen, "Research on scalable video watermarking algorithm based on H.264 compressed domain," *Optik (Stuttg).*, vol. 227, p. 165911, 2021.

[2] G. Kaur, S. S. Kasana, and M. K. Sharma, "An efficient watermarking scheme for enhanced high efficiency video coding/h.265," *Multimed. Tools Appl.*, vol. 78, no. 9, pp. 12537–12559, 2019.

[3] M. Asikuzzaman and M. R. Pickering, "An Overview of Digital Video Watermarking," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2131–2153, 2018.

[4] M. Goyani and G. Gohil, "Performance analysis of block and non block based approach of invisible image watermarking using SVD in DCT domain," *Commun. Comput. Inf. Sci.*, vol. 131 CCIS, no. PART 1, pp. 348–357, 2011.

[5] R. Thanki, V. Dwivedi, and K. Borisagar, "A hybrid watermarking scheme with CS theory for security of multimedia data," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 31, no. 4, pp. 436–451, 2019.

[6] G. M. E. M. Elahi and Y. H. Yang, "Online learnable keyframe extraction in videos and its application with semantic word vector in action recognition," *arXiv*, 2020.

[7] S. Mei, G. Guan, Z. Wang, S. Wan, M. He, and D. D. Feng, "Author ' s Accepted Manuscript reconstruction Video Summarization via Minimum Sparse Reconstruction," *Pattern Recognit.*, 2014.

[8] M. S. V. Kavita Sahu, "Key Frame Extraction From Video Sequence : A Survey," *Int. Res. J. Eng. Technol.*, vol. 04, no. 05, pp. 1346–1350, 2017.

[9] I. H. Ali and T. T. Al-Fatlawi, "Key Frame Extraction Methods," *Int. J. Pure Appl. Math.*, vol. 119, no. 10, pp. 485–490, 2018.

[10] C. S. Mithlesh and D. Shukla, "A Case Study of Key frame Extraction Techniques," pp. 1292–1298, 2016.

[11] U. Gawande, K. Hajari, and Y. Golhar, "Deep Learning Approach to Key Frame Detection in Human Action Videos," *Recent Trends Comput. Intell.*, pp. 1–16, 2020.

[12] S. Jadon and M. Jasim, "Unsupervised video summarization framework using keyframe extraction and video skimming," *2020 IEEE 5th Int. Conf. Comput. Commun. Autom. ICCCA 2020*, pp. 140–145, 2020.

[13] C. Gianluigi and S. Raimondo, "An innovative algorithm for key frame extraction in video summarization," *J. Real-Time Image Process.*, vol. 1, no. 1, pp. 69–88, 2006.

[14] S. Patel, A. Katharotiya, and M. Goyani, "A Survey on Digital Video Watermarking," vol. 2, no. 6, pp. 3015–3018, 2011.

[15] Y. Liu and P. Zhou, "A survey of Video Watermarking based on Motion Vector," no. Ccit, pp. 274–277, 2014.

[16] N. Tiwari, "Digital Watermarking Applications , Parameter Measures and Techniques," vol. 17, no. 3, pp. 184–194, 2017.

[17] A. Bhardwaj, V. S. Verma, and R. K. Jha, "Robust video watermarking using significant frame selection based on coefficient difference of lifting wavelet transform," *Multimed. Tools Appl.*, vol. 77, no. 15, pp. 19659–19678, 2018.

[18] W. Barhoumi and E. Zagrouba, "On-the-fly Extraction of Key Frames for Efficient Video Summarization," *AASRI*

Procedia, vol. 4, pp. 78–84, 2013.

[19] R. Singh, S. Singh, and N. Sharma, “A Review of digital Watermarking technique,” *Comput. IT Conf. Faridabad, Haryana, India, January*, pp. 1–7, 2019.

[20] N. Agarwal, A. K. Singh, and P. K. Singh, “Survey of robust and imperceptible watermarking,” no. October 2018, 2019.

[21] P. Garg and R. Rama Kishore, “Secured and multi optimized image watermarking using SVD and entropy and prearranged embedding locations in transform domain,” *J. Discret. Math. Sci. Cryptogr.*, vol. 23, no. 1, pp. 73–82, 2020.

[22] D. Singh and S. K. Singh, “DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection,” *Multimed. Tools Appl.*, 2016.

[23] S. Briefs, I. N. Elec, and T. Al, *Robust and Secured Digital Audio Watermarking Using a DWT-SVD- DSSS Hybrid Approach*. .

[24] F. Arab, M. Zamani, S. Poger, C. Manigault, and S. Yu, “A framework to evaluate the performance of video watermarking techniques,” *2019 IEEE 2nd Int. Conf. Inf. Comput. Technol. ICICT 2019*, pp. 114–117, 2019.

[25] Q. Su, Y. Niu, Q. Wang, and G. Sheng, “A blind color image watermarking based on DC component in thespatial domain,” *Optik (Stuttg).*, vol. 124, no. 23, pp. 6255–6260, 2013.

[26] V. M. Potdar, H. Song, and C. Elizabeth, “A survey of digital image watermarking techniques,” *2005 3rd IEEE Int. Conf. Ind. Informatics, INDIN*, vol. 2005, no. 6, pp. 709–716, 2005.

[27] X. L. Liu, C. C. Lin, and S. M. Yuan, “Blind Dual Watermarking for Color Images’ Authentication and Copyright Protection,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 5, pp. 1047–1055, 2018.

[28] T. K. Araghi, A. Bt, A. Manaf, M. Zamani, and S. K. Araghi, “A Survey on Digital Image Watermarking Techniques in Spatial and Transform Domains,” pp. 89–93, 2015.

[29] A. M. U. Wagdarikar, R. K. Senapati, and S. Ekkeli, *A secure video watermarking approach using CRT theorem in DCT domain*, vol. 521. Springer Singapore, 2019.

[30] M. I. Khan, M. Rahman, and I. H. Sarker, “Digital Watermarking for Image Authentication Based on Combined DCT , DWT and SVD Transformation.”

[31] P. Garg and R. R. Kishore, “Performance comparison of various watermarking techniques,” *Multimed. Tools Appl.*, 2020.

[32] H. Fang, H. Zhou, Z. Ma, W. Zhang, and N. Yu, “A robust image watermarking scheme in DCT domain based on adaptive texture direction quantization,” *Multimed. Tools Appl.*, vol. 78, no. 7, pp. 8075–8089, 2019.

[33] G. Singh and N. Goel, “Entropy based image watermarking using discrete wavelet transform and singular value decomposition,” *Proc. 10th INDIACom; 2016 3rd Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2016*, vol. 59, no. 11, pp. 2700–2704, 2016.

[34] R. Gupta, A. Mishra, and S. Jain, “A semi-blind HVS based image watermarking scheme using elliptic curve cryptography,” 2017.

[35] N. J. Janwe, “Video Key-Frame Extraction using Unsupervised Clustering and Mutual Comparison,” no. 10, pp. 73–84, 2016.