The Most Common Characteristics of Fragile Video Watermarking: A Review

Yasmin A. Hassan[1] and Abdul Monem S. Rahma[2]

[1]Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

[2]Department of Computer science, College of Science, Al-Maarif University College, Al-Anbar, Iraq

***Abstract*—The progress of network and multimedia technologies has been phenomenal during the previous two decades. Unauthorized users will be able to copy, retransmit, modify reproduction, and upload the contents more easily as a result of this innovation. Malicious attackers are quite concerned about the development and widespread use of digital video. Digital watermarking technology gives solutions to the aforementioned problems. Watermarking methods can alleviate these issues by embedding a secret watermark in the original host data, allowing the genuine user or file owner to identify any manipulation. In this study, lots of papers have been analyzed and studied carefully, in the period 2011–2022. The historical basis of the subject should not be forgotten so studying old research will give a clear idea of the topic. To aid future researchers in this subject, we give a review of fragile watermarking approaches and some related papers presented in recent years. This paper presents a comparison of many relevant works in this field based on some of the outcomes and improvements gained in these studies, which focuses on the common characteristics that increase the effect of watermarking techniques such as invisibility, tamper detection, recovery, and security.**

***Index Terms*—Fragile watermarking, Video watermarking, Tamper detection, Security, Invisibility.**

I. Introduction

Digital videos, such as online movies, network TVs, and mobile videos, are becoming increasingly common due to the rapid growth of the internet and multimedia technologies (Yu, Wang and Zhou, 2018). Protecting the copyright ownership of original videos, as well as authenticating original works' material has become a pressing concern. As an effective technique to handle the problem of copyright protection and multimedia content authentication, digital watermarking technology has become a study topic in the field of information security (Li, et al., 2020a).

Due to the availability of video content and modern video editing tools on the internet, however, accessing and manipulating video content has become a simple operation, compromising the process of authentication and copyright protection. As a result, it is more important than ever to create solutions that can protect copyrights, identify, and locate video modification (Elrowayati, et al., 2020). In most circumstances, a video editor is used to edit or change a digital video while a video that has been edited is no longer authentic. To solve this problem, additional information is added to this media to ensure authentication and copyright protection (Rahma, et al., 2016). The primary purpose of fragile watermarking is to determine whether or not the video has been tampered with by unauthorized users. Whenever the video has been altered, the algorithm should be capable to find the alteration place on the frames (Munir and Harlili, 2020).

Most watermarking systems are either robust or fragile, robust watermarking is for copyright protection and authentication while fragile watermarking is to detect modification (El Gamal, et al., 2013).

Intraframe and interframe tampering is the two forms of tampering. The insertion or removal of material within the frame is referred to as intraframe manipulation. Adding more frames, removing frames, changing the frame sequence, altering frames, and so on are all examples of interframe manipulation (Patil and Metkar, 2015).

Fragile watermarking may be classified into two kinds based on its purposes: Fragile watermarking for retrieving the original data (recovery) and fragile watermarking for manipulation detection capabilities. The tamper detection fragile watermarking can only detect and locate tampered zone, but it cannot recover the changed frame. Image recovery for tampered areas is essential in several instances (Wang, et al., 2018b).

The rest of this paper is organized as follows. Section II explains video watermarking and common types according to domains, cover media, and perception. In Section III, fragile watermarking has been presented as the core of this paper. In Section IV, the related works have been described;

ARO-The Scientific Journal of Koya University
Vol. XI, No. 1 (2023), Article ID: ARO.11113. 6 pages
DOI: 10.14500/aro.11113
Received: 15 November 2022; Accepted: 25 March 2023
Regular research paper: Published: 03 April 2023
Corresponding author's e-mail: yasmin.a@sc.uobaghdad.edu.iq

Section V, summarizes the characteristics of the effective fragile watermarks, in Section VI presents conclusions of this work.

II. Video Watermarking

Video watermarking is a relatively recent technology that has been proposed to address the issue of unauthorized digital video alteration and dissemination. Watermarking in videos embeds data for identification, intellectual property, and copyright protection (Hassan and Abbas, 2018).

Fragile, robust, and semi-fragile watermarks are the three most common types of video watermarks

A. Fragile watermarking technique is employed to validate integrity authentication in the video when it is modified or tampered with high transparency and huge watermark capacities (Agarwal and Husain, 2021).
B. Robust watermarking must withstand the majority of typical video processing operations, such as recompression and filtering, and may come at the expense of transparency and watermark capacity. It is mostly used to protect copyright.

A. Semi-fragile watermarking is unaffected by conventional video processing procedures, but it is vulnerable to malicious assaults, making it ideal for tamper detection (Zhou, et al., 2022).

The digital watermarking systems may be further divided into spatial domain watermarking and transform domain watermarking based on the embedding domain as mentioned in Fig. 1 (Wang, et al., 2018a).

The watermarked message is inserted into the host image by directly modifying its pixel values in the spatial domain. The least significant bit (LSB) watermarking strategy is the most used method in the spatial domain.

For every potential alteration on the host frame, this embedding approach has a high level of fragility. It has been extensively employed for picture authentication and recovery due to its simplicity (Begum and Uddin, 2020). In the transform domain, the watermark is concealed in the host image through modulating transform domain coefficients (Yu, Wang and Zhou, 2019). The discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) are the most often utilized transformations (SVD). The robust and semi-fragile watermarking procedures are frequently conducted in the transform domain to ensure improved resilience against alterations (Wang, et al., 2018b)

III. Fragile Watermarking

Fragile watermarking is a type of watermarking that allows for precise authentication [5]. Watermarks are embedded in files that may be verified to see whether they are the same watermarked file. Fragile watermarking is rarely used in everyday situations since any modification made to the file, whether on purpose or by mistake, will be considered a new file (Gutub, 2022). Fragile watermarking has a few specific applications, such as checking for tampering or changes to works-in-progress. Fragile watermarking has a few specific applications, such as checking for tampering or changes to works-in-progress, even if it was just due to noise (Akhtar et al., 2022).

A fragile watermark includes three elements: watermark insertion, tamper detection, and tamper localization

- Watermark insertion is a process that editing a secret key to the original picture before it is spread. For a peripheral user, the watermarked image is nearly identical to the original image.
- Tamper detection is mainly based on statistical processes and it can be verified on a sample image that has been appropriately analyzed by measuring the true positive (TP) and false positive (FP) rates on the altered image, which are calculated by dividing the number of pixels detected as tampered by the number of pixels that have been really tampered.
- Tamper localization identifies the image's altered parts. As a result of the tamper localization technique, a two-level image exhibiting the ground of the modified areas can be generated (Di Martino and Sessa, 2012).

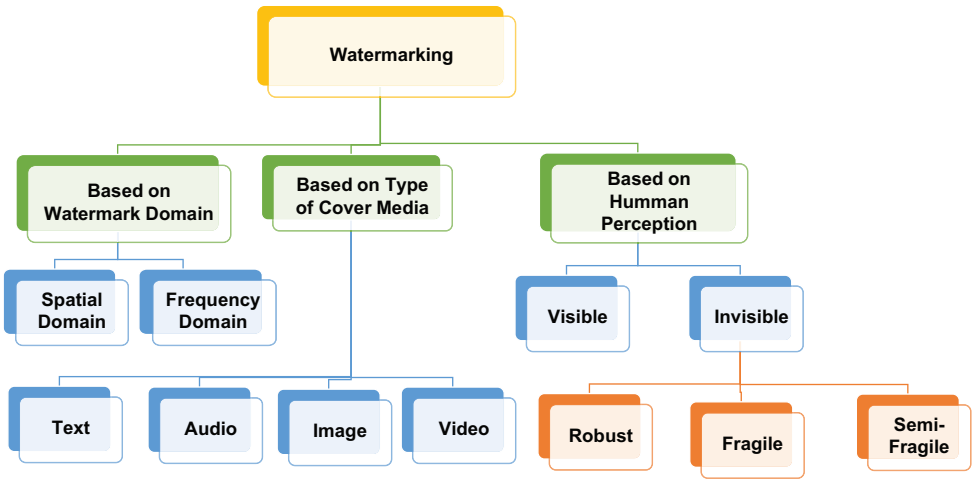

Fig. 1. General block diagram of watermarking.

IV. Related Work

Fragile Watermarking for digital video has been a popular research topic. Commercial software has recently made it quite easy to change digital video, increasing the need to verify video material authenticity (Makhrib and Karim, 2022). In this study, the most common techniques for fragile watermarking have been collected to solve the current problems mentioned above. The search was done in Google scholar, research gate, and Google as a big library to us and takes only initial results of searching in time 2011–2022.

- Zhi-yu and Xiang-hong (2011) provide a fragile watermarking-based technique for color video integrity authentication. The RGB color mode is converted to YST, which is used to insert watermarking into the original video. The simulation results demonstrate that the technique is capable of maintaining video quality while also detecting tampering and attacks on the source material.
- El Gamal, et al. (2013) present a method of video watermarking (fragile) capable of detecting tampering in spatial domains. A mathematical method is used to incorporate the watermark bits for each block independently. The suggested technique successfully detects a large variety of tampering threats with a high detection rate at a low computation cost.
- Patil and Metkar (2015) designed a technique of fragile video watermarking to determine the tampered area. The watermark is generated from block numbers and frame numbers that are inserted into the frame as a watermark in the frequency domain. This method is really sensitive to changes, has a high capacity and transparency, and can also notice manipulation.
- Ait Sadi, et al. (2017) offer a technique for ensuring the integrity of the H.264/AVC video stream employing separate authentication of each Group of Pictures (GOPs) inside the video based on a content fragile video watermarking mechanism. While keeping the original bitrate and perceptual quality, the suggested approach delivers an accurate authentication mechanism with great fragility and fidelity. Its ability to detect tampered frames in the case of spatial, temporal, and color changes has also been shown.
- Bhattacharya and Palit (2018) provide a method for reducing the reference strategy by combining robust picture characteristics with fragile watermarking approaches. The technique does not require any other data other than the input image. The watermark is built from the picture to be sent using robust image characteristics and then placed as a fragile watermark in the image itself.
- Munir (2019) provides a spatial domain fragile watermarking technique for ensuring the integrity of video digital material. To boost security, the watermark is encrypted before embedding by XOR-ing it with a random image. A chaotic map, such as the Arnold Cat Map, is used to produce a random picture. The algorithm can recognize and pinpoint the changed region of video frames quite effectively, according to the results of the experiments.
- Munir and Harlili (2019) suggest a fragile video watermarking technique based on chaos is suggested in the spatial domain. The watermark is a binary picture of the same size as the video frame size. To boost security, the watermark is coded using an XOR operation with a random picture before inserting. A cross-Coupled Chaotic Random Bit Generator (CCCBG) is used to create the random picture. The encrypted watermark is inserted into every RGB element of each frame.
- Hammami, et al. (2020b) offer a new semi-fragile frequency domain watermarking approach for surveillance video authentication. The system begins by producing a binary watermark using a unique watermark generation method. Regions of Interest (ROI) are recognized and employed as watermark holders throughout the embedding process. SVD and discrete wavelet transform (DWT) are used to decompose these areas into distinct frequency sub-bands.
- Li, et al. (2020a) present a semi-fragile video watermarking technique that can accomplish frame attack and video tamper detection at the same time performed by adding authentication code based on the numerical interaction of the DCT coefficients and the frame number as the watermark information.
- Munir and Harlili (2020) based on the chaotic map, a weak video watermarking was presented. The watermark is encrypted, watermark has been applied using an XOR operation with a random picture to boost security. "Cross-Coupled Chaotic Random Bit Generator is used to create the random picture (CCCBG)". Every RGB element of each frame contains the coded watermark.
- Aminuddin and Ernawan (2022) present a color image authentication based on blind fragile image watermarking for tamper detection and self-recovery. The proposed technique utilizes an LSB shifting algorithm that can decrease the pixel intensity variation between the cover and watermarked images.

Table I present a comparison of previous works in this field including the used technique, used metrics main achievement that researchers accomplish in their papers with the limitations, and the accessed results concerning PSNR for the period (2011–2022). As a result of this comparison, the most used technique for fragile watermarking is the least significant bit (LSB). It is fast and easy to apply and does not consume much time compared to the use of transform algorithms but it is easy to crack, therefore, fragile watermarking with LSB is used for tamper detection in real-time video in addition to robust watermarking to obtain an efficient and secured system.

V. Characteristics of an Effective Fragile Watermark

Based on the purpose of the watermarking algorithm, there are several features used to evaluate the efficiency of a fragile watermarking method.

A. Perceptibility: The inserted watermark should be completely invisible. It must be hard to notice it through human vision, and it should not affect the regular operation of the host image. In general, the stronger the watermark's security,

TABLE I
A Comparison Based on Previous Relevant Works

References	Technique	Evaluation metrics	Achievements	Limitations	Results (PSNR)
Zhi-yu and Xiang-hong, 2011	YST color mode and DCT	PSNR	Good security after encryption, effective detection of video attacks, and localizing the position of tampering.	No recovery.	*33.64 **19.1
El Gamal, *et al*., 2013	Spatial domain, block mean, and modulation factor.	PSNR	a minimal cost of computing and a high rate of detection against a variety of tampering attempts	Not all frames with watermarks can fully retrieve the watermark that is inserted.	*55.5 **49.2
Patil and Metkar, 2015	LSB and DCT	PSNR, SSIM	high capacity and transparency, and smaller video distortion.	not robust against compression.	*38.2 **19.4
Ait Sadi, *et al*., 2017	DCT	PSNR, SSIM, and video quality metric	The system is sensitive enough to identify altered spatial, temporal, and color frames that are tampered with in videos.	To find the altered frames, the algorithm needs extra time.	*40.05 **34.91
Munir, 2019	Arnold Cat Map	NM	The algorithm does a great job of locating and detecting changed areas in video frames.	Don't use transform domain and compression.	NM
Hammami, *et al*., 2020a	DWT and SVD	PSNR and BER	It effectively distinguishes between harmful and normal actions.	No recovery	*73.42 **48.74
Li, *et al*., 2020b	DCT	PSNR	The technique displays high resilience, as the embedded watermarked video's visual quality is almost unaffected.	NM	*38.1 **33
Aminuddin and Ernawan, 2022	LSB	PSNR and SSIM	More security due to using two LSB for embedding watermark	The proposed scheme consumes a large time.	*43.63 **22.39
Makhrib and Karim, 2022	Modified LBP, LSB	PSNR and MSE	The suggested method provides improved robustness, greater imperceptibility, and good invisibility.	NM	*54.42
Al-Otum and Ellubani, 2022	DWT and LSB	PSNR and SSIM	Good security and effective self-restoration and tamper detection for color images	Consume more time	*44.52 **31.47

*Highest result. **Lowest result. NM: Not mentioned, DCT: Discrete cosine transform, DWT: Discrete wavelet transform, LSB: Least significant bit, PSNR: Peak signal-to-noise ratio, SVD: Singular value decomposition, SSIM: Structural SIMilarity index

TABLE II
A Comparison of Different Watermarking Techniques with the Most Common Factors

References	Used technique	Transform	Size of block	Watermark type	Invisibility	Tamper detection	Recovery	Robustness
Zhi-yu and Xiang-hong, 2011	Frequency domain	YST and DCT	4×4	Fragile	Yes	Yes	No	Yes*
Zigomitros, Papageorgiou and Patsakis, 2012	Watermar-king in social network	No transform		Robust and semi-fragile	NM	Yes	NM	Yes
El Gamal, *et al*., 2013	Spatial domain, modulation	No transform	B×B	Fragile	Yes	Yes	Yes	Yes
Patil and Metkar, 2015	Frequency domain	DCT	8×8	Fragile	Yes	Yes	No	No
Bhattacharya and Palit, 2018	Frequency domain	SVD		Fragile	NM	NM	NM	Yes
Ait Sadi, *et al*., 2017	Motion vector	DCT		Fragile	NM	Yes	No	Yes
Wang, *et al*., 2018b	Spatial domain and frequency domain	NM	NM	Fragile	Yes	Yes*	Yes*	Yes
Munir, 2019	Spatial domain and Arnold Cat Map	DCT		Fragile	NM	Yes	Yes	Yes
Rakhmawati, Wirawan and Suwadi, 2019	Frequency domain	DCT, DWT, DCT-DWT	8×8	Fragile	NM	Yes	Yes	Yes
Li, *et al*., 2020a	Frequency domain	DCT	4×4	Semi-fragile	Yes	Yes	No	No
Munir and Harlili, 2020	Spatial domain based on chaos and cross-coupled chaotic random bit generator	No transform		Fragile	NM	Yes	Yes	Yes*
Hammami, Ben Hamida and Ben Amar, 2021	ROI, and QR	SVD and DWT		Semi- fragile	Yes	Yes	NM	Yes
Makhrib and Karim, 2022	Modified LBP, LSB	No transform		Fragile	Yes*	Yes	NM	NM
Al-Otum and Ellubani, 2022	LSB	DWT		Robust and fragile	Yes	Yes	Yes	Yes
Shukla, *et al*., 2022	LSB	No transform		Fragile	NM	Yes	No	Yes
Aminuddin and Ernawan, 2022	LSB	No transform	2×2	Fragile	Yes*	Yes	Yes	Yes

*Intentional effect. NM: Not mentioned, DCT: Discrete cosine transform, DWT: Discrete wavelet transform, LSB: Least significant bit, SVD: Singular value decomposition

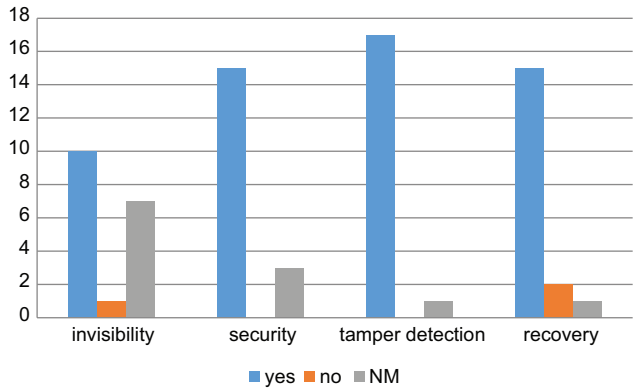

Fig. 2. The most common characteristics of this study.

the better the imperceptibility.

B. Tamper detection: A fragile watermark should be able to locate where the tampering has been done to determine the directions of attackers to prevent such attacks in the future. The effect of picture recovery is determined by the tamper detection capability.
C. Tamper recovery: The system must have the ability to detect unlawful picture alterations and recover photos from those that have been tampered with. The higher the tamper detection accuracy, the better the picture recovery outcome.
D. Robust to known attacks: The design should be as resistant to well-known attacks as possible, such as the general, collage, and disturbing attacks (Wang, et al., 2018b, Rakhmawati, Wirawan and Suwadi, 2019).

In Table II, a comparison was presented between previous researchers and their achievements through a set of factors, including invisibility, which should be achieved in most watermarking techniques to thwart unauthorized users and cut the road to them when trying to know the watermark data. Detection of tampering, the main goal of the fragile watermarks, locating the tampered zone, and knowing the direction of the piracy when manipulating the content of video frames. Not all watermarking systems achieve recovery properties although it may be an essential point in some systems depending on the used application.

Fig. 2 visually summarizes the characteristics and shows that the most previous researches achieve these characteristics and it can be included that the feature of detecting manipulation is the most applied characteristic. As a result, whenever these factors combine, the watermark achieves the best effect when it is added to the video.

VI. Conclusion

Digital watermarking is a technique in which information is inserted in media for authentication, copyright protection, tamper detection, or modification area. Digital watermarking methods, in general, handle the problem of manipulating frames by inserting secret data directly in the image and identifying the changed area immediately. Based on the analysis, the fragile watermarking methods are effective in real-time video processing in terms of finding the zone of tampering in the video in addition to robust watermarks to ensure copyright protection, the integrity of the video and, tamper detection in video. In this review, a comparison was presented between previous researchers and their achievements through a set of factors, including concealment, detection of change, retrieval, and safety, and as a result, whenever these factors combine, the watermark achieves the best effect when it is added to the video.

References

Agarwal, H. and Husain, F. 2021. Development of payload capacity enhanced robust video watermarking scheme based on the symmetry of circle using lifting wavelet transform and SURF. *Journal of Information Security and Applications,* 59, p. 102846.

Ait Sadi, K., Guessoum, A., Bouridane, A. and Khelifi, F. 2017. Content fragile watermarking for H.264/AVC video authentication. *International Journal of Electronics,* 104, pp. 673-691.

Akhtar, N., Saddique, M., Asghar, K., Bajwa, U.I., Hussain, M. and Habib, Z. 2022. Digital video tampering detection and localization: Review, representations, challenges and algorithm. *Mathematics,* 10, p. 168.

Al-Otum, H.M. and Ellubani, A.A.A. 2022. Secure and effective color image tampering detection and self restoration using a dual watermarking approach. *Optik*, 262, p. 169280.

Aminuddin, A. and Ernawan, F. 2022. AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking. *Journal of King Saud University-Computer and Information Sciences*, 34, pp. 5822-5840.

Begum, M. and Uddin, M.S. 2020. Digital image watermarking techniques: A review. *Information,* 11, p. 110.

Bhattacharya, A. and Palit, S. 2018. Blind quality assessment of image and video based on fragile watermarking and robust features. *Multidimensional Systems and Signal Processing,* 29, pp. 1679-1709.

Di Martino, F. and Sessa, S. 2012. Fragile watermarking tamper detection with images compressed by fuzzy transform. *Information Sciences,* 195, pp. 62-90.

El Gamal, A., Mosa, N. and El Said, W. 2013. A fragile video watermarking algorithm for content authentication based on block mean and modulation factor. *International Journal of Computer Applications,* 80, pp. 21-28.

Elrowayati, A.A., Alrshah, M.A., Abdullah, M.F.L. and Latip, R. 2020. Hevc watermarking techniques for authentication and copyright applications: Challenges and opportunities. *IEEE Access,* 8, pp. 114172-114189.

Gutub, A.A.A. 2022. Adopting counting-based secret-sharing for e-Video Watermarking allowing Fractional Invalidation. *Multimedia Tools and Applications,* 81, pp. 9527-9547.

Hammami, A., Ben Hamida, A. and Ben Amar, C. 2021. Blind semi-fragile watermarking scheme for video authentication in video surveillance context. *Multimedia Tools and Applications,* 80, pp. 7479-7513.

Hammami, A., Hamida, A.B., Amar, C.B. and Nicolas, H. 2020a. Regions based semi-fragile watermarking scheme for video authentication. *Journal of WSCG,* 28, pp. 96-104.

Hammami, A., Hamida, A.B., Nicolas, H. and Amar, C.B. 2020b. Regions based semi-fragile watermarking scheme for video authentication. In: *International Conference in Central Europe on Computer Graphics, Visualization and Computer Vision,* pp. 96-104.

Hassan, N.F. and Abbas, R.N. 2018. Proposed video watermarking algorithm based on edge or corner regions. *Engineering and Technology Journal,* 36, 25-32.

Li, C., Yang, Y., Liu, K. and Tian, L. 2020a. A semi-fragile video watermarking

algorithm based on H. 264/AVC. *Wireless Communications and Mobile Computing,* 2020, p. 8848553.

Li, C., Yang, Y., Liu, K. and Tian, L. 2020b. A semi-fragile video watermarking algorithm based on H. 264/AVC. *Wireless Communications and Mobile Computing,* 2020, p. 8848553.

Makhrib, Z.F. and Karim, A.A. 2022. Improved fragile watermarking technique using modified LBP operator. In: *2022 International Conference on Computer Science and Software Engineering (CSASE)*. IEEE, United States, pp. 132-137.

Munir, R. 2019. A secure fragile video watermarking algorithm for content authentication based on arnold CAT map. In: *2019 4th International Conference on Information Technology (InCIT).* IEEE, United States, pp. 32-37.

Munir, R. and Harlili, H. 2020. Application of chaos-based fragile watermarking to authenticate digital video. In: *Digital Forensic Science.* IntechOpen, London.

Munir, R. and Harlili, H. 2019. *Authentication of Digital Video Using Fragile Watermarking Algorithm Based on Chaotic Map*.

Patil, R.D. and Metkar, S. 2015. Fragile video watermarking for tampering detection and localization. In: *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI).* IEEE, United States. pp. 1661-1666.

Rahma, A.M., Abdulmunim, M.E. and Al-Janabi, R.J. 2016. New Watermark Algorithm support Based on Watermark Designing. *Diyala Journal For Pure Science,* 12, 1-11.

Rakhmawati, L., Wirawan, W. and Suwadi, S. 2019. A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability. *EURASIP Journal on Image and Video Processing,* 2019, pp. 1-22.

Shukla, A., Gupta, A., Jaglan, S. and Shivani, S. 2022. An efficient self-embedding fragile watermarking scheme based on neighborhood relationship. In: *Innovations in Computational Intelligence and Computer Vision.* Springer, Germany.

Wang, C., Shan, R. and Zhou, X. 2018a. Anti-HEVC recompression video watermarking algorithm based on the all phase biorthogonal transform and SVD. *IETE Technical Review,* 35, pp. 42-58.

Wang, C., Zhang, H. and Zhou, X. 2018b. Review on self-embedding fragile watermarking for image authentication and self-recovery. *Journal of Information Processing Systems,* 14, pp. 510-522.

Yu, X., Wang, C. and Zhou, X. 2018. A survey on robust video watermarking algorithms for copyright protection. *Applied Sciences,* 8, p. 1891.

Yu, X., Wang, C. and Zhou, X. 2019. A hybrid transforms-based robust video zero-watermarking algorithm for resisting high efficiency video coding compression. *IEEE Access,* 7, pp. 115708-115724.

Zhi-Yu, H. and Xiang-Hong, T. 2011, Integrity authentication scheme of color video based on the fragile watermarking. In: *2011 International Conference on Electronics, Communications and Control (ICECC).* IEEE, United States, pp. 4354-4358.

Zhou, L., Zuo, M.J., Shi, H., Zhang, Y. and Gong, L.H. 2022. Robust watermarking algorithm against the geometric attacks based on non-subsampled shearlet transform and Harris-Laplace detector. *Security and Communication Networks,* 2022, p. 7605595.

Zigomitros, A., Papageorgiou, A. and Patsakis, C. 2012. Social network content management through watermarking. In: *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, United States, pp. 1381-1386.