International Journal of Research in Engineering, Science and Management
Volume 5, Issue 11, November 2022
https://www.ijresm.com | ISSN (Online): 2581-5792

A Robust Hybrid Watermarking Scheme Using a New Colour Image Watermarking Algorithm Based on SVD and Arnold Scrambling Technique

K. Premkumar[1], S. A. Muhammad Yusuf[2], R. Thangapandi[3], M. R. Sankaranarayanan[4*], S. Sasivel[5]
[1]*Assistant Professor, SRM Institute of Science and Technology, Ramapuram, Chennai, India*
[2,3,4,5]*Student, SRM Institute of Science and Technology, Ramapuram, Chennai, India*

***Abstract*: Regular internet users have led to a dramatic increase in the rate at which digital information is transmitted or shared over the internet. Large-scale copyright infringement is discussed in this guide to show how simple it is to do. Digital multimedia such as photographs, articles, songs, and videos can easily be manipulated or fabricated. For this reason, some have suggested using digital image watermarking (DIW). Therefore, it is necessary to create a blind image watermarking (BIW) technique that outperforms both current BIW and non - BIW methods. In order to improve the BIW system's performance, we need to develop hybrid optimal approaches making use of the combined transformation techniques, which can achieve greater invisibility, robustness, embedding capacity, etc. With the advantages of both SVD and ARS (Arnold Scrambling), a novel hybrid SVD with ARS watermarking embedding and extraction technique is presented, allowing for greater invisibility and effective resilience against a wide range of geometrical and non- geometrical attacks. In addition, an ARS - based optimization method for optimum ESF's was developed to address issues with constraints in ESF's, leading to enhanced robustness and imperceptibility compared to the non-optimized case. When compared to other BIW methods in the literature, such as RDWT - SVD, RDWT - PCA with IGWO, RDWT -PCA -SVD with IGWO, and even RDWT -DCT -ARS, the one proposed here using SVD with ARS optimization provides superior robustness and imperceptibility.**

***Keywords*: SVD, ARS, Watermarking, PCA, DWT.**

1. Introduction

With the proliferation of online interactions and data transfers, the need for data and information- specific security services have grown. Digital watermarking is widely used as a means of providing authentication and non-repudiation [1]. Due to the proliferation of multimedia content, digital image watermarking is a hot topic of study [2].

Because of their durability and invisibility, transform domain techniques have become widely used for image watermarking (RAI). Digital image watermarking is a highly active research field due to its numerous potential applications, such as digital copyrights management and protection. Since the Internet has facilitated the dissemination, promotion, and monetization of works of authorship such as photographs, videos, documents, etc., it is essential that the publishing copyright be safeguarded.

All business applications have been moving towards the digital era due to the rapid advancements in current technologies such as communication, networked multimedia systems [3], and digital data storage. In addition, over the past two decades, internet use in the business world has skyrocketed as companies seek to increase productivity, efficiency, and security through the use of digitization. Digital information such as text, images, music, video, and software is exchanged over a public network and must be safeguarded [4].

The innovative technique of Digital Image Watermarking (DIW) has potential uses in the fields of medicine, the military, and archival storage. Textual, visual, aural, and video watermarks can all be permanently embedded in a file, making them extremely difficult to remove and virtually undetectable. Incorporating a covert digital information, watermark or not, is detectable. Although the embedded digital data is preserved, it is imperfect. It is for this reason that reversible watermarking was developed; this method is widely regarded as superior to encryption and allows for the recovery of the original data.

Watermarking prevents the loss of semantic information from the host data, which can occur in cryptography because the resultant data may not be visible or understandable even at the time of retrieval. Multiple watermarking techniques refer to the practise of embedding more than one watermark into a digital file simultaneously. In the same way that a physical signature guarantees the authenticity of a document, so too does a digitally issued DIW [5]. It's possible for a watermark to be shared among multiple copies or unique to each one (e.g., to identify the document source).

2. Methodology of Digital Image Watermarking

The two primary operations in DIW are the embedding and extracting processes [6], [7]. While the media files are being embedded, the watermark is added (digital data). As early as the 13th century, paper mill owners were inserting watermarks into their products to show that only their paper had been made.

As a result, its origins can be traced back to the demands of authorship verification, property assertion, and intellectual property protection. Stamps and banknotes quickly adopted

*Corresponding author: sm8159@srmist.edu.in

watermarking for this reason. Watermarks are predetermined patterns that can be covertly embedded in an object (such as paper) without the owner's knowledge.

To this end, we propose a robust formal mechanism that can be used to monitor and identify these harmful and unlawful actions. This desire stems from the fact that being able to identify such perpetrators is highly desirable.

Figure 1 depicts the overarching procedure of watermarking, in which the watermark is likely embedded in a signal that can withstand some level of noise by means of a function for embedding [8]. In the course of data transmission and exchange, the signal could be attacked using any number of attacking functions. The watermark can withstand the attack and be recovered by the end user with the help of a detecting/revealing mechanism.

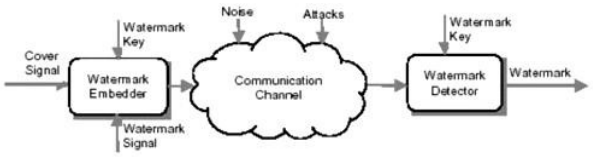

Fig. 1. Typical DIW setup

A. Motivation

The study of how to acquire BIW can be thought of as the primary research problem. Copyright problems have multiplied alongside the expansion of the internet and the availability of media applications. Therefore, safeguarding media files is an urgent concern. Applying digital watermarking methods to the content in question is an effective way to combat these types of problems.

Several BIW techniques are used to obfuscate data in the host image for purposes of data authentication and copyright protection. Because of this, there is a pressing need for a new generation of BIW techniques that can withstand multiple attacks while still producing an easily discernible watermark that has been extracted. In order to improve the watermark's durability and protection, hybrid watermarking techniques were proposed. Complete invisibility and high robustness are guaranteed by the proposed hybrid BIW approach.

Digital media (photos, videos, music, etc.) are widely disseminated online. Since digital media can be copied and altered so easily, protecting intellectual property has become an urgent issue. Researchers and businesses took notice of this gap in the market, and a novel information concealing format called BIW was born as a result. It is expected that BIW will serve as a very effective tool for protecting IP.

There have been numerous academic studies on watermarking, leading to the development of a variety of algorithms for the task, some of which are effective in both the frequency and spatial domains. In comparison to other methods, watermarks have the following benefits: It is impossible to find them. It is important to note that data is not lost during format conversion.

A BIW's RAI is an admirable trait. The quality of the watermarked information should be as close to that of the unaltered source material as is practically possible. The goal of this hybrid technique based on bio-optimization is to boost performance by enhancing RAI with reduced time complexity compared to currently used methods.

3. Analyzing the Literature

Several studies published over the past decade offer guidance on the design and implementation of digital watermarks for digital images in a variety of contexts. However, only a small fraction of them have been subjected to in-depth analysis in order to determine where the field currently stands. In the sections that follow, you'll find the explanations. Algorithms that mimic the way nature works are increasingly used as a heuristic approach to optimization problems. By treating watermark extraction as an optimization problem, some scientists have determined the best settings for the parameters in their methods.

Blind QoS estimation for multimedia communication systems was introduced by [9]. To estimate the quality of the communication system, digital watermarking is used here. The findings presented here are useful for evaluating emerging trends in mobile communication.

The security benefits of watermarking have been summarized by [10]. Information leakage has been quantified, and the security provided by spread spectrum watermarking has been analysed across a variety of use cases.

The real numbers were converted to integers using the cat swarm optimization (CSO) algorithm, developed by [11]. To do this, they used a fitness function based on numerical dissimilarity. Also, they have compared CSO's performance to that of particle swarm optimization (PSO) and a modified PSO with dynamic inertia for this specific application.

Additive, correlation, least significant bit, patchwork spread spectrum, and texture mapping are among the six spatial watermarking methods proposed by [12].

To protect the copyright of images and to strengthen them, [13] proposed a new method for data hiding by embedded image compression technique. Before being compressed further, images are watermarked with a secret message reading "Hello World" and encrypted with the original "Hello World" data.

Regarding human perception, [14] showed that many ink patterns look the same. Specifically, they suggested embedding watermarks using phase modulation in halftone images. The watermarked area of the cover image is modulated with threshold T1, while the surrounding areas are modulated with threshold T0. To begin, we'll create a T0 and T1 halftone from the cover image, which will serve as im0 and im1 respectively.

A method for color-blind watermarking was developed by [15]; it involves the use of QR decomposition to hide the original image within the watermarked one. Multiple attacks were also used on the watermarked image, revealing the superiority of the new method.

Cardinality analysis was also included in the geo- spatial watermarking proposal by [16]. In addition, BIW was simultaneously introduced for polylines in vector geo -spatial data. They used a ratio of the distances between the vertices of polylines as a feature.

Using a pseudo random address vector [17] proposed a spatial domain-based approach for BIW, making it difficult for an adversary to locate the watermark and ensuring the safety of the system. In order to verify the reliability of claimed locations, a number of geometrical and image processing attacks were applied.

When it comes to protecting digital images from unauthorised duplication [18] tackled the issue of watermark embedding and extraction, with the former being accomplished in the spatial domain through the modification of luminance components in the latter's host images. The classification as fragile watermarking is based on the results of experiments.

The cover image features are extracted using SVD, and [19] presented a robust copyright protection scheme based on FrFT and visual cryptography. The result showed robustness in the face of multiple signal- processing operations.

In the DCT -based extraction method presented by [20], the key is first used to seed a pseudo random number generator, and the resulting coefficients are applied to a forward DCT - decomposed image. The watermark is a rearrangement of the vector that was computed.

[21] proposed a method to incorporate a grayscale watermark into a coloured host image. For this, they've resorted to a colour space devoid of correlation. Further, GA is employed in the optimization process.

4. Proposed Model

The two most crucial steps in any watermarking system—the embedding and extracting processes—run simultaneously. To create a watermarked image, the watermark is first embedded into the source image, and then its detect ability is evaluated to determine the level of similarity.

At this point, we abstract the watermark from the attacked watermarked image and compare it to the original watermark to determine the algorithm's strength. To abstract the watermark, the initial image is used in NBIW but not in BIW.

Several studies have been revised to increase the efficacy of colour detection and the indiscernibility of watermarking methods by embedding watermark pictures in a hybrid domain, thereby addressing the limitations and restrictions of previously suggested watermarking methodologies.

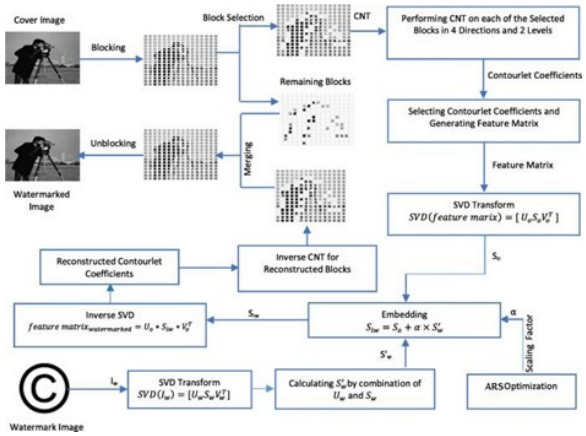

Fig. 2. Embedding a watermark with the help of SVD and optimizing it with ARS

Here, SVD, a linear algebra, is combined with the discrete cosine transform (DCT) and the radial basis function transform (RBFT) to produce a watermarked image that is both easily readable and secure against a wide range of geometric and non-geometric attacks. By combining transformations, we can alleviate the conflict between maximizing efficiency and preserving the integrity of the watermark.

A. The Method of Embedding Watermarks

The cover photo is denoted by C, the watermarked image by W, and the final watermarked image, W_{out}. Figure 2 displays the watermark embedding procedure and provides an in-depth analysis of the embedding method.

The step one, RDWT applies LPF's and HPF's to the rows and columns of the image to create four frequency bands. Only the LLC band has low frequency image characteristics among the four bands (LLC, HLC, LHC, and HHC). For this reason, it is considered during the watermarking process. In a similar vein, we get LLW by performing RDWT on W and. In order to proceed with the extraction process, the remaining three bands (LLw, HLw, and LHw) from the watermark RDWT procedure must be available.

The Step two is Used to discrete cosine transform (DCT) on both low pass components to generate a multi-band breakdown using multiple frequencies, making the embedding method universally applicable. The DCT is primarily concerned with embedding information in intermediate frequencies to mitigate various attacks. The result of applying DCT to LLC is LLCd, and the result of applying DCT to LLw is LLwd.

The third step is to apply the SVD process to each individual DCT output. For RAI in the embedding process, the SVD process divides the image into three matrices (U, S, and V). The results of SVD on LLCd are SC, UC, and VC, while the results for LL wd are Sw, Uw, and Vw. While the Uw and Vw outputs will be helpful for de-watermarking, the UC and VC outputs will be of use for embedding. The primary embedding operation will be carried out on the singular matrices Sw and SC because they contain the most relevant picture information.

The fourth and most crucial step of watermarking is data embedding, which involves manipulating the image data in relation to the ESF's. When this embedding factor is used, the system's defences are strengthened. The watermarked image can be difficult to recover if the embedding factor is incorrect. This means that it is challenging for an attacker to obtain the embedding factor if the user generates it using optimization techniques. As a result, we develop a bio- inspired ARS algorithm for making uniform ESF's.

Fifth, run the reverse SVD procedure with Snew, UC, and VC as inputs to get Wnew as the result. Create LL new by performing the IDCT on Wnew. Execute the IRDWT operation on LL new, HLC, LHC, and HHC to generate the final watermarked output image Wout.

B. The Extraction of Watermarks

In this case, we will call the extracted watermark output Wed, and the watermark embedding method's output W_{out}. Figure 3 depicts the watermark extraction procedure and provides an in-

Table 1
The effectiveness of SVD with ARS optimization

Metrics	SVD Without ARS Optimization			SVD With ARS Optimization
	0.01	0.02	0.1	
MSE	6.9222e-05	2.2568e-05	5.0378e-05	1.0827e-05
PSNR (in dB)	66.3406	70.5306	67.043	73.7205
SSIM index	0.96153	0.96891	0.95486	0.98843
NCC	0.99985	0.99996	0.99994	0.99998

depth analysis of the extraction method.

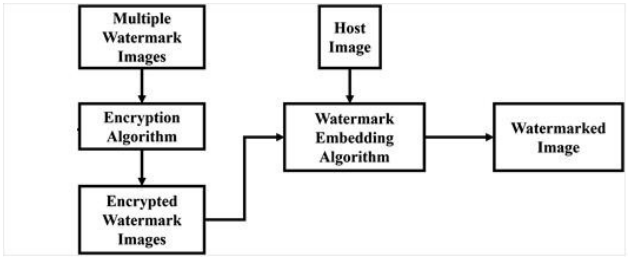

Fig. 3. SVD watermark extraction algorithm that uses the ARS optimization technique

- In the first step, four bands will be extracted from Wout via an RDWT operation. Among these frequencies, only the LLwout band has image characteristics at low frequencies. Therefore, it is assessed whether or not additional watermarking is necessary.
- The second stage is to perform a DCT operation on the LLwout low components. As a result of applying the DCT to LLwout, LLwoutd is generated.
- The SVD of LLwoutd produces Swout, Uwout, and Vwout at Step Three. Uwout and Vwout are not de-watermarkable outputs. Swout will be the primary target for data extraction due to the wealth of visual data it contains.
- In the fourth step, known as data extraction, the original singular matrix values are recovered by using the same alpha value obtained via ARS, the SC, and Swout as inputs to generate the output Sed.
- Fifth, we reverse the SVD process using Sed,Uw, and Vw as inputs to get Wed as the final result. Wednesday, perform the IDCT operation and store the file as LLed. Execute the IRDWT process on LLed, HLw, LHw, and HHw to generate the final extracted watermark output image Wed.

5. Result and Discussion

The goal of most DIW research is to develop a technique that effectively hides the watermark so that the viewer cannot detect it, resulting in a high RAI. Here, we present an in-depth analysis of the proposed BIW's performance in SVD, both with and without ARS optimization.

The optimization scheme ARS will be shown to be superior to older methods in a number of quantitative and qualitative respects. Keep your concealed watermark strong in the face of attacks designed to destroy or erase it. Therefore, an extensive experimental study of the proposed watermark embedding and extraction process under different conditions is included in this section as well a variety of quality metrics, and defending against attacks, all in the name of RAI.

The proposed results show superiority in conventional applications when compared to the outcomes of other conventional techniques. Figure 4(a) and Figure 4(b) depict the tried-and-true cover 4(c) and watermark images for the proposed BIW method 4(d).

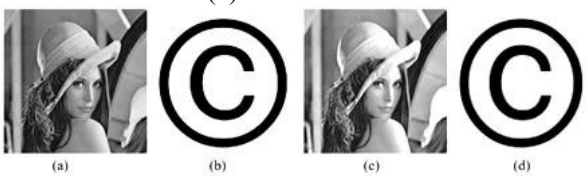

Fig. 4. Illustration of Embedding and Extraction with SVD without ARS Optimization One that provides protection, or a cover. Marker of Depth (b) To be watermarked, (c) Watermark images that were extracted (d)

The scenario is further supported by the results of calculating the various quality indicators shown in Table 1, which show that the proposed SVD with ARS optimization [95*] exhibits superior performance and higher RAI features for diverse ESF's of alpha 0.01, 0.02 and 0.1 shown in figure 5.

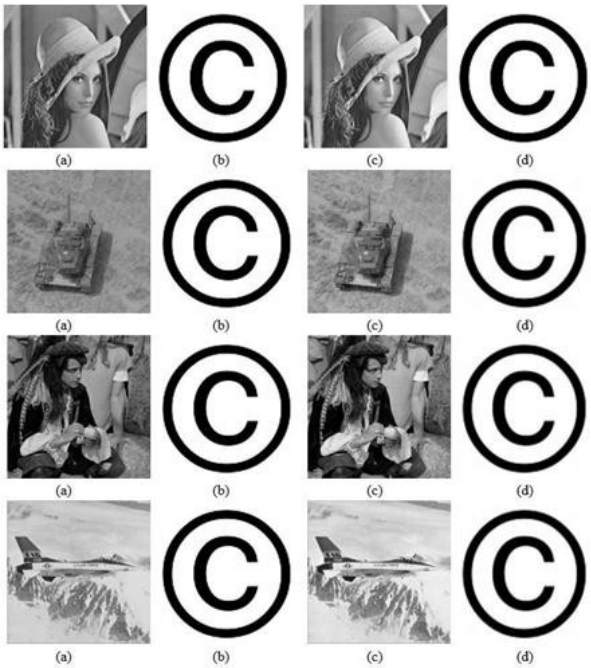

Fig. 5. A variety of attacks can be embedded and extracted using SVD without the use of the ARS optimization. One that provides protection, or a cover. Marker of Depth (b) Marked with a watermark (c), Images with watermarks that have been extracted (d)

6. Conclusion

The watermarking embedding and extraction method is described in this chapter using a novel hybrid SVD with ARS

optimization. Improved stealth and resistance to geometric and non-geometric attacks were the goals was proposed that a hybrid method be used, one that incorporated aspects of RDWT, DCT, and SVD. Moreover, an ARS -based optimization technique for optimum ESF's was developed, which improved RAI over the non-optimized condition, thereby addressing the issues related to constraints in ESF's. Visual analysis and qualitative evaluation show that the proposed BIW uses SVD with ARS optimization to achieve higher RAI than existing BIW techniques from the literature.

When compared to SVD with ARS and SVD without ARS, the performance of the SSIM index is increased by 1.356%, the NCC performance is increased by 1.089 percentage points, and the PSNR performance is increased by 1.91%. Moreover, bio-optimization algorithms are used to optimize the computational complexity of deep learning-based approaches by means of optimal feature selection. Furthermore, the watermark information can be embedded and extracted from the video using hybrid transforms without degrading the quality of the watermark, which improves the watermarking imperceptibility in comparison to the approaches presented in the literature.

References

[1] Z. Dai, C. Lian, Z. He, H. Jiang and Y. Wang, "A Novel Hybrid Reversible-Zero Watermarking Scheme to Protect Medical Image," in IEEE Access, vol. 10, pp. 58005- 58016, 2022.

[2] W. Huan, S. Li, Z. Qian and X. Zhang, "Exploring Stable Coefficients on Joint Sub-Bands for Robust Video Watermarking in DT CWT Domain," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 4, pp. 1955-1965, April 2022.

[3] M. Asikuzzaman, H. Mareen, N. Moustafa, K. -K. R. Choo and M. R. Pickering, "Blind Camcording-Resistant Video Watermarking in the DTCWT and SVD Domain," in IEEE Access, vol. 10, pp. 15681-15698, 2022.

[4] R. Karmakar, S. S. Jana and S. Chattopadhyay, "A Cellular Automata Guided Finite-State-Machine Watermarking Strategy for IP Protection of Sequential Circuits," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 2, pp. 806-823, 1 April-June 2022.

[5] B. Wang, S. Jiawei, W. Wang and P. Zhao, "Image Copyright Protection Based on Blockchain and Zero- Watermark," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 4, pp. 2188-2199, 1 July-Aug. 2022.

[6] W. Ding, Y. Ming, Z. Cao and C. -T. Lin, "A Generalized Deep Neural Network Approach for Digital Watermarking Analysis," in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 6, no. 3, pp. 613-627, June 2022.

[7] X. Zhong, P. -C. Huang, S. Mastorakis and F. Y. Shih, "An Automated and Robust Image Watermarking Scheme Based on Deep Neural Networks," in IEEE Transactions on Multimedia, vol. 23, pp. 1951-1961, 2021.

[8] F. Peng, Z. -X. Lin, X. Zhang and M. Long, "A Semi- Fragile Reversible Watermarking for Authenticating 2D Engineering Graphics Based on Improved Region Nesting," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 1, pp. 411-424, Jan. 2021.

[9] Kamili, N. N. Hurrah, S. A. Parah, G. M. Bhat and K. Muhammad, "DWFCAT: Dual Watermarking Framework for Industrial Image Authentication and Tamper Localization," in IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5108-5117, July 2021.

[10] J. Zhao, T. Zong, Y. Xiang, L. Gao, W. Zhou and G. Beliakov, "Desynchronization Attacks Resilient Watermarking Method Based on Frequency Singular Value Coefficient Modification," in IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 29, pp. 2282-2295, 2021.

[11] R. M. G. Ferrari and A. M. H. Teixeira, "A Switching Multiplicative Watermarking Scheme for Detection of Stealthy Cyber-Attacks," in IEEE Transactions on Automatic Control, vol. 66, no. 6, pp. 2558-2573, June 2021.

[12] W. H. Alshoura, Z. Zainol, J. S. Teh, M. Alawida and A. Alabdulatif, "Hybrid SVD-Based Image Watermarking Schemes: A Review," in IEEE Access, vol. 9, pp. 32931- 32968, 2021.

[13] H. -T. Hu, H. -H. Chou and T. -T. Lee, "Robust Blind Speech Watermarking via FFT-Based Perceptual Vector Norm Modulation with Frame Self-Synchronization," in IEEE Access, vol. 9, pp. 9916-9925, 2021.

[14] K. M. Hosny, M. M. Darwish and M. M. Fouda, "Robust Color Images Watermarking Using New Fractional-Order Exponent Moments," in IEEE Access, vol. 9, pp. 47425- 47435, 2021.

[15] F. Peng, B. Long and M. Long, "A General Region Nesting-Based Semi-Fragile Reversible Watermarking for Authenticating 3D Mesh Models," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 11, pp. 4538-4553, Nov. 2021.

[16] H. Ding et al., "A Compressed-Domain Robust Video Watermarking Against Recompression Attack," in IEEE Access, vol. 9, pp. 35324-35337, 2021.

[17] K. Sehra et al., "Robust and Secure Digital Image Watermarking Technique Using Arnold Transform and Memristive Chaotic Oscillators," in IEEE Access, vol. 9, pp. 72465-72483, 2021.

[18] H. Fang et al., "Deep Template-Based Watermarking," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 31, no. 4, pp. 1436-1451, April 2021.

[19] G. Tong, Z. Liang, F. Xiao and N. Xiong, "A Residual Chaotic System for Image Security and Digital Video Watermarking," in IEEE Access, vol. 9, pp. 121154- 121166, 2021.

[20] L. -Y. Hsu and H. -T. Hu, "QDCT-Based Blind Color Image Watermarking with Aid of GWO and DnCNN for Performance Improvement," in IEEE Access, vol. 9, pp. 155138-155152, 2021.

[21] K. M. Hosny, M. M. Darwish and M. M. Fouda, "New Color Image Zero-Watermarking Using Orthogonal Multi- Channel Fractional-Order Legendre-Fourier Moments," in IEEE Access, vol. 9, pp. 91209-91219, 2021.