Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1051

ORIGINAL RESEARCH ARTICLE

An effective application of watermarking techniques in the transform domain for content authentication

Sunil Kumar Vishwakarma[1,*], Birendra Kumar Sharma[2], Syed Qamar Abbas[3]

[1] *Department of Computer Science & Engineering, APJ AKTU, Lucknow 226031, India*

[2] *Department of Computer Application, Ajay Kumar Garg Engineering College, Ghaziabad 201009, India*

[3] *Department of Computer Science & Engineering, AIMT, Lucknow 226301, India*

*** Corresponding author:** Sunil Kumar Vishwakarma, sunilvishwakarma83@gmail.com

ABSTRACT

Internet media consumption, especially in the forms of audio and video, has become ubiquitous in modern life. Multimedia signals, data alterations, and backup copies are all more likely to occur with digital data. This creates a security risk in digital systems, making sensitive data vulnerable. Due to security flaws, it is now a danger in the realm of digital technology. The most difficult issues to solve in the digital age are authentication and copyright protection. The use of digital watermarking to secure online content is an exciting development. Watermarking is a technique wherein an organization's logo or ownership information is permanently embedded into the original data without degrading the quality of the data itself. With the right decoding method, a watermark can be recovered from the host image while remaining imperceptible to the human eye. By dispersing the embedded data throughout the original image, the watermarking is made more secure. The watermarked image is also treated by combining the red and green planes using inverse DWT. The watermark can be retrieved thanks to an extraction technique that is the inverse of the one used to embed it. Known as a non-blind watermarking technology, the suggested detector is given access to all information collected by the encoder. The method is vulnerable to image degradation when confronted with Salt & Pepper noise or Gamma noise.

Keywords: DWT; SVD; watermarking; NC; PSNR

ARTICLE INFO

Received: 27 July 2023
Accepted: 8 October 2023
Available online: 6 August 2024

1. Introduction

Over the past few decades, digital technology has played a crucial role in the dissemination of information. Most transactions involving digital media or data are handled via the Internet. As the internet continues to expand, more and more industries are turning to electronic publishing methods, such as e-marketing, e-library, e-mail, e-magazine, e-newspaper, e-advertising, e-ticket booking, online audio, online video, online transactions, real-time broadcasting, and so on [1]. The ability to store data digitally, compress it, edit it, transfer it, and disperse it via the internet are all ways in which digital technology has improved our lives. However, the company's owners are concerned about issues like the unauthorized duplication of audio and video signals. It's not hard to create pirated content.

The information is simply copied and pasted from one location to another. The creators have the power to safeguard their own work from any dangers. Today's threats in digital technology stem from inadequate data encryption. Multimedia applications are starting to pay more attention to authentication and copyright protection. When

it comes to online authentication, watermarking is an insecure method at best[2]. Multimedia transmissions must have a digital signature or watermark placed in them to offer proof of authentication and prevent unauthorized duplication. The term "digital watermarking" describes this process. Original data like music, image, and video may be protected from unauthorized modification by including a firm logo or symbol within the material without degrading the data's quality.

The watermark can survive attacks like cropping, histogram equalisation, and De-gamma in the extraction process by simply being detected in the host image or video. Watermarking is widely utilised in a variety of industries, including digital photography, broadcast monitoring, e-commerce, and content verification. DRM, or digital rights management, is a set of procedures that allows for the licencing of digital media files. DRM relies heavily on two technologies: encryption and watermarking[3].

Copyright protection requires a few things of the watermarking algorithm. Capacity, robustness, and stealth are the three pillars upon which watermark specifications are built depicted in **Figure 1**. The quantity of information added to the host image depends on the capacity of the watermark. The robustness feature protects images from manipulation[4]. The degree of opacity is determined by the alpha value, which also specifies the watermark image's intensity levels.

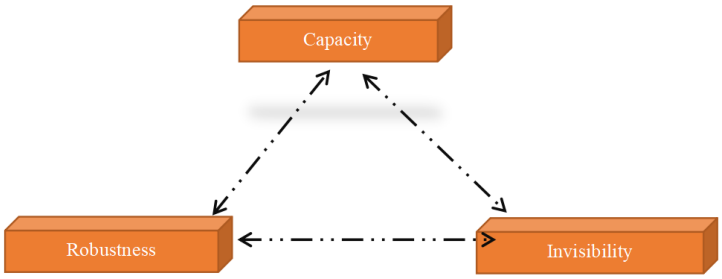

Figure 1. Magic triangle for watermarking requirements.

Several strategies are used to categorize the watermarking system based on its application. There are two main categories for this condition: those who are blind and those who are not. Blind techniques do not require any input information during the extraction process, but non-blind techniques do require a host picture, watermark image, and a key[5].

Multiple authorized copies of a document are distributed by its owner. For verification purposes, we use source-based watermarking. Using this procedure, you can determine if the document has been altered in any way. Using this technique, a unique watermark is transmitted to each recipient[6]. Using this strategy, the document is less likely to be illegally resold.

When a picture is watermarked, the watermark image is superimposed over the original, and may be seen by the naked eye. Watermarking that is invisible to the naked eye is commonly used to include secret information. It's also divided into two categories, robust and subtle, for example. Because of its durability, frequency domain watermarking is the most crucial method. It is often referred to as watermarking in the transform domain[7]. The frequencies of several of the image's components have been changed from their original values. Spectral coefficients are more accurate in representing the HVS's unique properties. In order to achieve this, the watermark will be encoded into the image's spectral coefficients.

In the fields of image processing, watermarking, and compression, the wavelet transform is a common tool. There are two primary types of wavelet transforms, the continuous wavelet transform (CWT) and the discrete wavelet transform (DWT)[8]. DWT can analyze signals in the time domain at many resolutions. This means the spatial frequency analysis is quite good. It provides time resolution that improves with lower frequencies and frequency resolution that improves with higher frequencies. Images and videos that have short bursts of high quality and longer bursts of low-resolution work well with this technique. Improving the trade-

off between watermarking's robustness, perception, and capacity is a major task. In comparison to DCT, wavelet transform has a deeper comprehension of HVS.

2. Existing work done

Numerous strategies were offered to realize a successful watermarking system in accordance with the investigators' in-depth understanding of spatial domain watermarking systems. The idea of watermarking was developed by authors, and the watermark itself consists of a pixel reformat[9]. Histogram equalization and Salt & Pepper attacks are resistant to this strategy, however resizing, geometrical, and cropping attacks are not.

The watermark's most significant bit (MSB) is spatially embedded into the host image's least significant bit (LSB). They reasoned that if the alpha factor was raised, the original image's visual quality would decrease and vice versa. The authors authenticated their work by including the Halal Logo in the watermark. A quick response (QR) code was created in order to insert the watermark within the message[10]. They elaborated on how minor adjustments can have significant effects on the perceived quality of an image. For spatial domain watermarking, they separated the pixels into MSB and LSB. The results of the PSNR, MSE, and NC measurements have been tallied. With this method, we get an MSE of 0.47 and an NC of 0.8 although the quality of the resulting images is reduced by 50%[11].

In this technique, researchers insert a smaller object into a larger one several times. If many watermarks were to be destroyed in an attack, the survival of even one would be considered a victory. While LSB substitution is straightforward, it does come with a number of downsides[12]. It may be able to deal with alterations like cropping, but the watermark will likely be lost in the face of additive noise or lossy compression. The method locates the watermark, which can be altered by a third party. The PN number generator allows for LSB replacement, which is necessary for a high-performing system[13]. The watermark was encoded using a seed-key. Because of this, the watermark is more secure and protected from being observed by third people. There would be minimal visual change to the cover art if seed-key watermarking were not applied everywhere. The LSB adaptation proves to be a straightforward and authentically potent stenographic instrument. However, it is not as sturdy as watermarking applications need it to be. The solution for image watermarking was developed by researchers and is generated via LSB insertion[14]. They gave two separate keys, such as a Stego key and an encryption key, to ensure the security of the data. All of the necessary watermark bits have been successfully inserted at all of the image's pixels, at a rate of 4.02 bits per picture element.

The patent security method and attack characterization were both praised by the writers. In this case, we use Direct Sequence Spread Spectrum (DSSS) to insert data into the image. Using JPEG compression and Gaussian noise, the author explained the robustness of the watermark data[15]. For the sake of official document security, it was determined that digital images should be watermarked using a transform domain watermarking procedure that makes use of a well-known transform, namely DCT. They used DCT by first cutting the image into 8 × 8 squares, and then changing the frequency coefficient using a spread spectrum sequence to convey their message[16]. In the intended procedure, they assume responsibility for assessing potential outcomes. They looked into the JPEG compression and Gaussian noise assaults processes and found flaws in other attacks that prevented them from reaching their goals.

Researchers developed a fractal encoding method and DCT digital watermarking algorithm to enhance the performance of the standard DCT approach. As the first layer of encryption, fractal encoding is used to encode the image, and then the encoded parameters are employed in the DCT method[17]. The PSNR is significantly enhanced using this strategy. Zernike moment (ZM) analysis is applied to global/local watermarking by the authors. For cropping, rotation, photometric, and geometric attacks, PSNR is used to evaluate image quality.

Compressed video watermarking was simplified using bit-by-bit processing by the authors. The

watermark bits in this approach are embedded in a pseudo-random number generator[18–20]. To prevent further embedding in the low frequency coefficients, the Y-frame is chosen, and the watermark bits are placed into the DCT coefficients.

A new approach to copyright protection employing a blind watermarking methodology was proposed by researchers. The LL coefficients are altered using a wavelet transform, and the watermark bits are placed in there. Each subband's blocks are then applied to the host image with the updated SVD coefficient. Support Vector Regression (SVR) was used for training, and the obtained original coefficients are used in the extraction procedure[21].

To make SVD-based watermarking techniques more secure and scalable, the authors proposed two improvements. According to the first suggestion, the quality of the image would degrade less noticeably if the coefficients of 'U' were modified in the column rather than the row. adjusting coefficients in the row vector of 'VT' would result in less noticeable degradation than adjusting the column vectors, as highlighted by the second proposal[22]. They implemented these suggestions and analyzed their impact on concealment and strength. In order to integrate the watermark, the author has chosen not one, but two planes: the 'U' plane and the 'V' plane.

A ripplet-II transform was proposed by the investigators, and it is robust against rotation attacks. A cost function of perceptual transparency is first formulated in the ripplet-II domain, and then the ridge regularization constraint is applied to the cost function to get rid of the singularity issue in the suggested method. space-time coding in colour images was proposed by the authors to reduce visual distortion and make them resistant to a wide range of attacks.

3. The objective of the research work

The current study focuses on exploring several methods for addressing the aforementioned difficulties.

To verify data ownership with low-overhead watermarking methods employing DWT-SVD for multimedia signals

4. The proposed work

In this study, we present a method for the efficient embedding and extraction of watermarks from picture and video signals. Several types of attacks, including geometrical attacks, filtering attacks, and Gaussian noises, are used to test the watermark's robustness.

The PSNR and the NC are used to measure the efficiency of the watermarking system. The host/watermark images must have a single value of 'S' for the suggested detection system to work. The 'S' can be an alpha factor or an intensity factor. Non-blind watermarking is another name for this method. The suggested system uses a pipeline design to separate the input image into rows and columns so that L and H bands can be extracted. In the next paragraphs, we detail the entire procedure for embedding and extracting.

The pepper picture that served as the host was watermarked. Because these photographs have been used for verifying assaults, they are uncompressed raw images (PNG format). This section describes in greater detail how DWT and SVD transforms are used in the watermark embedding process depicted in **Figure 2**. Input host is a coloured photo, whereas the watermark is a grayscale photo used for ownership verification.

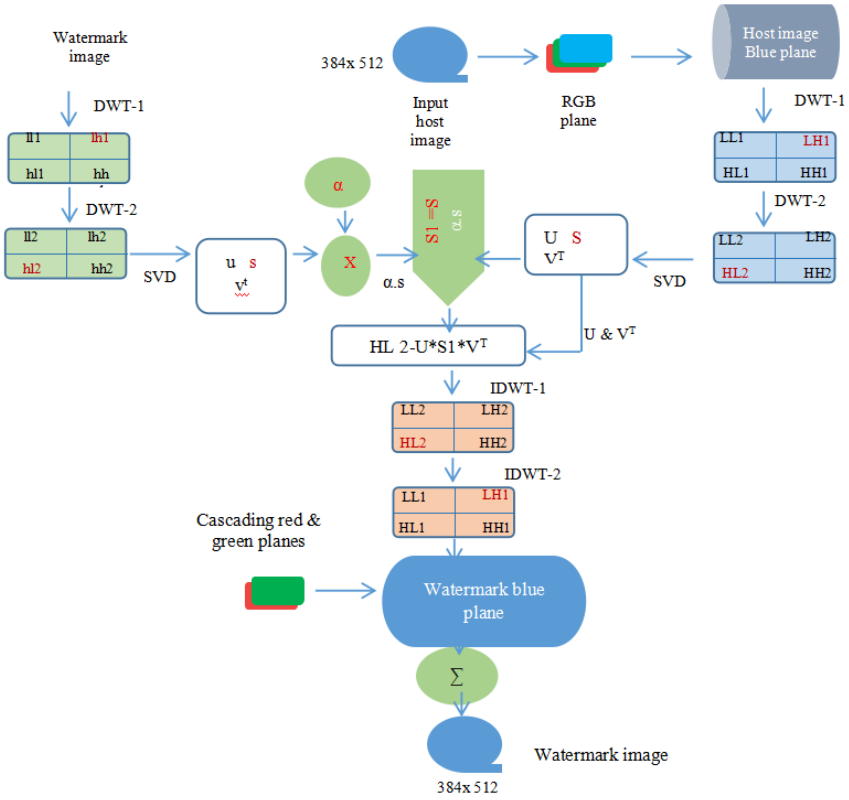

Figure 2. Architecture of proposed image watermark embedded process.

4.1. Embedding process

1) The host image is decomposed into the RGB colour space, and the blue channel is then chosen for embedding.

2) Four sub-bands (LL1, LH1, HL1, and HH1) are created when I-level DWT is performed on the blue plane.

3) To get LL2, LH2, HL2, and HH2, a DWT of level II is applied to the blue plane's LH1 sub-band.

4) After applying the SVD transform, the HL2 sub-band breaks down into the terms in the equation.

$$HV = ASV^{T} \quad (1)$$

5) Decomposing the watermark image requires applying steps 1–4, and embedding requires choosing a single value.

6) Before embedding, a mathematical analysis in matrix format has been performed, and the watermark picture has been scaled to match the size of the host image.

7) The singular value of the watermark picture s is multiplied by a scaling factor set to 0.443.

8) The singular value of the host image S is calculated by adding the modified singular value of the watermark (x s) to the singular value of the host image S.

$$S1 = S + (\propto \times s) \quad (2)$$

9) Orthogonal elements have been combined to recreate HL2. The host image's U and V are provided by

$$HL2 = U \times S1 \times V \quad (3)$$

10) To reconstruct the LH1 sub-band from the LL2, LH2, and HH2 bands, an Inverse Discrete Wavelet Transform (I Inverse DWT) is applied to HL2.

11) The 384 × 512 watermarked image is created by extracting the LL1, LH1, HL1, and HH1 sub-bands and applying II level IDWT to recreate the blue plane.

4.2. Extraction process

The logo or symbol embedded in the data can be used as proof of ownership if the data can be extracted from its watermark. The detection method proposed for image watermark extraction is depicted in **Figure 3**. In this section, we break out the detection procedure in detail.

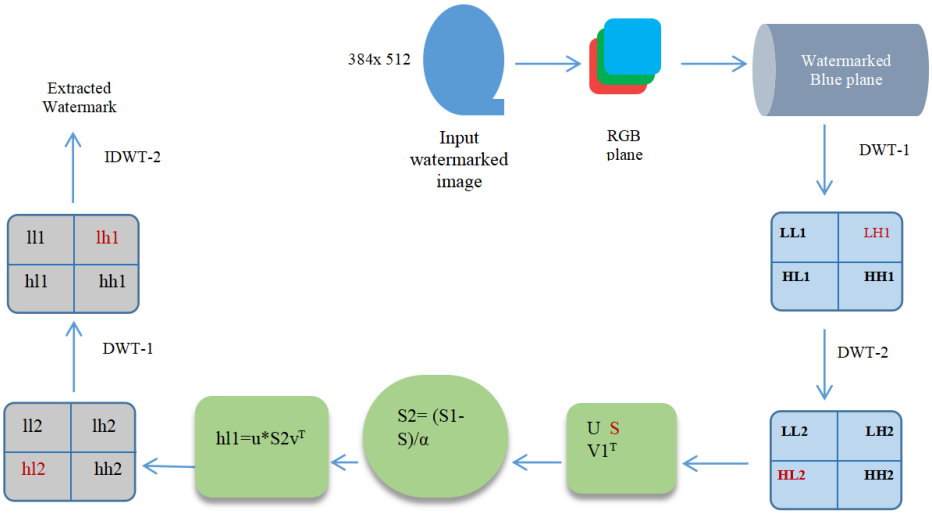

Figure 3. Architecture of proposed image watermark extraction process.

1) A watermarked image is composed of red, green, and blue layers.

2) The blue plane is subjected to a DWT of level I, yielding the four sub-bands LL1, LH1, HL1, and HH1.

3) When the LH1 sub-band of the blue plane is subjected to DWT at level II, the resulting sub-bands are LL2, LH2, HL2, and HH2.

4) When the SVD transform is applied to the HL2 sub-band, it is broken down into its constituent parts. U1 S1 V1T

5) Using the below formula, we can calculate the watermarked image's singular values.

$$s2 = \frac{S1 - s}{\propto} \tag{4}$$

6) The equation hl1 = u × S2 × v^T (3.5) describes the reconstructed sub-band hl1 of the watermark picture, which was created by combining the orthogonal elements u and 'v'

$$h11 = u \times S2 \times v^T \tag{5}$$

7) To reconstruct hl2, we first extract the ll1, lh1, and hh1 sub-bands, and then apply the inverse DWT at the I level to the lh1 sub-band.

8) Reconstructing the watermark image from the ll2, lh2, hl2, and hh sub-bands requires applying an inverse IDWT of level II.

5. Result and discussion

5.1. Peak to signal ratio

The PSNR of an image is a defining parameter since it allows for the analysis of the interference of noisy components. The human visual system can also be calibrated using PSNR. A decibel (dB) is the unit of measurement. The lower the PSNR number, the more lossy information is preserved in the image. Mean squared error (MSE) between the unaltered and watermarked image is the basis for determining PSNR.

$$\text{PSNR} = 10.\log_{10}\frac{\text{Max}_i}{\sqrt{\text{MSE}}} \tag{6}$$

Mean squared error, where Max_i is the highest intensity value that can be found in the image, and MSE is the standard deviation. Image *X.Y* is the original, image *B* is the noise-free version, and image *b* is the noisy approximation of *X.Y*. The mean squared error (MSE) is defined mathematically as:

$$\mathrm{MSE} = \frac{1}{\mathrm{XY}} \sum_{i=0}^{\mathrm{X}-1} \sum_{j=0}^{\mathrm{Y}-1} [B(i,j) - b(i,j)]^2 \tag{7}$$

5.2. Normalized correlation (NC)

This parameter is used to measure the similarity between the extracted watermark and the original watermark image. In ideal condition the NC will be unity and if NC is less than 1, the resultant image will appear with noise.

$$\mathrm{NC} = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} (A_{i,j} - \hat{A})(B_{i,j} - \hat{B})}{\sqrt{\sum_{i=1}^{m} \sum_{j=1}^{n} (A_{i,j} - \hat{A})^2 \; \sum_{i=1}^{m} \sum_{j=1}^{n} (B_{i,j} - \hat{B})^2}} \tag{8}$$

In **Table 1**, we can see that DWT at three different settings yields different PSNR values for the watermarked image and the extracted watermark.

Table 1. Analysis for selection of II level DWT decomposition.

S. No.	Decomposition level	PSNR in dB	
		Watermarked image	**Extracted watermark after JPEG compression**
1	Level I	43.95	32.15
2	Level II	44.57	32.06
3	Level III	44.38	32.25

PSNR values at three DWT decomposition levels are displayed in **Figure 4**. The values show that the II level decomposition is superior to the I level decomposition in terms of output. However, there is no noticeable performance boost at the III level of decomposition. The PSNR of the extracted watermark after JPEG compression is displayed in **Figure 4**. It is plain to see that, between levels II and III, there is no appreciable change in the PSNR of the extracted watermark. As a result, the calculation cost for implementation is reduced by fixing the DWT level at the II level for the subsequent embedding procedure.

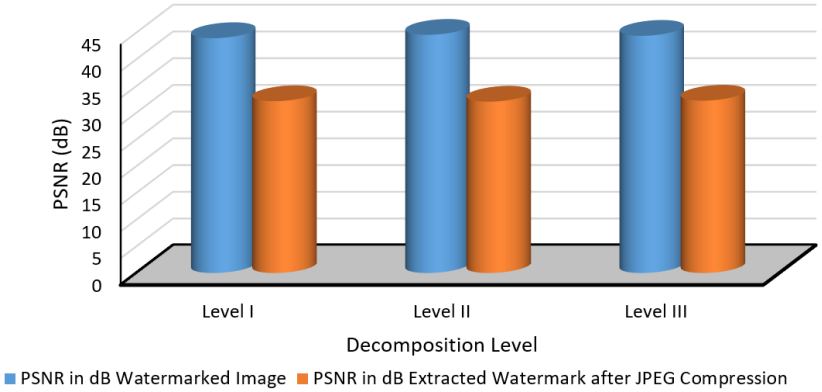

Figure 4. Analysis for selection of II level DWT decomposition.

The PSNR of the watermarked image and the extracted watermark, both compressed using JPEG, are displayed in **Figure 5** for the various SVD planes. Based on the PSNR values of 32.09 dB for the watermarked version and 44.05 dB for the extracted version (**Table 2**), it can be concluded that the plane 'S' (singular values) is appropriate for embedding watermark. Watermark embedding is not a good fit for the orthogonal 'U' and 'V' components.

Table 2. Analysis of watermarking in SVD components.

S. No.	Decomposition level	PSNR in dB	
		Watermarked image	**Extracted watermark after JPEG compression**
1	U	47.59	−3.049
2	S	44.89	33.18
3	V	47.34	−8.19

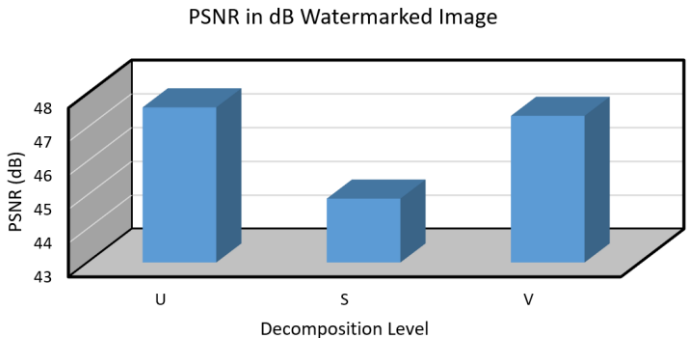

Figure 5. Analysis of watermarked image PSNR in SVD components.

Figure 6 presents the PSNR comparison of SVD components for different decomposition levels.

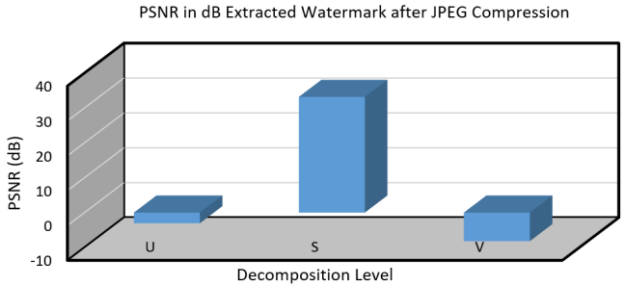

Figure 6. Analysis of watermarked image PSNR in SVD components.

Therefore, protecting multimedia assets is a challenging task. Watermarking is a digital authentication and copy protection technique that can be used to track down illegal copies of media. To help curious minds understand as much as they can about digital watermarking, the authors of this paper present a detailed algorithm for the process. This study explains the watermarking technique for embedding and extracting visual information using the proposed detection method. PSNR and NC are used to evaluate the quality of the raw images, and a parametric search is used to test out different singular values, colour planes, and intensity values.

6. Conclusion

This information may now be transmitted in an understandable format, which is yet another advantage of the modern means of communication made possible by the rapid expansion of technological capability and the demand for multimedia service delivery. Digital content during data exchange makes use of being easily updated and copied. Therefore, safeguarding multimedia files is a difficult undertaking. Watermarking is a form of digital copy protection and authentication technology that can be used to identify and locate pirated copies of content. This study provides a comprehensive algorithm for digital watermarking, which should enable creative researchers learn as much as possible about the topic. Using the proposed detection method, this research details the watermarking approach for embedding and extracting visual signals. Raw image performance is evaluated using PSNR and NC, and parameters such as singular values, colour planes, and intensity values are explored via a parametric search. II level DWT-SVD uses a novel method to watermark embedding algorithm to generate a secure watermark. The proposed detection system cannot read the

watermark without the full set of data from the encoder.

Author contributions

Conceptualization, SKV; methodology, SKV; validation, SQA; formal analysis, BKS and SQA; investigation, BKS, SKV and SQA; resources, SQA; data curation, SKV; writing—original draft preparation, SKV and BKS; writing—review and editing, SKV and BKS; visualization, SKV and BKS; supervision, SKV, BKS and SQA. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Jadhav AA, Babar RV, Gaikwad MS. Hardware implementation of digital watermarking system for real time captured image transmitting. 2015 International Conference on Pervasive Computing (ICPC). Published online January 2015. doi: 10.1109/pervasive.2015.7087148
2. Shanmugam M, Chokkalingam A. Performance analysis of 2 level DWT-SVD based non blind and blind video watermarking using range conversion method. Microsystem Technologies. 2018, 24(12): 4757-4765. doi: 10.1007/s00542-018-3870-x
3. Joshi AM, Mishra V, Patrikar RM. FPGA prototyping of video watermarking for ownership verification based on H.264/AVC. Multimedia Tools and Applications. 2015, 75(6): 3121-3144. doi: 10.1007/s11042-014-2426-z
4. Rajkumar VF. Entropy based Robust Watermarking Scheme using HADAMARD Transformation Technique. International Journal of Computer Applications. 2011, 12(9): 14-21. doi: 10.5120/1712-2293
5. Garimella A, Satyanarayan MVVK, Murugesh PS, Niranjan UC. VLSI Implementation of Online Digital Watermarking Techniques with Difference Encoding for the 8-bit Gray Scale Images'. In: Proceedings of the IEEE International Conference on VLSI Design; 2003. pp. 283-288.
6. Roy V, Shukla S. Effective EEG Motion Artifacts Elimination Based on Comparative Interpolation Analysis. Wireless Personal Communications. 2017, 97(4): 6441-6451. doi: 10.1007/s11277-017-4846-3
7. Shahdoosti HR, Salehi M. Transform-based watermarking algorithm maintaining perceptual transparency. IET Image Processing. 2018, 12(5): 751-759. doi: 10.1049/iet-ipr.2017.0898
8. Makbol NM, Khoo BE, Rassem TH. Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. IET Image Processing. 2016, 10(1): 34-52. doi: 10.1049/iet-ipr.2014.0965
9. Narwade NS, Deshmane NP, Elchatwar P, Pande PL. Robust watermarking for Geometric Attacks using DFT. International Journal of Emerging Trends and Technology in Computer Science. 2013, 2(2): 20-25.
10. Mohanarathinam A, Kamalraj S, Prasanna Venkatesan GKD, et al. Digital watermarking techniques for image security: a review. Journal of Ambient Intelligence and Humanized Computing. 2019, 11(8): 3221-3229. doi: 10.1007/s12652-019-01500-1
11. Kumar S, Gupta U, Singh AK, et al. Artificial Intelligence. Journal of Computers, Mechanical and Management. 2023, 2(3): 31-42. doi: 10.57159/gadl.jcmm.2.3.23064
12. Liu X, Li F, Wen B, et al. Removing Backdoor-Based Watermarks in Neural Networks with Limited Data. 2020 25th International Conference on Pattern Recognition (ICPR). Published online January 10, 2021. doi: 10.1109/icpr48806.2021.9412684
13. Lee YS, Seo YH, Kim DW. Blind Image Watermarking Based on Adaptive Data Spreading in n-Level DWT Subbands. Security and Communication Networks. 2019, 2019: 1-11. doi: 10.1155/2019/8357251
14. Li C, Zhang Z, Wang Y, et al. Dither modulation of significant amplitude difference for wavelet based robust watermarking. Neurocomputing. 2015, 166: 404-415. doi: 10.1016/j.neucom.2015.03.039
15. Roy V. An Improved Image Encryption Consuming Fusion Transmutation and Edge Operator. Journal of Cybersecurity and Information Management. 2021, 8(1): 42-52. doi: 10.54216/jcim.080105
16. Kandi H, Mishra D, Gorthi SRKS. Exploring the learning capabilities of convolutional neural networks for robust image watermarking. Computers & Security. 2017, 65: 247-268. doi: 10.1016/j.cose.2016.11.016
17. Kumar S. Reviewing Software Testing Models and Optimization Techniques: An Analysis of Efficiency and Advancement Needs. Journal of Computers, Mechanical and Management. 2023, 2(1): 32-46. doi: 10.57159/gadl.jcmm.2.1.23041
18. Naranjo-Torres J, Mora M, Hernández-García R, et al. A Review of Convolutional Neural Network Applied to Fruit Image Processing. Applied Sciences. 2020, 10(10): 3443. doi: 10.3390/app10103443
19. Shukla S, Roy V, Prakash A. Wavelet Based Empirical Approach to Mitigate the Effect of Motion Artifacts from EEG Signal. 2020 IEEE 9th International Conference on Communication Systems and Network Technologies

(CSNT). Published online April 2020. doi: 10.1109/csnt48778.2020.9115761
20. Senan EM, Alzahrani A, Alzahrani MY, et al. Automated Diagnosis of Chest X-Ray for Early Detection of COVID-19 Disease. Hemanth J, ed. Computational and Mathematical Methods in Medicine. 2021, 2021: 1-10. doi: 10.1155/2021/6919483
21. Dhillon A, Verma GK. Convolutional neural network: a review of models, methodologies and applications to object detection. Progress in Artificial Intelligence. 2019, 9(2): 85-112. doi: 10.1007/s13748-019-00203-0
22. Alzahrani A. Enhanced Invisibility and Robustness of Digital Image Watermarking Based on DWT-SVD. Algalil FA, ed. Applied Bionics and Biomechanics. 2022, 2022: 1-13. doi: 10.1155/2022/5271600