IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 41, No. 5, October, 2024, pp. 2297-2315
Journal homepage: http://iieta.org/journals/ts

Enhanced Security and Robustness in Color Image Watermarking Using DWT-HD and Quaternion SVD under Hybrid Attacks

Arun Kumar Patel*, Prabhat Patel

Department of ECE, UIT, RGPV, Bhopal 462033, India

Corresponding Author Email: arun_patel10@yahoo.com

https://doi.org/10.18280/ts.410507

Received: 29 November 2023
Revised: 15 February 2024
Accepted: 29 March 2024
Available online: 31 October 2024

Keywords:
encryption, Color Image Watermarking (CIW), dual-key security, Heisenberg Decomposition (HD), Discrete Wavelet Transform (DWT), Quaternion Singular Value Decomposition (QSVD), hybrid attacks, Normalized Correlation (NC), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM)

ABSTRACT

Securing color images through watermarking presents significant challenges, particularly when subjected to complex hybrid attacks. The objective of this study is to enhance both the security and robustness of Color Image Watermarking (CIW) by developing a novel method that integrates Discrete Wavelet Transform (DWT) and Quaternion Singular Value Decomposition (QSVD) with Heisenberg Decomposition (HD). This combined approach, referred to as DWT-QSVD-HD, has been tested rigorously under various hybrid attack scenarios. The method employs a dual-key strategy, utilizing a logo watermark and the HH component of the R-level DWT, to enhance robustness. A modified watermark insertion rule is proposed, leveraging both keys simultaneously within the HD-QSVD domain, which significantly complicates unauthorized decoding efforts. The LAB color space is utilized during the pre-processing stage to maximize entropy, with entropy analysis providing justification for this adaptation. To further bolster security, the watermarked image is encrypted using a simplified fast AES algorithm, adding an additional layer of protection and improving the watermark's resilience. The performance of the proposed method is evaluated against existing techniques using parametric analysis, optimized via the Fruit Fly Optimization Algorithm (FOA) for key metrics such as Normalized Correlation (NC), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Measure (SSIM). The method demonstrates exceptional performance across various image sizes, maintaining an NC above 0.995 for 64×64 images. Notably, under motion blur attacks, the proposed method improves the NC from 0.8322 to 0.9003 for 256×256 images. The impact of individual and hybrid watermark attacks is systematically assessed, with results showing superior extraction and recovery of image quality when using the proposed technique.

1. INTRODUCTION

The global proliferation of imaging data, particularly during the COVID-19 pandemic, has underscored the critical need for robust and secure techniques to protect and authenticate color imaging databases. The massive volumes of color imaging data captured daily, particularly for patient documentation and authentication, demand the development of a universal standard for image data protection solutions. Watermarking has emerged as a vital method for safeguarding copyright and ensuring the authenticity of color imaging data. Key requirements for effective watermarking include robustness against various attacks, invisibility of the watermark, and efficient recovery of the embedded data.

Recent observations have highlighted that watermark images are increasingly subjected to multiple hybrid attacks simultaneously, necessitating an urgent evaluation and enhancement of watermarking methods under such conditions. Achieving a higher level of robustness through dual-key approaches has become a critical objective in this domain. While significant research efforts have focused on enhancing the robustness of CIW methods, there remains a need for further exploration, particularly in the context of hybrid attacks. The classification of transform based methodologies is given in the Figure 1.

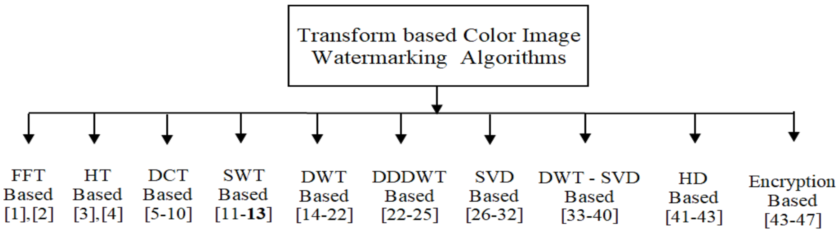


Figure 1. Classification based on transform domain approaches for CIW

Table 1. Abbreviations and nomenclatures

Abbriviations		Nomenclatures	
AES	Advanced Encryption Standard	R_{cover}	Red component of cover image
CIW	Color Image Watermarking	G_{cover}	Green component of cover image
DFT	Discrete Fourier Trasform	B_{cover}	Red component of cover image
DCT	Discrete Cosine Teasform	PHP^T	HD coeffciecnts vectors
DWT	Discrete Wavelet Trasform	Ci	Decomposed matrices of scalar values
DL	Dictionary Learning	$U_C, S_C, V_C{}^T$	SVD coeffciecnt value vectors
DHT	Hilbert Transform	R_{opt}	Adapted DWT levels
ED	Edge Detection	X_{LL}	Low pass DWT coefficient
FFT	Fast Fourier Transform	H_{sw}, S_{wk}, S_w	HD coefficient of X_{LL} component
FOA	Fruit Fly Optimization Algorithm	SVw	Scaled singular values of watermark
HD	Heisenberg Decoposition	α	SVD scaling factor
HH	High Pass- High Pass Coefficients	Sw	Decomponsed watermark sigular value
IDWT	Inverse Discrete Wavelet Arasfom	Sc	Decomposed cover image singular value
LAB	Color Space Formate	m*n	Size of the image matrix
NC	Normalized Corelation	Key(m)	Is random key matrix
PSNR	Peak Signal to Noise Ratio	Enc_{img}	Encrypted image
EGB	Red Gree Blue Space	H_{sw}^	SVD coefficient vector for Recovery
SSIM	Structure Similarity Index Measure	Sw^	Recovered SVD value
SVD	Singular Value Decomposition	NC	Normalized correlation
SWT	Stationary Wavelet Trasform	Psnr	Peak signal to noise ratio

Transformation-based watermarking strategies aim to improve the robustness and invisibility of embedded watermarks, with the latter being more effectively achieved in the transform domain. These methods are, therefore, the primary focus of this study. Early research proposed discrete Fourier transform (DFT)-based approaches [1, 2], which, despite their initial promise, were found to be susceptible to noisy attacks and prone to visual artifacts in the watermarked images. Consequently, these methods have been supplanted by Hilbert transform (HT)-based techniques [3, 4], which, although offering improved performance, are limited by their payload capacity and sensitivity to noise, making watermark extraction challenging.

Further advancements in this field have led to the exploration of discrete cosine transform (DCT) [5], stationary wavelet transform (SWT) [6], DWT [7], and double-density DWT (DD-DWT) techniques for robust image watermarking. However, these methods also exhibit vulnerabilities, particularly to geometric attacks, highlighting the need for comprehensive testing. To address these challenges, hybrid transform domain combinations are proposed, which leverage the strengths of multiple transformations. Abbreviations and nomenclature used in this work are presented in the Table 1.

One such approach is the use of a shift-invariant edge detection (ED)-based mask to enhance watermark robustness, as suggested by Tiwari and Singh [7]. The proposed HD facilitates the insertion of watermarks into specific frequency bands that are less susceptible to standard attacks such as noise and compression. In this study, a multi-level DWT is applied to decompose the host image into a series of sub-bands, with the resulting coefficients fed into the HD. The watermarking process is further strengthened by incorporating singular value decomposition (SVD).

Watermarking techniques must be resistant to the common assaults encountered in copyright protection algorithms. The field of CIW is particularly challenging, as it requires the development of watermarks that remain durable and undetected under various attack scenarios. A critical requirement of any watermarking method is the ability to preserve structural similarity following successive attacks, while maintaining the integrity of both low and high-frequency information in the cover color images. Additionally, watermark invisibility and robustness against various attacks are paramount, as is the design of algorithms that perform equally well on both color and grayscale images.

The proposed methodology combines dual-key secure image watermarking with an encryption-based approach to enhance robustness. DWT is commonly employed in hybrid combinations with SVD-based techniques to improve data integrity and protection. Recent advancements in encryption-based approaches have further contributed to the enhancement of CIW methods. A comprehensive review of CIW literature and transformation-based techniques is provided sequentially in this work, highlighting the evolution of methodologies aimed at improving watermark robustness and invisibility.

a) Research on CIW

Singh et al. [8] demonstrated that spatial domain-based watermarking methods exhibit faster processing times and can deliver comparable performance against scaling and noise attacks. However, these methods are less effective than transform domain methods when subjected to attacks such as rotation, compression, and Gaussian filtering. The findings suggest that although transform domain methods offer superior robustness, they are computationally complex. Tan et al. [9] recommended the use of the YCbCr colour space after embedding the data, although the reproduction of colour images in this space has yet to be thoroughly investigated. Chaitanya et al. [10] presented a method for CIW that utilizes the DWT-DCT-SVD domain, embedding the watermark within the blurred colour components of the RGB space, defined separately as:

$$\begin{aligned} R_{\text{cover}} &= cover\_image\ (:,:,1) \\ G_{\text{cover}} &= cover\_image\ (:,:,2) \\ B_{\text{cover}} &= \text{cov}er\_image\ (:,:,3) \end{aligned} \tag{1}$$

b) Edge-Based Methods

High-frequency attributes, such as boundaries or contours where physical lighting varies dramatically across image regions, can be identified as colour data edges. These edges contain significant information, making them a popular choice for invisible watermarking. Huang et al. [11] recently employed SWT along with ED, utilizing an adjustable embedding parameter with a peak PSNR guarantee to enhance image watermarking. In addition to integrating boundary coefficients into the HH subcarrier of SWT [12, 13], image dilation has been applied to increase robustness. However, the primary challenge of this method lies in the transparency of the watermark, which requires additional scaling. Liu et al. [14] recently proposed a hybrid combination of HD with SVD and DWT to improve watermarking robustness.

c) DWT-Based Watermarking

Previous studies [15-22] have employed L-level DWT to embed watermark logos into input images. Chaturvedi and Shukla [15] proposed an optimal DWT-based approach, visually presenting the results. Shukla et al. [16] suggested using DWT to create an effective watermarking method for medical images under rotational attacks, while Singh et al. [17] focused on selecting appropriate DWT coefficients. He and Hu [18] developed a DWT-DCT-SVD-based digital image steganography algorithm for securing images through a hybrid approach, although the DCT remains sensitive to blocking effects. Su and Chen [19] and Su [20] proposed a blind watermarking approach, utilizing column ED for robustness. Ellinas and Manolakis [21] suggested an ED-based technique that incorporates watermarked images into subgroups of decomposed DWT coefficients. The authors implemented watermark embedding by applying a contrast sensitivity function (CSF) to wavelet coefficients with respect to edge coefficients to boost exclusion. Ellinas and Manolakis also proposed an efficient wavelet-based ED watermarking method in 2008, where a Sobel ED mask was used to identify edges in a multiple DWT image. A 3x3 structured mask was employed to perform morphology dilation on the identified edge image, followed by the addition of zero-mean Gaussian noise as a watermark pattern [21]. Other methods, including least significant bit (LSB) [22], Chinese remainder theorem (CRT) [23], and multimedia watermarking [24, 25], have also been proposed.

Vidya and Sujithra [25] proposed a 3D video watermarking technique, while Lai and Tsai [26] utilized DWT-SVD for watermarking. Kadian et al. [27] introduced a modified redundant DWT-SVD (RDWT-SVD) approach. Despite the varying number of edges in each image block, several DCT-based watermarking algorithms have been referenced in the literature [28-30]. Zeng [28] proposed using zero-masking technologies to reduce blocking artefacts in DCT-coded images, while Al-Haj [29] and Abdulrahman and Ozturk [30] introduced a DWT-DCT hybrid combination for image watermarking. Ansari et al. [31] proposed a safety approach using block-based SVD for watermarking, combining DWT and spatial domains, though the method appears relatively simple. Gong et al. [32] proposed the application of intelligent ED in a robust watermarking model employing DWT permutations, while Rykaczewski [33] designed a wavelet-based system using SVD to preserve ownership. Sunesh et al. [34] developed and evaluated a watermarking technique using DWT-SVD, noting potential areas for further growth.

The primary objective of this study is to enhance the security of colour images by developing a robust and straightforward watermarking solution for the copyright protection of high-definition colour imagery data. The performance of the algorithm has been evaluated under noise, median filtering, cropping, and rotation attacks. To optimize the robustness of the watermarking process, Liu et al. proposed a more effective hybrid transformation method combining HD with the conventional DWT-SVD procedure. True colour images are often generated using various imaging modalities, with human visual perception better understanding and segmenting colour characteristics. The adaptive adoption of the LAB colour space is recommended to improve performance and robustness, with entropy expected to increase in this space.

In the current research, true colour images are converted from the RGB to the LAB colour space. The vertical axis of the CIE-LAB colour space represents L, or Lightness, with values ranging from 0 to 128. The comparison of the LAB colour space in relation to the RGB image is illustrated in Figure 2, where the L component exhibits a significantly higher visual representation and entropy, as observed in the Lena image. The Lena image is used in this study for the validation of the results obtained from existing research works.

Watermarking has broad applications in versatile imaging systems, as depicted in Figure 3. Various strategies have been developed to enhance the transparency and resilience of watermarking systems. This study aims to support lightweight security measures and evaluate performance under hybrid attacks.

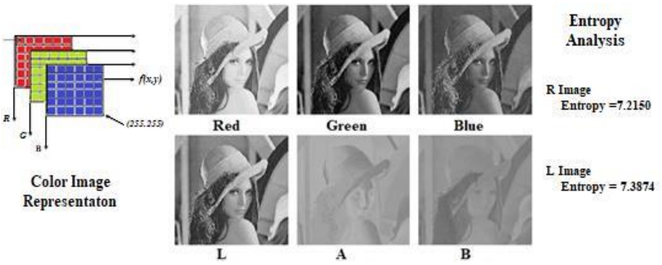


Figure 2. Image and color spaces representation

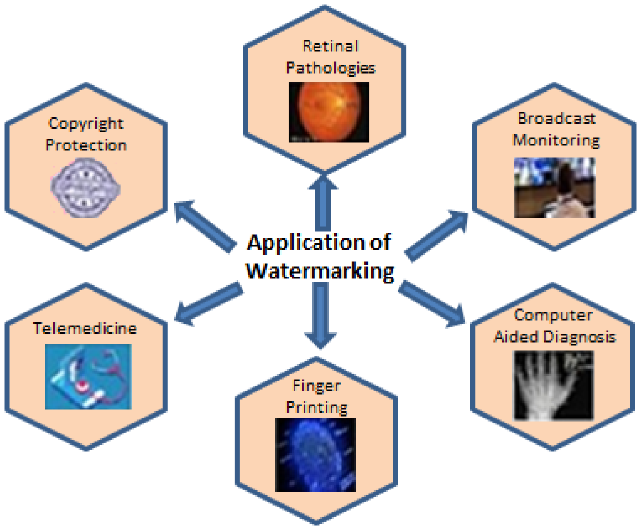


Figure 3. Wide scope of Image based watermarking uses

1.1 Contribution of work

In this paper, the major contribution is to design a robust dual-SVD key-based watermarking algorithm for authentication and protection of color images. The key problem of robustness is addressed by introducing the Q-SVD of the HH wavelet subband and a combination of HD decompositions as the DWT-QSVD-HD algorithm. The use of the HH subband maintains the invisibility of the watermark.

The primary benefit of combining the HD is to improve performance under noisy attacks. Another major contribution of the paper is to use the LAB color space with entropy for evaluating the performance under various attacks and the better recovered quality of the watermark from attacked images. To improve the security of the watermark, simplified fast AES encryption is used in combination with watermarking. Also, results are evaluated under attacks with encryption and without encryption.

The structure similarity and the correlation measures are used for comparing the performance of three DWT-based watermarking methodologies. The performance is compared with recent publications and evaluated under various attacks. For the Lena image used for validation, the FOA is used for the attack analysis. A wide range of color images are considered for the evaluation. Specific case studies of the various parameters under compression attacks, such as compression ratio, quality factor, and strengths, are evaluated to demonstrate the efficiency of the proposed method. The paper also contributed to evaluating the performance of watermark extraction and image reproduction even in the worst cases of hybrid attacks with a combination of rotation, filtering, JPEG, and noisy attacks. Three cases of hybrid attacks are considered for evaluation, and the extracted results are presented as color images. The proposed method is capable of sustaining itself even under hybrid attacks. The FOA optimization is used for the PSNR and scaling factor evaluation of attacks.

1.1.1 Key advantages

The proposed method is an advanced modification of Liu et al. [14]. The first contribution is to replace SVD with Q-SVD. This aids in robustness. Secondly, the use of LAB space offers visual quality improvement. Thirdly, security in terms of AES encryption is offered. The hybrid attack evaluation is the novelty of the work.

The remaining paper first reviews the limitations of existing transformation-based true CIW methods designed for protecting the color imaging data in Section 2. In Section 3, wavelet-based watermarking methods are briefly discussed, as are the basic ideas of DWT decomposition and its benefits, along with the numerous limitations and challenges of watermarking approaches. The concepts of color space models and SVD, as well as their attributes, are discussed in the next section. The Lab color model is proposed for watermarking in this paper since it is intended to increase the image brightness and entropy. For reconstruction, the luminance component L of LAB color space is separated, and the chroma components (A and B) are preserved separately. CIW in LAB color space demonstrates a significant advancement over the prior method [34]. Section 5 sequentially explains the proposed methodology. Finally, results of the CIW for MI and entropy analysis, as well as watermark embedding and reconstructing, are described. Section 6 discusses the quantitative evaluation based on entropy, SSIM, PSNR, and NC as parametric measures. Finally, in the next section, the paper is concluded, along with the scope of work. The performances of three watermarking methodologies are presented for evaluation.

2. RELATED WORK OF SECURE WATERMARKING

There are many image security algorithms that have been proposed in the past to fulfill the requirements. Early days of image security methods like cryptography and steganography may lead to complexity and poor visual quality of the recovered output images. Watermarking-based methods have recently gained significant popularity and have proven secure. To improve resilience, DWT-SVD-based watermarking methods are frequently used in the literature. The fundamental advantage of DWT is that it maintains invisibility, while SVD makes it difficult to erase watermarks without harming the image. Several safe image watermarking techniques were suggested in the previous studies [35-38]. Bose and Maity [35] have used singular values for selected wavelet sub-band coefficients of image data, so this research proposes an image embedding procedure for a sparse watermark. Using the Dictionary Learning (DL) technique, the watermark image is rendered sparse. But DL-based methods are complex and vulnerable to attacks. Next, a watermark decoder designed around the concept of compressed sensing (CS) is created within the context of an alternating direction method of multiplication (ADMM). Yasmeen and Uddin [36] offered multi-level operations of DWT with SVD hybrid combinations that are utilized to imbed and extract watermark features. But performance is required to be tested under hybrid attacks.

Sivananthamaitrey and Kumar [37] have proposed a watermarking method with two watermarks implanted in a color image. It is reliable and has a large embedding capacity. Using the SWT in combination with SVD decomposition, a grayscale image is used as one of the watermarks to show who owns the host image (SVD). The LSB approach is used to include a binary watermark to identify tampering, but it has low robustness. Naffouti et al. [38] have also recently used the DWT and SVD values to provide an advanced image watermarking technique in this study. The study first subjects a grayscale cover image to DWT decompositions at the sender side, and then subjects the original HH (high-high) components to Eigen decomposition. A similar procedure is carried out on a watermark image in grayscale. Next, the inverse DWT (IDWT) is used to combine two unitary and one diagonal matrix to create a digital watermarked image. They stated that DWT-SVD is efficient for invisible watermarking.

Singh and Singh [39], in their article, propose a new reliable and blind watermarking system for copyright protection based on DWT-SVD and DCT with Arnold Cat Map (ACM) encryption. Unauthorized reading and false-positive detection watermarking security issues in SVD-based methods are fixed by the suggested solution, but using the ACM map is predictable. The middle singular value of each block with a size of 4×4 of the (DWT) sub-bands of the host picture contains the DCT transform coefficients of these MSB and LSB values. However, the DWT-SVD-DCT method is computationally expensive, and errors or noise are introduced during transformations. Zear et al. [40] have studied an algorithm for multiple watermarking for healthcare applications based on DWT, DCT, and SVD. For identity authentication, the suggested solution employs three watermarks—a color Lump image watermark, a doctor's signature or identification code, and patient diagnostic data as text watermarks. Luo et al. [41] have studied DWT along with HD combined with SVD decomposition as the foundations of the unique picture watermarking technique suggested in this research. The host image is first divided into a number of sub-bands during the embedding process using multilevel DWT, and the resulting coefficients are then utilized as the input for HD. The SVD is simultaneously used to operate the watermark.

The method seems robust due to the hybrid combination, but it is simple and requires more effort.

Rajput et al. [42] have also proposed a scheme with HD and SVD with discrete wavelet modification that is used to breakdown the cover image and watermark image (DWT). Following the use of SVD, an optimal scaling factor is used to directly include each unique value of the watermark into the CI singular components. Nazir et al. [43] have researched to offer an improved and reliable watermarking technique paired with a 4D hyper-chaotic system, and we examine its performance by extending and differentiating the previous work. In this work, they contribute by using an improved algorithm to watermark and protect color images. This algorithm combines a 4D hyper-chaotic system with HD, SVD, and DWT transformations for decomposition techniques (IEFOA). The HD_SVD method offers higher capacity and improved imperceptibility.

Mannepalli et al. [44] have designed a brand-new hybrid design combining block-chain-based encryption and invisible image watermarking. ED of the DWT coefficient is used to achieve the watermarking. The L-level DWT transform is used to decompose the color image and provide multi-resolution coefficients. To produce the edge coefficients, the HH wavelet band is subjected to ED. The watermark embedding uses edge coefficients and dilation differences to increase resilience. A block-chain-based hash technique designed for color photos is used to encrypt the watermark image. Yao et al. [45] have created a new way to manage secure digital watermarking that is based on block chains and multiple bits. They suggest using a self-learning watermark embedding algorithm to add pictures and binary messages to a hidden space of pictures. The method offered resistance to a wide range of attacks (geometric transform, JPEG, noise, etc.).

Rathord and Rai [46] have proposed an improved hybrid transformation method that combines the DWT-SVD technique with the HD combination. The entropy maximization stage of pre-processing adapts the LAB color space. The entropy analysis is the basis for the color space adaptation. We use parametric analysis of NC, PSNR, and SSIM to check how well the suggested and existing methods work on color images. The effectiveness of current watermarking techniques may be compromised by numerous assaults. Sahila and Thomas [47] have proposed prohibiting illegal access to multimedia data like audio, video, and photos; digital watermarking confers authority. An SVD-AES-based digital picture watermarking technique is the foundation of our research effort, which enables secure digital image transfer over networks. SVD-based watermarking is used initially. An image is encrypted using the advanced encryption standard (AES) technique after watermarking. AES decryption produces the watermarked image once the encrypted image has been sent via networks. The AES-128 encryption algorithm is used in the suggested procedure. The algorithm exhibits resistance to copy-and-paste, copy-and-paste, and cryptographic attacks such as brute-force attacks.

Pulgam and Shinde [48] have used encrypted watermarks for medical imaging. Gafsi et al. [49] have provided an enhanced chaos-based cryptosystem that can quickly encrypt and decrypt confidential color images. A complicated chaos-based pseudo-random noise PRNG-based security is suggested. High-dimensional characteristics have presented new vulnerabilities unless appropriately planned. Zhang and Ding [50] have designed an enhanced chaos-based cryptographic system that could quickly encrypt and decrypt confidential color images. To provide a high-quality key with high unpredictability behavior, high entropy, and high complexity, a complicated chaos-based PRNG is suggested. The secret image is to be encrypted using an upgraded architecture that relies on permutation, substitution, and diffusion features.

Mokashi et al. [51] have studied the authentication of images that are robust against attacks. A hybrid watermarking approach made up of the DWT-DCT in combination with the SVD (DWT-DCT-SVD) is proposed. Here, DWT-DCT-SVD is used to obtain the singular values of watermarks 1 (fingerprint) and 2 (signature). To increase its dependability, durability, and originality, the image is enhanced with a combination of watermarking techniques and two biometric traits. A dual anti-counterfeiting technique for QR codes is provided by Xun et al. [52], employing a combination of encryption and digital watermarking schemes. First, an RSA-based encryption mechanism is used to encrypt the authentication data. The watermark itself is encrypted by RSA, but neither the embedding approach nor its embedding locations are traced. The overall summary of the secure image watermarking methods is presented in Table 2. It can be concluded that the use of the encryption standard in combination with watermarking may significantly improve the overall performance.

It is clear from the summary in Table 2 that the ASE is the most efficient encryption standard, but the speed concern is still a challenge as watermarking uses hybrid transformation, which makes the algorithm bulkier.

Table 2. Summary of the secure image watermarking methods based on the encryption standards

Author	Methodologies	Encryption Used	Performance Parameter	DATA Base Type
Bose and Maity [35]	DL-based approach abbreviated as (ADMM) using the SVD for the spares watermarking. Using CS	Security using CS domain	PSNR, SSIM, FSIM	Color Images
Yasmeen and Uddin [36]	Multi-level operations of DWT and SVD. DCT for video watermarking	No encryption is mentioned as future scope of work	PSNR, SSIM, NC	Video Data
Sivananthamaitrey and Kumar [37]	A Genetic algorithm (GA) based optimum method of dual watermarking using SWT and SVD	No encryption included.	Time complexity and embedding capacity are evaluated	Color Image and Normal Image
Naffouti et al. [38]	Have used the combination of the, SVD, and DWT for the watermarking	No encryption involved	PSNR, (MSE), (SSIM), (UIQI), (NC)	GreyScale Image
Singh and Singh [39]	A blind image watermarking using DWT-SVD, and DCT	No only copy right protection	PSNR	Multimedia Use of Images

Zear et al. [40]	Multi transform security-based watermarking DWT, DCT, SVD, And BPNN is used for the extraction process	Transform based security	PSNR, BER and NC	Color Images Modalities
Luo et al. [41]	An DWT, HD, SVD based watermarking using FAO optimization	No encryption is not involved	NC, PSNR and SSIM	Color Image
Rajput et al. [42]	A Hybrid HD, SVD, DWT based watermarking	No	NC, PSNR, BER, NAE, SSIM	Color Image
Nazir et al. [43]	Have used DWT, HD, SVD, based watermarking using FOA optimization	Hyper chaotic encryption is applied on watermark	PSNR, SSIM, and NC	Color Image
Mannepalli et al. [44]	Have proposed and ED based watermarking in DWT, ED, Using the HH coefficients.	BC based encryption is adopted	PSNR, NC	Color Image
Yao et al. [45]	Have used the DWT-SVD based watermarking approach	used the BC environment	PSNR	Grey Scale Image
Rathord and Rai [46]	DWT-SVD, HD based serial watermarking	No encryption	PSNR-SSIM	Color Image
Sahila and Thomas [47]	A combination of the SVD-based watermarking with the AES based encryption	AES encryption is applied to securing the watermark	PSNR and NC	Color Image
Gafsi et al. [49]	Have used various encryption standards for watermarking SVD	AES, and TDES encryption	PSNR-SSIM	Color Image
Zhang and Ding [50]	Have proposed image security method using AES encryption	AES encryption for security.	NCPR, UWAC	Color Image
Mokashi et al. [51]	A hybrid approach of the DWT-DCT-SVD	Encryption for QR code	PSNR-SSIM	Video File

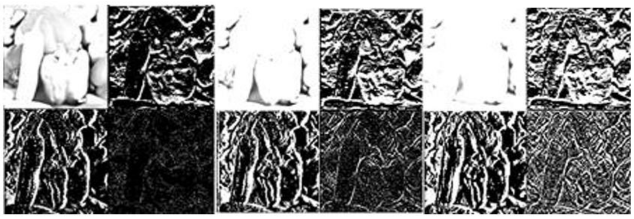
2.1 Related work to intelligent and hybrid attacks

Watermarking techniques must be resistant to a wide range of threats. In recent studies, the hybrid attack [53-56] has been considered for evaluation. Xiao et al. [53] have proposed an algorithm for watermarking applications using DWT based on FOA to eliminate the issue of transparency and robustness. FOA is simple and has proven efficient for optimal scaling. Awasthi and Srivastava [54] proposed a dual image watermarking technique for data security that utilizes lifting wavelet transformation (LWT), PSO-SVD, and JAYA optimization. The method seems computationally complex. And simply using SVD might require more robustness. Ahmadi et al. [55] have preset the dual-color image intelligent PSO-based optimization in the SVD domain watermarking. The PSO is stochastic and comparatively slow to converge. Laishram and Manglem Singh [56] have designed a blind watermarking approach for the medical images, considering the various hybrid attack analyses. ROI-based watermarking is used. Mehraj et al. [57] have designed watermarking for heritage multimedia and also considered hybrid attack evaluations for watermarking cases. It is found that watermark extraction and image reproduction are still ill-posed problems under hybrid attacks. This paper presents a new intelligent image watermarking scheme based on DWT and SVD using the human visual system (HVS) and particle swarm optimization (PSO). The cover image is transformed by one-level (DWT), and then the LL sub-band of the transformed image is chosen for embedding. To achieve the highest possible visual quality, the embedding regions are selected based on HVS. Ahmadi et al. [58] and Ahmadi et al. [59] present an intelligent DWT-SVD-based watermarking, including PSO optimization for invisibility improvement. The best HVS-quality regions are selected for embedding the watermark. A blind CIW approaches by watermarking for copyright protection. The watermark is proposed to be embedded in the B channel of RGB space. The method performs significantly well. Ahmadi et al. [60] have added the additional digital signature for optimally watermarking implementations. Watermark schemes have discovered and developed their advantages by means of singular-value decomposition. Therefore, in recent decades, there has been a significant increase in the use of the SVD domain in many new image watermarking schemes, which show high robustness and imperceptibility. The material in this article is crucial and has the potential to help researchers create effective, resilient, and hybrid SVD-based picture watermarking systems. Sharma et al. [61] have proposed a nature-inspired secure, and intelligent approach to image watermarking. They have intelligently scrambled the watermark data with the use of a chaotic map for embedding. Prabha and Sam [62] have adopted grasshopper optimization, which is in a chaotic domain for secure watermarking design, but the method looks computationally complex. Hosny and Darwish [63] have used fractional order moments using the chaotic map for watermark embedding. Hasan et al. [64] have used the DWT-DCT combination for securing watermark information. Kazemi et al. [65] have proposed an ML-based CIW approach using NN-based computation. Garg and Kishore [66] used the PSO to find the optimal watermarking solution. Recently, Yamni et al. [67] proposed the use of Artificial Bee Colony (ABC) optimization to improve the effectiveness of the CIW system, stating that optimization can be effective in selecting the optimal scaling factor.

3. CHALLENGES AND MOTIVATIONS

Most of the watermarking techniques have been created utilizing 2D grayscale photos. Conventional color RGB picture watermarking technologies face several limitations, such as a significant memory requirement for computation and data storage, or an excessively high computational cost. It is assumed that slight parameterization changes and the visual appearance of images can be jeopardized in the face of increased security and algorithmic robustness. Thus, a dual watermark embedding technique is presented in this research to add additional resilience rather than somewhat compromising parameter quantities. There are still many problems. Robustness is a factor that needs to be carefully considered. Some intense video processing may alter the watermark signal may be altered by some intensive video processing. For an intended use, a specific factored check must be defined. The collusion attacks with real-time watermarking, as suggested in the literature, present some significant difficulties. The perceptual measures are enhancing the effectiveness of numerous picture watermarking methods. Using the video's perceptual qualities instantly is difficult. Design concerns, needs analysis, selection of watermarking methods, speed, resilience, and indeed the associated tradeoffs are challenges while watermarking.

By first transforming RGB photos to grayscale 2D images, earlier techniques inserted watermarks. Due to the limitation of most wavelet transform methods to 2D dimensions, this study suggests that before watermarking, employ picture measurements as well as convert 3D photos to LAB spaces. Both color and grayscale photographs should work nicely with the suggested technique. The image dimensions should be recognized as both a 3D and 2D distribution, utilizing the techniques listed below: It is common practice to use the DHT to make watermarking systems more resilient. A technique called DWT is used to downsample a picture into sub-bands with multiple resolutions by using high- and low-pass wavelet filters. Each DWT level generates four sub-bands: LL, LH, HL, and HH, which correspond to the L-low and H-high pass filters. Figure 4 recreates the DWT-decomposed experiment for input images up to levels 1 to 3. The wavelet-based DWT clearly offers stronger resistance as a consequence of enhanced embedding options and is therefore frequently chosen to increase the robustness of watermarking techniques.



a) 1st level b) 2nd Level c) 3rd level

Figure 4. DWT decomposition example images

4. HD AND SVD FOR IMAGE PROCESSING

In this paper, it is proposed to use a hybrid combination of the HD and SVD decompositions. The mathematical modeling of each of these methods is presented in this section.

HD: represents the Heisenberg Decomposition, it is a matrix decomposition used for only square matrix decomposition [13, 14].

A nxn square size matrix X may be decomposed using HD as given in Eq. (2).

$$PHP^T = HD(X) \tag{2}$$

SVD: The SVD method is a mathematical factorization algorithm used for real complex image matrixes. Using SVD, the cover image is decomposed into a wavelet sub-band matrix Ci of size $m * n$, represented as the product of three matrices containing scalar values as follows:

$$C_i = U_C * S_C * {V_C}^T \tag{3}$$

where, S_C represets the singular values of the cover image. The values of S_C are all non-zeros and are placed diagonally in the matrix. The use of SVD for the watermark insertion process is robust and less affected by most of the attacks. Similarly, the inverse process is also the multiplication of all three decomposed matrices together. Therefore, SVD is most widely being used for watermarking digital images.

5. PROPOSED WATERMARK EMBEDDING

To provide robustness, the paper suggested a revised dual-high-security technique. After supplementing the HD decomposition, the suggested watermarking technique replaces the SVD values, as well as embeds a watermark logo within the decomposed DWT coefficients. This paper proposes to replace SVD with QSVD and combine it with HD for better robustness. By distributing the watermark data among several components of the decomposed matrix, HD increases the signal's redundancy. As a result, it becomes more challenging for hackers to use attacks like noise addition, filtering, and compression to remove watermarks. The above approach makes two key and valuable contributions. The block diagram of the proposed watermark embedding method is presented in Figure 5. The dual key is used to embed the watermark serially every time a different text numeric key is used for embedding.

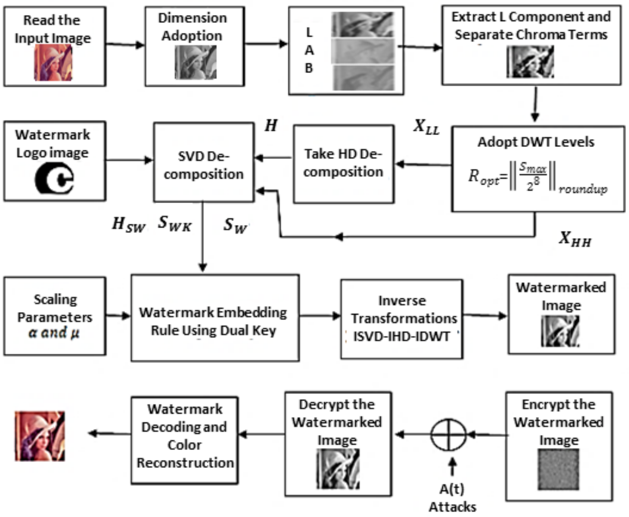

Read the Input Image
Dimension Adoption
L
A
B
Extract L Component and Separate Chroma Terms
Watermark Logo image
SVD De-composition
H
Take HD De-composition
X_{LL}
Adopt DWT Levels
$R_{opt} = \left\| \frac{S_{max}}{2^8} \right\|_{roundup}$
H_{SW}
S_{WK}
S_W
X_{HH}
Scaling Parameters α and μ
Watermark Embedding Rule Using Dual Key
Inverse Transformations ISVD-IHD-IDWT
Watermarked Image
Watermark Decoding and Color Reconstruction
Decrypt the Watermarked Image
A(t) Attacks
Encrypt the Watermarked Image

Figure 5. Block diagram of proposed dual key based robust secure encrypted watermark embedding methodology with attacks

The above approach makes three key contributions:

a) It adaptively incorporates the DWT level according to the image size and adopts the L color component containing more entropy. The robust DWT-QSVD-HD-DUAL key-based watermarking is proposed, which embeds the watermark using the singular values exchange concept.

b) Although the paper makes the entire process faster than study [41], and as a major contribution, the secure AES encryption is combined for better robustness. The DWT level is kept constant at 2 by altering the size of the watermark. The dual key embedding with QSVD values is proposed to make the algorithm unique.

c) The FOA optimization is used for the scaling parameter adaptation for PSNR calculation and balancing invisibility and robustness. Additionally, three cases of hybrid attack analysis are performed in addition to standard attacks.

The additional security is provided by using the AES-based modified fast encryption algorithm. The attacks are applied to the encrypted watermark during transmission, and thus, with the combination of decryption at the receiver side, the robustness is improved in the proposed method.

5.1 Watermark embedding

The mathematical Eqs. (4) and (5) provide the step-wise watermark embedding. The embedding rule given by Eq. (6) uses α as a scaling factor for maintaining visibility. The sequential algorithm for embedding the watermark, known as Algorithm 1, is presented below:

Algorithm 1: Watermark Embedding

```
Input: Lim, and logo
Output: Wim→Watermarked L image
1. Read true color image C.
2. Convert RGB to LAB color formats.
3. Adopt the number of DWT levels and scaling factor to implement the watermark. The number of DWT levels is adopted as R.
Adopted DWT levels
        $R_{opt}=\left\|\frac{S_{max}}{2^8}\right\|_{roundup}$    (4)
4. Then R level DWT LL image of L component
        $X_{LL}=\underbrace{DWT}_{R_{opt}}(\text{Lim})$    (5)
5. Converted to HD and adopt the size of the LL component.
        $H_i = H_{sw} * S_{wk} * S_w$    (6)
6. Embed using SVD values to produce a watermarked image.
7. Read and resize the LL component to fit the logo or signature image (optional).
8. Find the SVD values of LL-DWT and watermark and signature data matrixed by using the embedding rule.
9. Use a scaling factor with SVD values to maintain the invisibility.
        $SV_w = S_{LL} + \alpha * (S_w + S_S)$    (7)
10. Finally, the watermarked images are reproduced by taking the inverse SVD and DWT transforms and then reproducing the color RGB image back from LAB.
11. Apply the watermark attacks for evaluation.
end Algorithm
```

5.2 Secure watermark generation and reconstruction

This paper proposes to incorporate the rapid AES algorithm by taking a single permutation combination. The encryption is a combination of shuffling and encoding procedures.

Modified AES

In this paper, a straightforward customized rapid AES encryption technique regarding video security is suggested; initially the random key was generated as:

$$\text{key}(m) = \text{Rand}(\text{Key}(m.n)) \tag{8}$$

The XORing principle, which itself is defined simply, is employed to encrypt images.

$$Enc_{img}(m,n) = \text{Img}(m,n) \otimes \text{key}(m,n) \tag{9}$$

Algorithm 2 presents the suggested encryption method.

Algorithm 2: Rapid AES

```
1. Watermarked image is input as $Im_{in}$ in the $L$ component domain with dimensions [n, m].
2. Key matrix generation ← $R$ow-column shifting.
        $key(:,m) = key\Big((1+(m-1)^*n)::\big(((m-1)^*n)+n\big)\Big)$    (10)
3. Image encryption
        $Enc_{img}(ind1, ind2) = Img(\, ind1, ind2) \otimes \text{key}(ind1, ind2))$    (11)
4. Add watermark attack to the encrypted image
        $\text{Wimg}=\text{Enc}_{\text{img}}+\text{Atk}$    (12)
5. Decrypt iamge
```

It can be observed that the SVD and HD values are used as the dual-key formulation of the watermarking to make it secure. The logo SVD and the HD values are employed for the embedding process.

5.3 Watermark reconstruction and color reproductions

The final step of the algorithm is the regeneration of the true color recovered image back from the LAB space. This is a two-step procedure. First, the watermark decoding is achieved using Eq. (13).

$$w^\wedge = (H_{sw}{}^\wedge - H_{sw})./a; \tag{13}$$

The overall extraction process is given in Algorithm 3. Then, in the second part, the RGB color image is reproduced from the LAB color space.

Algorithm 3: Watermark Extraction

```
Input: The watermark host image Wimg, scaling array, DWT level R,
Output: WE →Recovered image, RE and Extracted watermark WE
1. Read true color watermarked image Wimg.
2. Perform R-level DWT decomposition ← LLw, LHw, HLw, HHw
3. Apply HD to the size of the LLw component.
        $H_i = H_{sw} * S_{wk} * S_w$    (14)
4. The extracted singular value $Sw^\wedge$ is gained by:
        $Sw^\wedge = (H_{sw}{}^\wedge - H_{sw})./a$    (15)
```

```
5. Take inverse SVD for watermark extraction $W_R$

        $W_R = Uw^{\wedge} * Sw^{\wedge} * Vw'$        (16)

6. Take inverse DWT to reproduce the image.
7. Replace $w^{\wedge}$ with LAB (:,:,1) →Convert LAB to RGB
   back
8. Apply watermark attacks to the evaluation.
End Algorithm
```

5.4 Attack analysis

The above-mentioned procedure is repeated for the 16 various watermark attacks. In the first part of the paper the method of the DWT-HD-SVD is validated as proposed by the study [41]. Dusing the validation part the attacks are applied over the watermarked image itself. And the parametric evaluation is carried out. Letter the concept is extended to proposed secure dual security approach.

6. RESULTS AND DISCUSSIONS

In this section, the expected outcomes of the proposed watermarking methods are presented. This paper has preset the results in two passes. In the first pass, the results of the proposed watermarking using dual-key DWT-HD-SVD-dual are presented and validated against the work of Luo et al. [41]. The results of the watermarking are also compared with those of Rathord and Rai [46]. In the second part of the section, the parametric evaluation of the performance is also presented. Additionally, proposed secure watermarking with encryption is implemented, and qualitative and quantitative results are preset. The attack analysis of the proposed encrypted watermark is carried out for the logo of the study [43], and the results are compared. The two input color images taken from reference papers are used for the current study's presented in Figure 6. The two kinds of logo images are also shown in Figure 6 (c) and Figure 6 (d), respectively, from the researches [41, 43].

The first stage of basic watermarking and extraction results is shown in Figure 7 for the Lena image with the L component. The efficiency of the watermark retrieval can be clearly observed. The comparison of watermark extraction results for Rathord and Rai [46] with our proposed dual key-based wavelet watermarking is given in Figure 7. It can be observed from the figure that the proposed approach clearly outperforms the existing approach and recovers the closest approximate watermark. In addition, the watermarked image's visual quality is also improved. The attack analysis is carried out using the FOA. Using optimization may improve the invisibility and robustness criteria of watermarking. The performance of watermarking is evaluated under the exposure of attacks, viz., filtering, different types of noises, cropping attacks, in addition to JPEG compressions, sharpening, motion blur, and rotation.

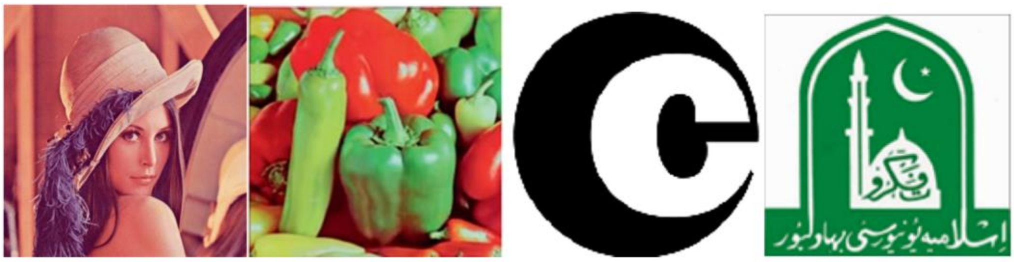

a) Lena image b) peppers mage c) copyrighrt logo [41] d) watermark [43]

Figure 6. Host and the watermark input images used for evaluation in the recent studies. The Host images of 512×512 and watermark of 356×356 sizes are considered

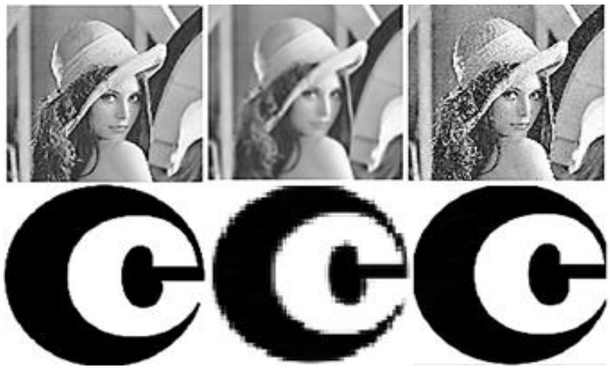


Figure 7. Comparison of the extracted watermark using the Rathord and Rai [46] and proposed dual key based Watermarking

6.1 Performance evaluation under attacks

The proposed method's performance is evaluated using 12 different types of attacks on the watermark images. To evaluate the performance, statistical parametric features are extracted and evaluated under various attacks.

The basic properties and the parameters used for the various attacks are shown in Table 3. The mask sizes and variances need to be observed. The mathematical values of the parameters are defined as follows:

Table 3. Description of the attacks used for comparative analysis [43]

Attack	By [43]	Proposed
Filter attack	Mean filter (3×3)	Mean filter (3×3)
	Median filter (3×3)	Median filter (3×3)
	Wiener filter (3×3)	Wiener filter (3×3)
Noise attack	Salt and pepper noise (0.001)	Salt and pepper noise (0.01)
	Speckle noise (0.001)	Speckle noise (0.01)
	Gaussian noise (0.001)	Gaussian noise (0.001)
Motion blur	Theta=4, length=7	Theta=5, length =10
Sharpening	0.8	0.9
Rotation	2 degrees	5 degrees

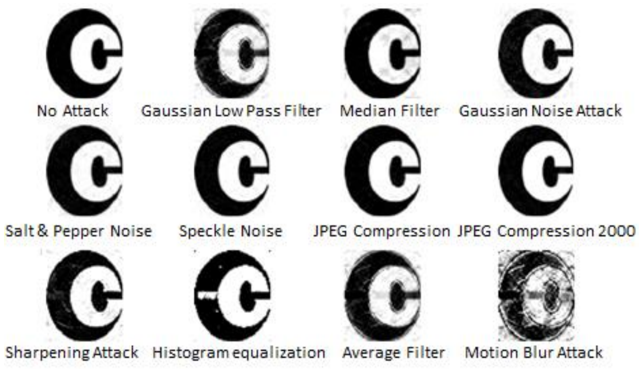


Figure 8. Validation of results for watermarking with Luo et al. [41] for the Lena image under various attacks

To further validate the code's effectiveness, the watermark extraction is validated under various attacks, as shown in Figure 8. Validation is shown for watermarking with Luo et al. [41] DWT-SVD-HD for the Lena image. It can be observed that watermarks are successfully recovered in all cases of attacks.

Figure 8 compares Luo et al. [41]'s validations of the performance of the watermarking results. Figure 8 demonstrates that the proposed dual-key-based secure watermarking method is capable of efficiently recovering the watermark under various noise and filtering attacks, including sharpening and histogram equalization. Only slight performance degrades in the case of large motion blur concerns.

A. Parametric performance under attacks using FOA

To demonstrate performance under various attacks, this section presents the variation of PSNR performance across different scaling parameters, which are plotted against different attacks. The FOA optimization, as proposed in Algorithm 4, is employed to determine the optimal scaling parameters α\alphaα for improving robustness during the attack analysis.

Algorithm 4: Using FOA to Find the Optimal Scaling Factor

```
Input: ← Scaling factor array, α=S(i=1, 2, . . . , t); λ, ωi(i=1, 2, 3); FOA population location, Xa, Ya; $N_{\max\_itr}$, population size MG, Img as host image, watermark image C.
Output Variables: → Optimal scaling factor, α;
1: Embed watermark ← using the proposed Algorithm 1, → (DWT-SVD-HD-Dual).
2: Generate a watermarked image $W_{Img}$.
3: Simulate with K attacks as smell concentrations ←using $S_i$ the scaling factor.
4: Encrypt watermarked image $W_{Img}$ using the
   modified AES Algorithm 2.
5. Apply extraction to the decrypted watermarked image $D_{Img}$ to get the extracted watermark W*i.
6: Evaluate the statistical parameters NC, SSMI, and
     PSNR, ←for each $S_i$ Scaling factor.
7: Update OEF and determine searching distance;
8: Determine the value of judgment for smell concentrations.
9: Using the updated OEF smell judgment function is gained.
10: Optimally determine the maximum smell concentration.
11: Calculate the population size MG,
    if (MG is satisfied)
            Stop loop and save the optimal scaling
        else
            update MG value
    end
12. Return output optimal α;
End Algorithm
```

B. Quantitative PSNR performance comparison

The performance comparison of the achievable PSNR values for the Lena image is shown in Table 4 for the three methodologies. Table 4 shows that the proposed method performed well in PSNR compared to the existing methodology of Liu et al. [14], but due to the use of the dual key, more robustness is observed. The proposed method improves the SNR over the Liu et al. [14] by approximately 0.11 dB.

Table 4. Performance comparison of PSNR for existing and proposed method based on DWT-HD-SVD for Lena image

Parameter	DWT-HD-SVD [41]	DWT-HD-SVD-LAB	DWT-HD-QSVD-Dual
Watermaked	30.86189	30.98119	30.97568
Extrected	19.20601	19.35788	19.41516

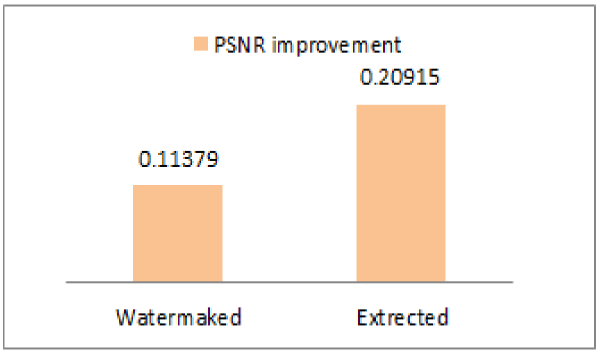


Figure 9. The PSNR improvement in dB with DWT-HD-SVD dual key method

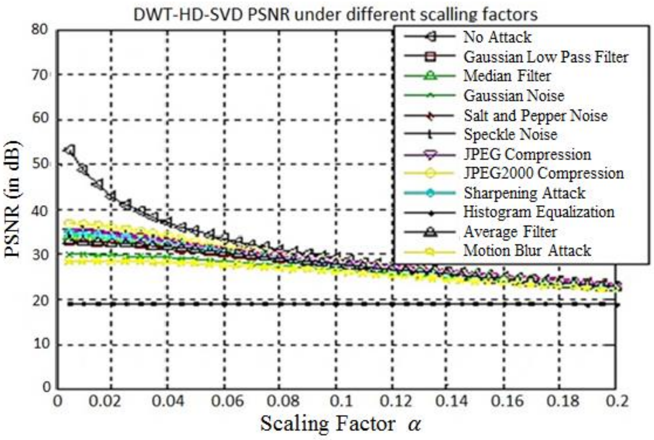
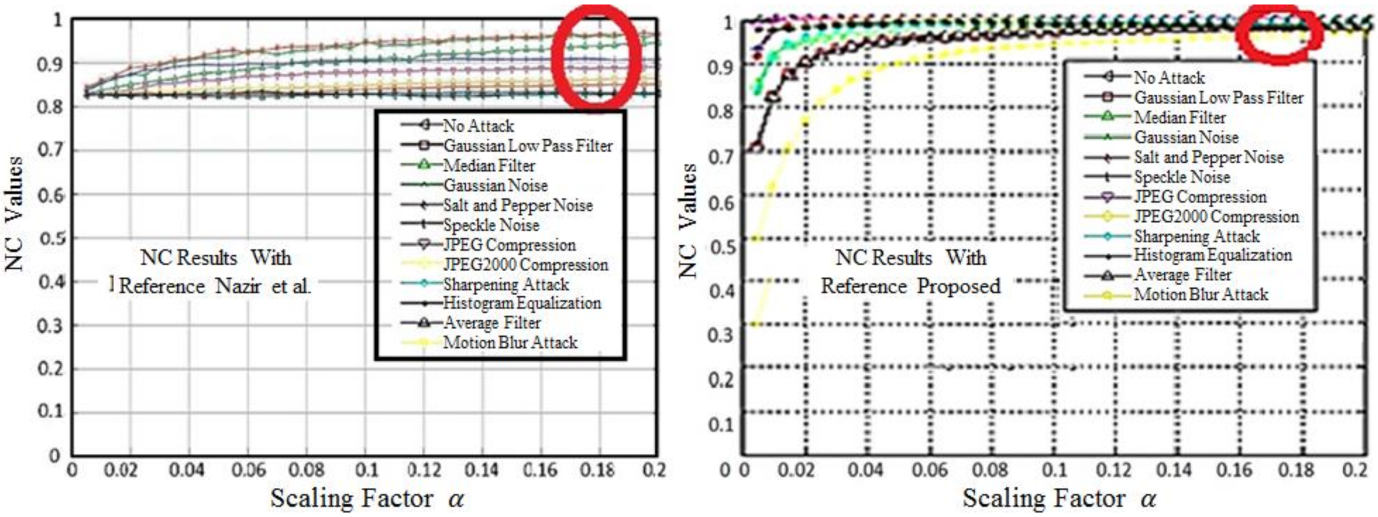


Figure 10. Results of the PSNR comparison for different attacks with proposed method



a) Results of Base R*eference* Nazir et al. [43]   b) Result of the NC for our Proposed DWT-SVD-HD Dual

Figure 11. Results of the NC calculated by the proposed dual key based method under the different attacks

$$\text{Psnr} = \frac{\sum f(x,y)^2}{\sum(f(x,y) - W(x,y))^2} \tag{17}$$

The extracted PSNR offers a significant improvement over the dual-key method of around 0.6 dB. The parametric performances of PSNR improvement in dB are shown in Figure 9 and are evaluated and plotted in bar chart form for PSNR.

Figure 10 shows that the proposed dual-key-based security method has a better capacity for watermark extraction. It is observed that the proposed method outperforms the existing one for different watermark sizes (128×128 and 64×64). Figure 10 displays the PSNR comparison results for various attacks using the proposed method. In this paper, Gaussian filter, median filters, Gaussian noise, average filter, and motion blur attacks are considered for evaluating the performance under the presence of Gaussian filter. Attacks for different attacks are presented in Figure 10.

Figure 11 shows that for the motion blur attack, the NC value is the lowest, as shown by the yellow color mark. But overall, all NC values terminate at more than 0.95, which is good performance under attacks. Figure 11 also compares the NC values of our proposed method with those of Nazir et al.'s NC study [43]. It can be clearly observed that the proposed method outperforms all attacks and offers higher NC values. It can be observed from the red circle that the NC variation is significantly less for all attacks in our proposed method, which justifies the performance improvement over the existing approach.

$$NC(x,y) = \int f(x,y) * f(x-t, y-t)' \tag{18}$$

Similarly, the results of the SSIM of the proposed method are validated and calculated for the proposed dual-key-based method for different attacks.

$$SSIM(x,y) = \frac{(2\mu_x\mu_x + C_1) * (2\sigma_{xy} + C_2)}{(\mu_x{}^2 + \mu_y{}^2 + C_1)(\sigma_x{}^2 + \sigma_y{}^2 + C_2)} \tag{19}$$

It can be observed that the proposed method offers significantly higher SSIM values, as using dual-level security to add more robustness and a and a slight compromise to SSIM values is considerable. The Gaussian noise performance is at its minimum for SSIM, and it is even in the range of above 0.7. The performance improvement with the proposed LAB-Dual Key-based watermarking can be clearly observed from the comparison of performance under the different attacks. For proposed and existing methods, as shown in Figure 12, there is a significant improvement in the SSIM performance.

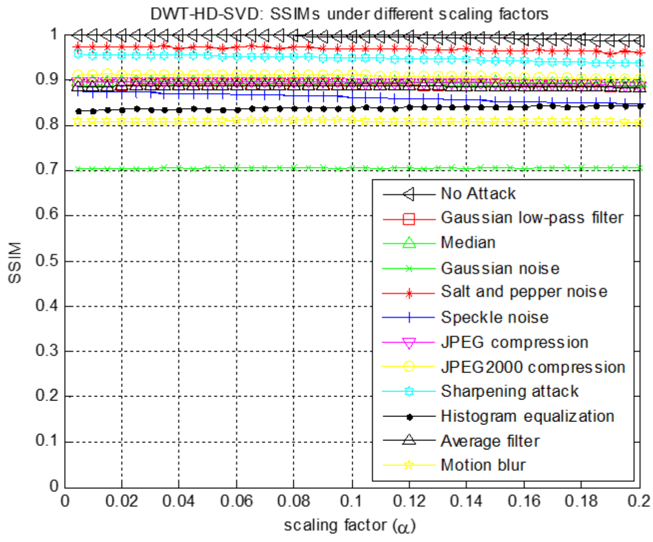


Figure 12. Results of the SSIM comparison for different attacks with proposed DUAL key based DWT-SVD-HD dual method

6.2 Secure encrypted watermarking outcomes

This paper has proposed a rapid encryption standard for securing the watermarked image during transmission or storage. This section presents the qualitative and quantitative evaluation of the secure watermarking results of the proposed method. While in the second pass of the paper, the attacks are applied to the encrypted images and reconstruction is carried out, and the results are compared with the method of the paper [43]. An example of the various attacks applied to the Lena image is shown in Figure 13.

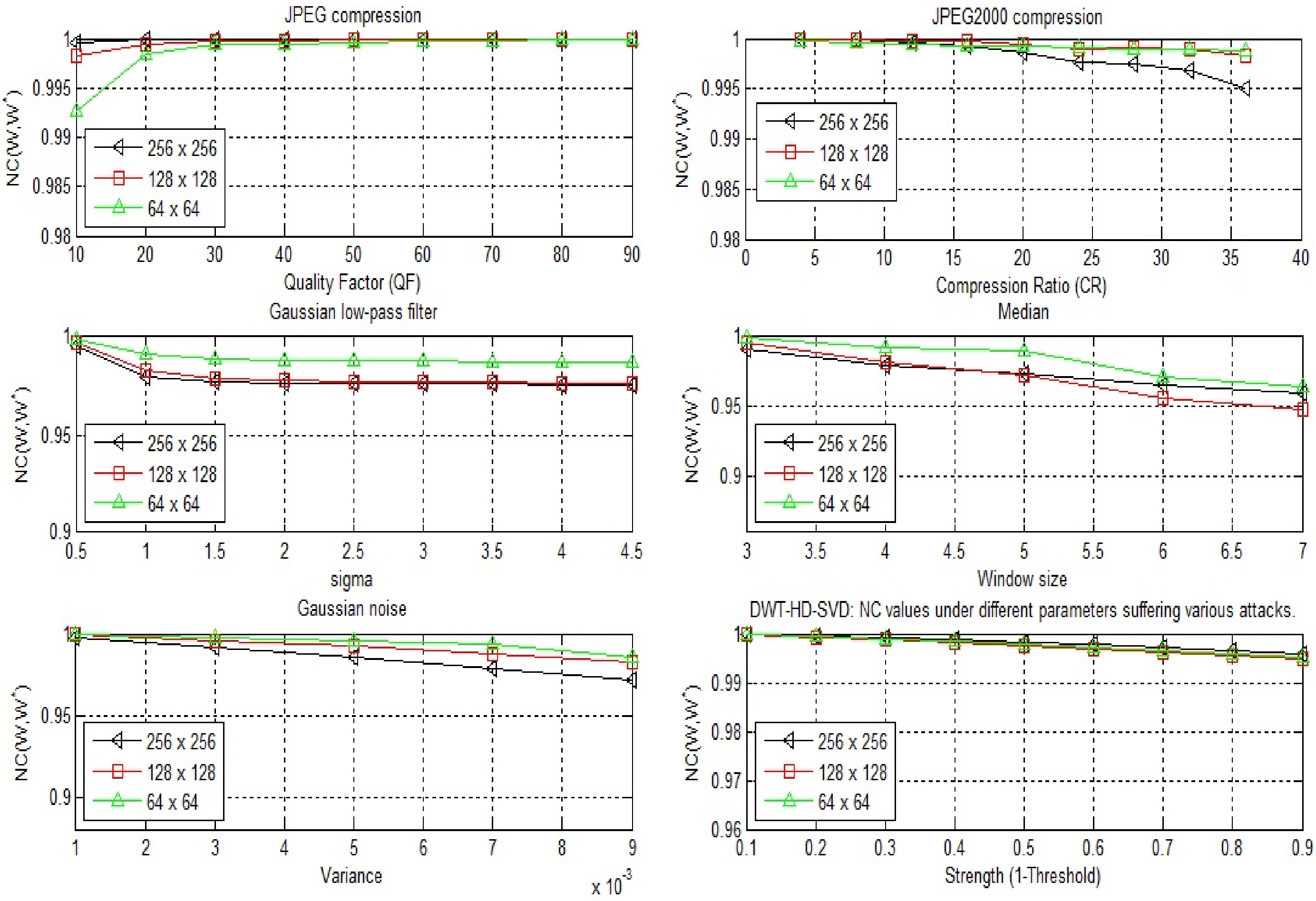


Figure 13. Results of our Dual key embedding under JPEG attack with FOA optimization

It can be clearly observed from Figure 13 that the NC values are evaluated under the variation of different noise variances and the compression ratio, quality factor, and window sizes. The proposed method offers significant NC values under various noises and even for different image sizes. Three image sizes (256×256, 128×128, and 64×64) are considered for the evaluation in the paper.

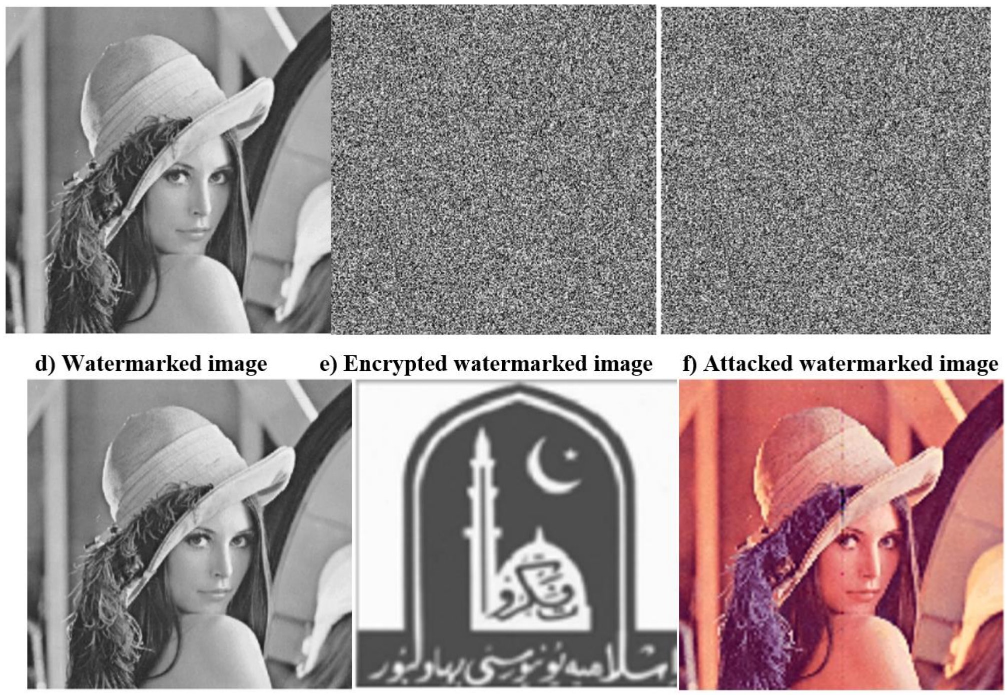
It is observed that NC is maximum for the 256×256 size, and as the quality factor might increase, the overall NC value is achieved to be around 100 percent. The performance under JPEG compression 2000 is evaluated for different compression ratios. It is found that at the lower compression ratio, the NC value is near 1, and as the CR increases, the minimum NC is offered as 0.995 for the 64x64 size, which shows the effectiveness of the proposed DWT-SVD-HD-Dual method. The low-pass filter performance of NC improves as the size of the image decreases.

6.2.1 Qualitative comparison with the previous study [43]

The extracted results for crypto weights for the encrypted image under different noise attacks are shown in Figure 14. It can be observed that, with significant invisibility and shuffling, the encrypted data is robust and secure. An example of the sequential outcomes is shown in Figure 14, plotted using the proposed method and the watermark by Nazir et al. [43] for salt and pepper noise attacks.

The quality of the encryption remains consistently high even under various noisy attacks, as observed from the crypto weights in Figure 15. The proposed method performs equally well for different kinds of attacks in terms of crypto weights. Since the attacks are applied in the encrypted domain, the quality of the histogram equalization attack is superior in this method.

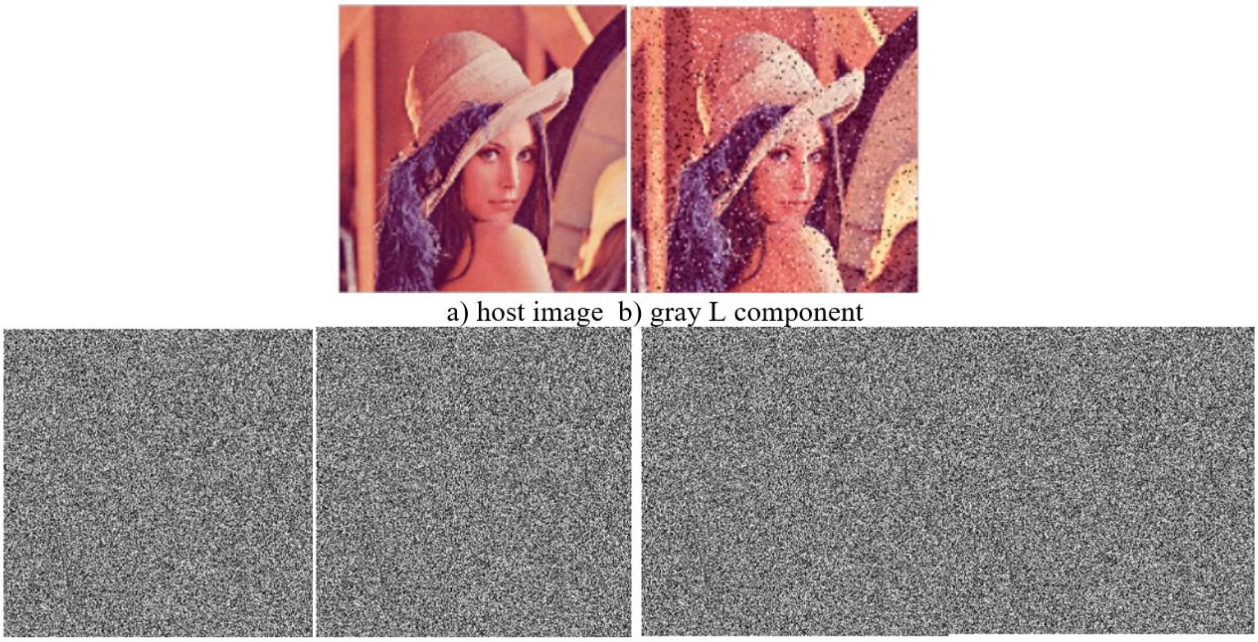
a) 512x512 Host image **b) L component 512x512** **c) 256x256 watermark**



d) Watermarked image e) Encrypted watermarked image f) Attacked watermarked image

g) Decrypted watermarked image h)Extracted Watemark i) recovered image

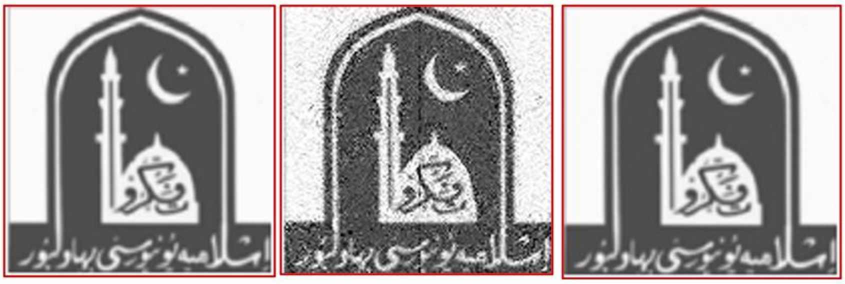
Figure 14. Sequential results under secure watermark for Salt & Pepper Noise attacks



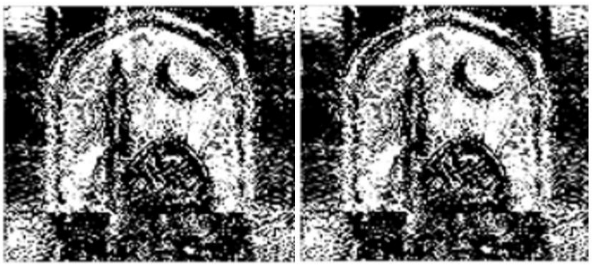
a) host image b) gray L component

c) encrypted watermarked image, d) speckle noise image e) Salt & Pepper Noise f) Gaussian noise

Figure 15. Results of proposed DWT-SVD-HD watermarking under various attacks



a) Gaussian noise attack b) with Speckle noise c) with salt &pepere noise



d) UnderAverage filter e) Under the motion blur

Figure 16. Results of the extracted watermark under the AES secure encrypted watermarked image exposed to various attacks

6.2.2 Attacks analysis for watermark with Nazir et al. [43]

The results of the watermark attack analysis applied to the encrypted images are evaluated in Figure 16. The results are preset for the extracted watermark under the AES secure encrypted watermarked image exposed to various attacks. The quality of the extracted watermark is clearly observed, and even in the worst case of motion blur, the watermark is visible in Figure 16 (e), justifying the efficiency even considering the higher level of noise in the worst cases.

6.3 Evaluation of hybrid attacks

Another experiment was carried out to justify the performance under the evaluation of hybrid attacks.

There are two independent cases of hybrid attack analysis considered in this paper: 1) simple watermarking + attacks without encryption; 2) watermarking + AES encryption + attacks.

Case 1: Hybrid attacks without encryption.

The results of the evaluation of secure watermark extraction under the exposure of various dual hybrid watermark attacks are presented in Figure 17.

In this case, hybrid attacks are applied to the watermarked image. Figure 17 shows the evaluation of results for watermark extraction. Using double hybrid attacks as combinations shown in Figure 17 (b-e), The low-pass filter and the noisy attacks are considered in the case of the rotation attack for analysis.

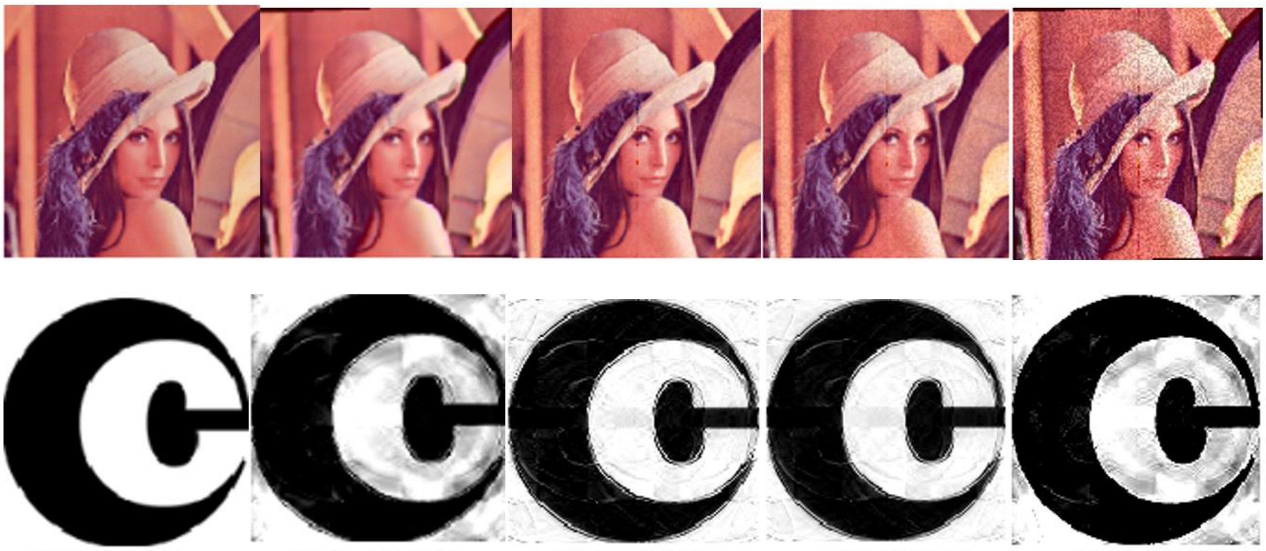
In any case, only two attacks are applied simultaneously. It can be concluded from the figure that for the PSNR of 27.91420 without attacks, the respective PSNR for each attack case is shown in Figure 17.

For noisy attacks, a significant PSNR in the range of 25 to 26 is achieved even in hybrid attacks. But in the case of a rotation attack, PSNR is reduced to 18 dB. But the quality of the recovered image is relatively visually pleasing.

Additionally, multiple hybrid attacks are applied to the watermarked image. Figure 18 shows the evaluation of the results for this case. Four attacks, including rotation, Gaussian low pass filter, noise, and JPEG compression, are applied in the combinations shown in Figure 18.

The types of noisy attacks are changed from Gaussian, salt & pepper, and speckle noise, keeping other attacks the same as rotation and compression attacks. Results corresponding to the different noise cases are shown in Figure 18.

It can be concluded that in multi-hybrid attacks, PSNR is reduced from 27.91420 to 18 dB, and the quality of reproduction is still justified by the NC values as shown in Figure 18.



PSNR=25.2302 PSNR= 18.35450 PSNR=26.60018 PSNR=26.21914 PSNR=16.89580

a) Original image, b) Rotation + Lowpass Gaussian filter, c) Gaussian Noise + Lowpass filter, d) Speckle Noise + Lowpass filter, e) Rotation + Speckle noise

Figure 17. The result evaluation of secure watermark extraction under the exposure of the various dual hybrid watermark attacks

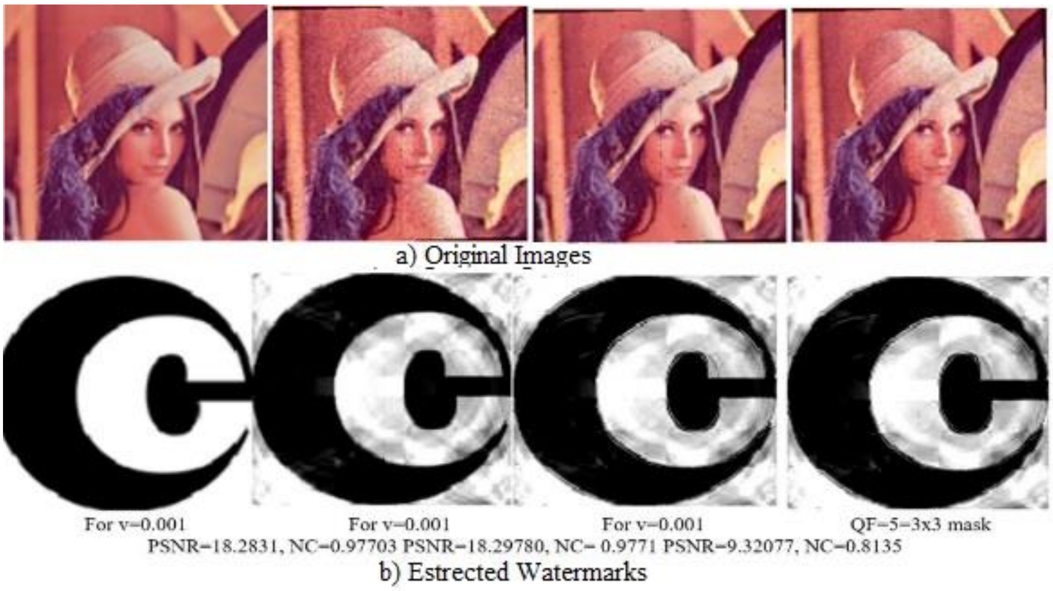


Figure 18. The result evaluation under the various multiple hybrid attacks including JPEG, Rotation, Gaussian filter, and Noise. a) Original Image, b) watermark extracted

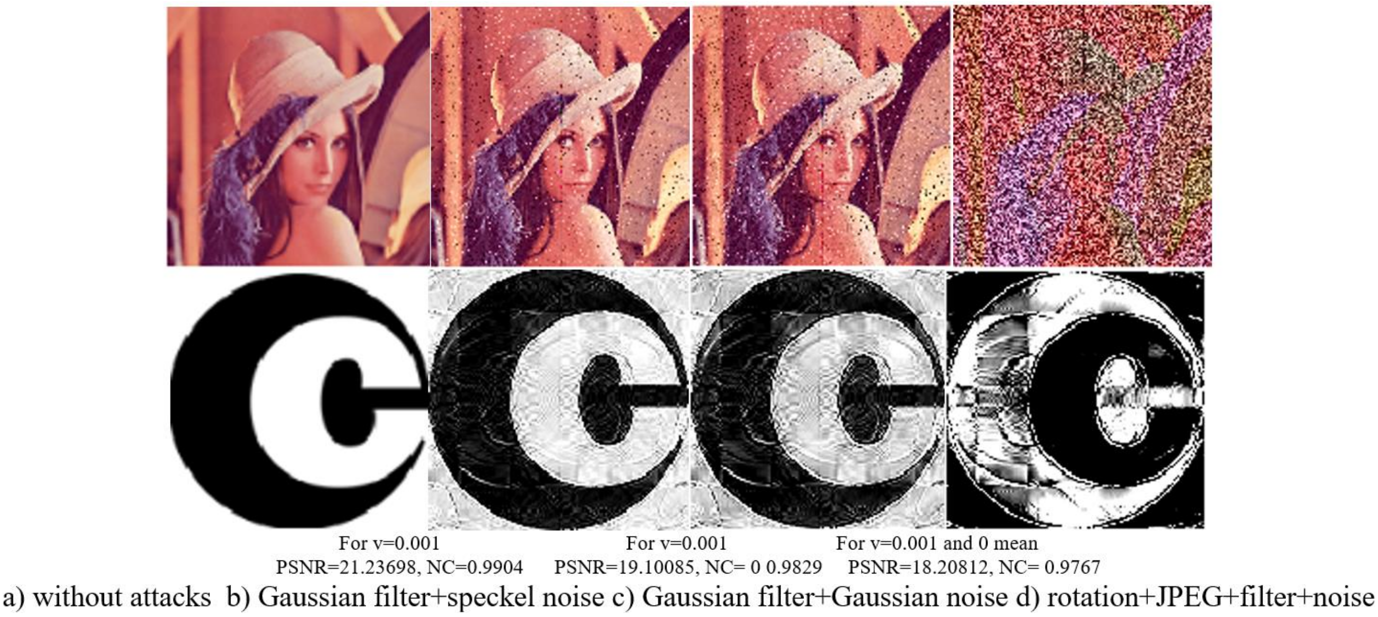

For v=0.001
PSNR=21.23698, NC=0.9904
For v=0.001
PSNR=19.10085, NC= 0 0.9829
For v=0.001 and 0 mean
PSNR=18.20812, NC= 0.9767
a) without attacks
b) Gaussian filter+speckel noise
c) Gaussian filter+Gaussian noise
d) rotation+JPEG+filter+noise

Figure 19. The result evaluation under multiple hybrid attacks applied on Encryption domain

Table 5. Comparison of the PSNR for the watermark extraction under hybrid attacks

Images	Original Image	Rotation +Low Pass Gaussian Filter Attacks	Gaussian Noise +Low Pass Filter Attacks	Speckle Noise +Low Pass Filter Attacks	Rotation+Speckle Noise Attacks
Lena	PSNR=25.2302	PSNR=18.35450	PSNR=26.60018	PSNR=26.21914	PSNR=16.89580

Table 6. Comparison of the PSNR and NC for watermark extraction under various hybrid attacks using compression

Cases	Parameter	Gaussian Noise+Lowpass Filter Attacks	Speckle Noise + Low Pass Filter Attacks	Rotation+Speckle Noise Attacks
Attack with watermark image	PSNR	PSNR=18.2831	PSNR=18.29780	PSNR=9.32077
	NC	NC=0.97703	NC=0.9771	NC=0.8135
Attack with Encrypted image	PSNR	PSNR=21.23698	PSNR=19.10085	PSNR=18.2081
	NC	NC=0.9904	NC=0 0.9829	NC=0.9767

Case 2: Hybrid attacks applied to an encrypted image

As a special case, hybrid attacks are applied to the encrypted image instead of the watermarked image. Figure 19 shows that, in the case of dual hybrid attacks, the performance is relatively stable.

$$H_{atk} = A1 + A2 + \cdots .. An \tag{20}$$

$$A_1{=}GLP_{atk}, A_2{=}GN_{atk}, A_3{=}Ro_{atk}, A_4{=}Comp_{atk} \qquad (21)$$

It can be observed from Figure 19 that although watermark extraction is still possible under hybrid attacks, for several hybrid attacks, including filtering, noise rotation, and JPEG compression, the performance of image recovery is still an ill-posed problem.

The PSNR performance of reconstruction is shown under hybrid attacks in Table 5. It can be observed that for noisy and filter attacks, the performance is nearly identical to the true image case, with less than 4% error in PSNR. This reflects the efficiency of the proposed method in the noisy case.

The qualitative comparisons of parameters are given for the two cases of hybrid attacks as shown in Table 6. It can be observed that using the encrypted watermark may offer a higher recovery PSNR for all attack cases. Thus, the proposed secure watermarking is more robust under noisy attacks using AES encryption.

7. DISCUSSION AND SCOPE

The paper proposes a robust and secure watermarking approach taking advantage of QSVD and HD decompositions, and dual keys are used for the encryption process. The advantage of using HD is that it offers improved performance under noisy attacks. Following major observations addressed after the comprehensive studies.

- It has been noted that although PSNR is decreased in multi-hybrid attacks, notable improvements in reproduction quality are still achievable. Under hybrid attacks, it is still possible to retrieve the watermark, and the quality of picture recovery remains unchanged for severe multiple hybrid attacks, such as filtering, noise rotation, and JPEG compression algorithms.
- It can be observed that using the encrypted watermark may offer a higher recovery PSNR for all attack cases, but the recovery becomes slightly more difficult under multiple hybrid attacks of noise, rotation, and compression simultaneously.

The proposed method is applicable in any case of a color image database and may be used for securing color medical images in the future. Financial imaging, data security, and digital broadcasting are some of the expected applications of the proposed research.

8. CONCLUSIONS AND FUTURE SCOPES

The primary contribution of this study lies in enhancing the robustness of watermarking through the implementation of dual-key security, while leveraging the combined strengths of encryption and watermarking techniques. The analysis of hybrid attacks has also been a significant focus of this work. The proposed method employs HD and DWT-QSVD to develop a dual-key-based hybrid algorithm. In this approach, the logo image serves as the first key, while the HH component of the R-level DWT is introduced as the second key to further bolster robustness. The method adapts to various DWT levels based on image size, and a modified watermark insertion procedure is proposed by simultaneously utilizing both keys within the QSVD domain. The pre-processing stage incorporates the LAB color space for entropy maximization, with the adoption of this color space justified by entropy analysis. Dual-level encrypted watermarked images are generated using a modified fast AES algorithm, representing a novel technique in this domain. The findings suggest that enhanced security contributes to the creation of a more robust watermark, reflecting the efficacy of the current method.

The proposed technique is evaluated on color images using parametric studies of NC, PSNR, and SSIM. It is concluded that the dual-key-based method outperforms existing techniques across different watermark sizes, specifically 128×128 and 64×64. A significant improvement in SSIM performance is observed. Notably, for the motion blur attack on 256×256 images, the NC is improved from 0.8322 to 0.9003, and for the average filter, it is enhanced from 0.9294 to 0.9552.

Further analysis reveals that NC reaches its maximum at 256×256, and as the quality factor increases, the NC value approaches 100%. The method's effectiveness is also assessed under JPEG 2000 compression, where it is found that at lower compression ratios, the NC value remains close to 1. As the compression ratio increases, the lowest NC value observed is 0.995 for the 64×64 size, demonstrating the efficiency of the proposed DWT-SVD-HD-Dual technique. The results presented for the extracted watermark under the fast modified AES-secured encrypted image, even when subjected to numerous attacks, confirm the robustness of the approach. Even under worst-case scenarios with higher levels of noise, the quality of the extracted watermark validates the method's efficiency. Additionally, it is concluded that watermark extraction remains feasible even under severe hybrid attacks, with a significant PSNR in the range of 25 to 26 dB being achieved for double attacks. However, when multi-hybrid attacks are applied in the encryption domain, recovering the original image remains a challenging issue, particularly for JPEG and rotation attacks.

Future work could explore various embedding rules and wavelet filters to further enhance performance. Additionally, a comparison of optimization techniques and different transform domain approaches could be employed to improve robustness. The performance of the proposed method could also be tested in various imaging applications, including medical imaging scenarios, to validate its broader applicability.

REFERENCES

[1] Poljicak, A., Mandic, L., Agic, D. (2011). Discrete Fourier transform-based watermarking method with an optimal implementation radius. Journal of Electronic Imaging, SPIE Digital Library, 20(3): 033008. https://doi.org/10.1117/1.3609010

[2] Cedillo-Hernandez, M., Cedillo-Hernandez, A., Garcia-Ugalde, F.J. (2021). Improving DFT-based image watermarking using particle swarm optimization algorithm. Mathematics, 9(15): 1795. https://doi.org/10.3390/math9151795

[3] Mohashin, A.H.M., Dhar, P.K., Shimamura, T. (2019). Blind image watermarking based on discrete Hilbert transform and polar decomposition. In 2019 11th International Conference on Knowledge and Smart Technology (KST), Phuket, Thailand, pp. 78-81. https://doi.org/10.1109/KST.2019.8687512

[4] Agarwal, R., Santhanam, M.S., Srinivas, K. (2016). Digital watermarking: An approach based on Hilbert

transform. In 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, pp. 1035-1042. https://doi.org/10.1109/CCAA.2016.7813887

[5] Chu, W.C. (2003). DCT-based image watermarking using subsampling. IEEE Transactions on Multimedia, 5(1): 34-38. https://doi.org/10.1109/TMM.2003.808816

[6] Singh, R., Rawat, P., Shukla, P. (2017). Robust true color image authentication using 2-D stationary wavelet transforms and edge detection. In IET International Conference ICBISP Chaina.

[7] Tiwari, A., Singh, V. (2013). Digital image watermarking using DWT and shift invariant edge detection. International Journal of Computer Technology and Electronics Engineering (IJCTEE), Corpus ID: 20820219.

[8] Singh, S.P., Rawat, P., Agrawal, S. (2012). A robust watermarking approach using DCT-DWT. International Journal of Emerging Technology and Advanced Engineering, 2(8): 300-305.

[9] Tan, Y., Qin, J., Xiang, X., Ma, W., Pan, W., Xiong, N.N. (2019). A robust watermarking scheme in YCbCr color space based on channel coding. IEEE Access, 7: 25026-25036. https://doi.org/10.1109/ACCESS.2019.2896304

[10] Chaitanya, K., Reddy, E.S., Rao, K.G. (2014). Digital color image watermarking in RGB planes using DWT-DCT-SVD coefficients. International Journal of Computer Science and Information Technologies (IJCSIT), 5(2): 2413-2417.

[11] Huang, Y., Niu, B., Guan, H., Zhang, S. (2019). Enhancing image watermarking with adaptive embedding parameter and PSNR guarantee. IEEE Transactions on Multimedia, 21(10): 2447-2460. https://doi.org/10.1109/TMM.2019.2907475

[12] Pourhadi, A., Mahdavi-Nasab, H. (2020). A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain. Multimedia Tools and Applications, 79(29): 21653-21677. https://doi.org/10.1007/s11042-020-08960-0

[13] Moad, M.S., Zermi, N., Khaldi, A., Kafi, M.R. (2023). Stationary wavelet-based image watermarking for e-healthcare applications. Cybernetics and Systems, 1-16. https://doi.org/10.1080/01969722.2023.2166253

[14] Liu, J., Huang, J., Luo, Y., Cao, L., Yang, S., Wei, D., Zhou, R. (2019). An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access, 7: 80849-80860. https://doi.org/10.1109/ACCESS.2019.2915596

[15] Chaturvedi, A.K., Shukla, P.K. (2020). Effective watermarking technique using optimal discrete wavelet transform and sanitization technique. Multimedia Tools and Applications, 79(19): 13161-13177. https://doi.org/10.1007/s11042-020-08639-6

[16] Shukla, P.K., Rawat, P., Singh, R., Dutta, P.K. (2021). Efficient watermark reconstruction for medical images under rotation attacks using DWT. 3rd Smart Cities Symposium (SCS 2020), 2021: 492. https://doi.org/10.1049/icp.2021.0956

[17] Singh, A.K., Kumar, B., Dave, M., Mohan, A. (2015). Multiple watermarking on medical images using selective discrete wavelet transform coefficients. Journal of Medical Imaging and Health Informatics, 5(3): 607-614. https://doi.org/10.1166/jmihi.2015.1432

[18] He, Y., Hu, Y. (2018). A proposed digital image watermarking based on DWT-DCT-SVD. In 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), Xi'an, China, pp. 1214-1218. https://doi.org/10.1109/IMCEC.2018.8469626

[19] Su, Q., Chen, B. (2017). A novel blind color image watermarking using upper Hessenberg matrix. AEU-International Journal of Electronics and Communications, 78: 64-71. https://doi.org/10.1016/j.aeue.2017.05.025

[20] Su, Q. (2016). Novel blind colour image watermarking technique using Hessenberg decomposition. IET Image Processing, 10(11): 817-829. https://doi.org/10.1049/iet-ipr.2016.0048

[21] Ellinas, J.N., Manolakis, D.E. (2007). A robust watermarking scheme based on edge detection and contrast sensitivity function. In International Conference on Computer Vision Theory and Applications. Scitepress, 2: 93-100. https://doi.org/10.5220/0002047900930100

[22] Elbasi, E., Kaya, V. (2018). Robust medical image watermarking using frequency domain and least significant bits algorithms. In 2018 International Conference on Computing Sciences and Engineering (ICCSE), Kuwait, Kuwait, pp. 1-5. https://doi.org/10.1109/ICCSE1.2018.8374221

[23] Singh, P. (2016). An efficient CRT based digital image watermarking using double density wavelet transform. International Journal of Computer Science and Network-IJCSN, 5(5). http://hdl.handle.net/10760/30195

[24] Agoyi, M., Seral, D. (2012). A multimedia watermark scheme based on double density dual-tree discrete wavelet transform and singular value decomposition. In 2012 20th Signal Processing and Communications Applications Conference (SIU), Mugla, Turkey, pp. 1-4. https://doi.org/10.1109/SIU.2012.6204569

[25] Vidya, K., Sujithra, T. (2018). Robust DWT-SVD based blind watermarking for DIBR 3d video. In 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP), Chennai, India, pp. 1-6. https://doi.org/10.1109/ICCCSP.2018.8452818

[26] Lai, C.C., Tsai, C.C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Transactions on Instrumentation and Measurement, 59(11): 3060-3063. https://doi.org/10.1109/TIM.2010.2066770

[27] Kadian, P., Arora, N., Arora, S.M. (2019). Performance evaluation of robust watermarking using DWT-SVD and RDWT-SVD. In 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, pp. 987-991. https://doi.org/10.1109/SPIN.2019.8711681

[28] Zeng, B. (1999). Reduction of blocking effect in DCT-coded images using zero-masking techniques. Signal Processing, 79(2): 205-211. https://doi.org/10.1016/S0165-1684(99)00094-8

[29] Al-Haj, A. (2007). Combined DWT-DCT digital image watermarking. Journal of Computer Science, 3(9): 740-746. https://doi.org/10.3844/jcssp.2007.740.746

[30] Abdulrahman, A.K., Ozturk, S. (2019). A novel hybrid DCT and DWT based robust watermarking algorithm for color images. Multimedia Tools and Applications, 78: 17027-17049. https://doi.org/10.1007/s11042-018-7085-z

[31] Ansari, I.A., Ahn, C.W., Pant, M. (2018). On the security

of" block-based SVD image watermarking in spatial and transform domains". In 2018 International Conference on Digital Arts, Media and Technology (ICDAMT), Phayao, Thailand, pp. 44-48. https://doi.org/10.1109/ICDAMT.2018.8376493

[32] Gong, L.H., Tian, C., Zou, W.P., Zhou, N.R. (2021). Robust and imperceptible watermarking scheme based on Canny edge detection and SVD in the contourlet domain. Multimedia Tools and Applications, 80: 439-461. https://doi.org/10.1007/s11042-020-09677-w

[33] Rykaczewski, R. (2007). Comments on "An SVD-based watermarking scheme for protecting rightful ownership". IEEE Transactions on Multimedia, 9(2): 421-423. https://doi.org/10.1109/TMM.2006.886297

[34] Sunesh, V. M., Sangwan, N., Sangwan, S. (2017). Digital watermarking using DWT-SVD algorithm. Advances in Computational Sciences and Technology, 10(7): 2161-2171.

[35] Bose, A., Maity, S.P. (2022). Secure sparse watermarking on DWT-SVD for digital images. Journal of Information Security and Applications, 68: 103255. https://doi.org/10.1016/j.jisa.2022.103255

[36] Yasmeen, F., Uddin, M.S. (2021). An efficient watermarking approach based on LL and HH edges of DWT-SVD. SN Computer Science, 2(2): 82. https://doi.org/10.1007/s42979-021-00478-y

[37] Sivananthamaitrey, P., Kumar, P.R. (2022). Optimal dual watermarking of color images with SWT and SVD through genetic algorithm. Circuits, Systems, and Signal Processing, 41(1): 224-248. https://doi.org/10.1007/s00034-021-01773-y

[38] Naffouti, S.E., Kricha, A., Sakly, A. (2023). A sophisticated and provably grayscale image watermarking system using DWT-SVD domain. The Visual Computer, 39(9): 4227-4247. https://doi.org/10.1007/s00371-022-02587-y

[39] Singh, D., Singh, S.K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimedia Tools and Applications, 76(11): 13001-13024. https://doi.org/10.1007/s11042-016-3706-6

[40] Zear, A., Singh, A.K., Kumar, P. (2018). A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine. Multimedia Tools and Applications, 77: 4863-4882. https://doi.org/10.1007/s11042-016-3862-8

[41] Luo, Y., Li, L., Liu, J., Tang, S., Cao, L., Zhang, S., Qiu, S., Cao, Y. (2021). A multi-scale image watermarking based on integer wavelet transform and singular value decomposition. Expert Systems with Applications, 168: 114272. https://doi.org/10.1016/j.eswa.2020.114272

[42] Rajput, S.S., Mondal, B., Warsi, F.Q. (2023). A robust watermarking scheme via optimization-based image reconstruction technique. Multimedia Tools and Applications, 82(16): 25039-25060. https://doi.org/10.1007/s11042-023-14363-8

[43] Nazir, H., Bajwa, I.S., Samiullah, M., Anwar, W., Moosa, M. (2021). Robust secure color image watermarking using 4D hyperchaotic system, DWT, HBD, and SVD based on improved FOA algorithm. Security and Communication Networks, 2021: 1-17. https://doi.org/10.1155/2021/6617944

[44] Mannepalli, P.K., Richhariya, V., Gupta, S.K., Shukla, P.K., Dutta, P.K. (2021). Block chain based robust image watermarking using edge detection and wavelet transform. Research Square. https://doi.org/10.21203/rs.3.rs-766105/v1

[45] Yao, Q., Xu, K., Li, T., Zhou, Y., Wang, M. (2023). A secure image evidence management framework using multi-bits watermark and blockchain in IoT environments. Wireless Networks, 1-13. https://doi.org/10.1007/s11276-023-03229-4

[46] Rathord, S.S., Rai, M. (2021). Adaptive colour space based robust image watermarking using serial DWT-HD-SVD domain. International Journal of Engineering and Innovative Technology, 10(9). https://doi.org/10.51456/IJEIT.2021.v10i09.001

[47] Sahila, K.M., Thomas, B. (2021). Secure digital image watermarking by using SVD and AES. In Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI, Springer Singapore, 2020: 805-818. https://doi.org/10.1007/978-981-15-9509-7_65

[48] Pulgam, N.D., Shinde, S.K. (2022). Analysis of different encryption techniques used in watermarking algorithm for the security of medical image. In 2022 10th International Conference on Emerging Trends in Engineering and Technology-Signal and Information Processing (ICETET-SIP-22), Nagpur, India, pp. 1-6. https://doi.org/10.1109/ICETET-SIP-2254415.2022.9791814

[49] Gafsi, M., Abbassi, N., Hajjaji, M.A., Malek, J., Mtibaa, A. (2020). Improved chaos-based cryptosystem for medical image encryption and decryption. Scientific Programming, 2020: 1-22. https://doi.org/10.1155/2020/6612390

[50] Zhang, Q., Ding, Q. (2015). Digital image encryption based on advanced encryption standard (AES). In 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Qinhuangdao, China, pp. 1218-1221. https://doi.org/10.1109/imccc.2015.261

[51] Mokashi, B., Bhat, V.S., Pujari, J.D., Roopashree, S., Mahesh, T.R., Alex, D.S. (2022). Efficient hybrid blind watermarking in DWT-DCT-SVD with dual biometric features for images. Contrast Media & Molecular Imaging, 2022(1): 2918126. https://doi.org/10.1155/2022/2918126

[52] Xun, Y., Li, Z., Zhong, X., Li, S., Su, J., Zhang, K. (2019). Dual anti-counterfeiting of QR code based on information encryption and digital watermarking. In Advances in Graphic Communication, Printing and Packaging: Proceedings of 2018 9th China Academic Conference on Printing and Packaging, Springer Singapore, pp. 187-196. https://doi.org/10.1007/978-981-13-3663-8_27

[53] Xiao, Z., Sun, J., Wang, Y., Jiang, Z. (2015). Wavelet domain digital watermarking method based on fruit fly optimization algorithm. Journal of Computer Applications, 35(9): 2527. https://doi.org/10.11772/j.issn.1001-9081.2015.09.2527

[54] Awasthi, D., Srivastava, V.K. (2023). Performance enhancement of SVD based dual image watermarking in wavelet domain using PSO and JAYA optimization and their comparison under hybrid attacks. Multimedia Tools and Applications, 82(23): 35685-35717. https://doi.org/10.1007/s11042-023-14723-4

[55] Ahmadi, S.B.B., Zhang, G., Rabbani, M., Boukela, L., Jelodar, H. (2021). An intelligent and blind dual color

image watermarking for authentication and copyright protection. Applied Intelligence, 51: 1701-1732. https://doi.org/10.1007/s10489-020-01903-0

[56] Laishram, D., Manglem Singh, K. (2022). A watermarking method resilient against many hybrid attacks for color medical images. In Proceedings of International Conference on Advanced Computing Applications: ICACA, Springer Singapore, 2021: 425-445. https://doi.org/10.1007/978-981-16-5207-3_36

[57] Mehraj, S., Mushtaq, S., Parah, S.A., Giri, K.J., Sheikh, J.A. (2023). A robust watermarking scheme for hybrid attacks on heritage images. Journal of Ambient Intelligence and Humanized Computing, 14(6): 7367-7380. https://doi.org/10.1007/s12652-022-04445-0

[58] Ahmadi, S.B.B., Zhang, G., Wei, S., Boukela, L. (2021). An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics. The Visual Computer, 37(2): 385-409. https://doi.org/10.1007/s00371-020-01808-6

[59] Ahmadi, S.B.B., Zhang, G., Wei, S. (2020). Robust and hybrid SVD-based image watermarking schemes: A survey. Multimedia Tools and Applications, 79(1): 1075-1117. https://doi.org/10.1007/s11042-019-08197-6

[60] Ahmadi, S.B.B., Zhang, G., Rabbani, M., Boukela, L., Jelodar, H. (2021). An intelligent and blind dual color image watermarking for authentication and copyright protection. Applied Intelligence, 51: 1701-1732. https://doi.org/10.1007/s10489-020-01903-0

[61] Sharma, S., Sharma, H., Sharma, J.B., Poonia, R.C. (2023). A secure and robust color image watermarking using nature-inspired intelligence. Neural Computing and Applications, 35: 4919-4937. https://doi.org/10.1007/s00521-020-05634-8

[62] Prabha, K., Sam, I.S. (2022). Optimal blind colour image watermarking based on adaptive chaotic grasshopper optimization algorithm. The Imaging Science Journal, 70(5): 326-343. https://doi.org/10.1080/13682199.2023.2167545

[63] Hosny, K.M., Darwish, M.M. (2022). Robust color image watermarking using multiple fractional-order moments and chaotic map. Multimedia Tools and Applications, 81(17): 24347-24375. https://doi.org/10.1007/s11042-022-12282-8

[64] Hasan, N., Islam, M.S., Chen, W., Kabir, M.A., Al-Ahmadi, S. (2021). Encryption based image watermarking algorithm in 2DWT-DCT domains. Sensors, 21(16): 5540. https://doi.org/10.3390/s21165540

[65] Kazemi, M.F., Pourmina, M.A., Mazinan, A.H. (2020). Analysis of watermarking framework for color image through a neural network-based approach. Complex & Intelligent Systems, 6: 213-220. https://doi.org/10.1007/s40747-020-00129-4

[66] Garg, P., Kishore, R.R. (2020). Optimized color image watermarking through watermark strength optimization using particle swarm optimization technique. Journal of Information and Optimization Sciences, 41(6): 1499-1512. https://doi.org/10.1080/02522667.2020.1802124

[67] Yamni, M., Daoui, A., Karmouni, H., Sayyouri, M., Qjidaa, H., Wang, C., Jamil, M.O. (2023). A powerful zero-watermarking algorithm for copyright protection of color images based on quaternion radial fractional hahn moments and artificial bee colony algorithm. Circuits, Systems, and Signal Processing, 42(9): 5602-5633. https://doi.org/10.1007/s00034-023-02379-2