

Hybrid Optimization-Based Robust Watermarking Using Denoising Convolutional Neural Network

Dhiran Kumar Mahto

NIT Patna: National Institute of Technology Patna

Amit Singh (✉ amit.singh@nitp.ac.in)



NIT Patna: National Institute of Technology Patna

Research Article

Keywords: Copyright protection, Optimization, Security, Watermarking, Transform domain, DnCNN

Posted Date: November 16th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-1055534/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License. [Read Full License](#)

Abstract

Colour images have been widely used in many aspects of life; however, copyright violation issues related to these images motivate research efforts. This paper aims to develop an enhanced watermarking algorithm for producing a watermarked image using hybrid optimisation with high imperceptibility and robustness. The algorithm is based on spatial and transform domains and begins by embedding multiple secret marks into cover media using an optimal scaling factor. The multi-type mark contributes an additional level of authenticity to the proposed algorithm. Furthermore, the marked image is encrypted using an improved encryption scheme, and the denoising convolutional neural network (DnCNN) is employed to enhance the robustness of the proposed algorithm. The results reveal that the proposed watermarking algorithm yields low computational overhead, excellent watermark capacity, imperceptibility, and robustness to common filtering attacks. Moreover, the comparison shows that the proposed algorithm outperforms other competing methods.

1. Introduction

In recent years, internet-based services have been widely used, and colour images are extensively shared online as a common information carrier [1]. Online services such as social media, e-banking, e-healthcare and e-learning have become an important part of our day-to-day activities [2]. This insecure channel has been effectively used for the last few decades for the transmission of multimedia content. Internet technologies have proved to be high speed, indispensable and cost-effective at transmitting media, but, at the same time, they do not provide reliable security when transmitting such content [3]. In these circumstances, transmitting media can be risky and, due to certain security concerns, is an open issue for potential researchers to examine how to make multimedia content more secure. In general, to address these problems, robust and secure watermarking schemes have drawn the attention of the scientific community. In this scheme, digital marks are invisibly concealed into carrier media to maintain the ownership and integrity of multimedia content [4, 5]. A digital mark (s) is a data string that can be used for several purposes. Digital watermarking properties such as robustness, invisibility and embedding capacity are mutually exclusive in nature and, therefore, must be balanced to achieve high performance [6].

Optimisation-based watermarking is frequently used by researchers to manage invisibility and robustness at the same time [7–10]; however, these approaches still suffer from limited watermark capacity and security.

To overcome the issues discussed above, we have developed an enhanced watermarking algorithm for colour images. Our contributions are summarised as follows:

- 1) The fusion of spatial (magic cube) and transform domain (LWT-Schur-T-SVD) encryption methods are adopted to implement our algorithm, which embeds multiple marks. LWT examines the input in integer form and eliminates the reversibility issue of other wavelet transforms [11]. Furthermore, Schur decomposition allows for speedier and more robust watermarking [12]. The tensor SVD [13], as opposed to the traditional SVD, is used to embed watermarks for improved robustness, and a pseudo-magic cube scheme [14] is used to enhance embedding capacity.
- 2) Hybrid optimisation procedures called 'HPSOF' [15] have been designed and are employed to compute the scaling factor. A good relationship between invisibility versus robustness is maintained through the factor.
- 3) To enhance security, improved SIE scrambling [16] is used to encrypt the watermark image.
- 4) DnCNN is used on the recovered watermark image to improve the scheme's robustness [17].
- 5) Multiple marks are concealed in the host media channel to produce the final watermark. This contributes an additional authenticity to the suggested algorithm.

The remaining sections of this paper are arranged as follows: the literature review is presented in section 2; the proposed hybrid optimisation-based watermarking approach is discussed in section 3; the experimental results are presented in section 4; and the paper concludes in Section 5.

2. Related Work

In this section, a few well-known related colour image watermarking techniques are briefly discussed, and Table 1 summarises and compares the contributions of various notable methods. Sharma et al. [18] demonstrated a watermarking approach using artificial intelligence in the transform domain. To provide an additional level of security, the mark is encrypted with chaotic maps. To embed the mark, the singular score of the host media is modified with respective RGB channels of principle components of encrypted watermarks. Experiments demonstrate that the scheme is robust and secure. In [19], the author suggested spatial domain-based watermarking using Schur decomposition. This scheme has the advantages of spatial as well as transforms domain techniques, resulting in fewer computations and improved robustness; however, it has a lower embedding capacity. Sharma et al. [20] demonstrated a watermarking approach incorporating the fusion of lifting wavelet transform (LWT) and discrete cosine transform (DCT) techniques and further applied the artificial bee colony (ABC) algorithm to improve visual quality and robustness. This scheme is robust against various attacks, but a detailed security analysis needs to be conducted. Singh [21] developed a robust watermarking scheme for telehealth applications using LWT and DCT techniques. Before being concealed in the host media, the signature watermark is encrypted with message-digest (MD5) coding, and the patient report is encoded with BCH coding to enhance the robustness and privacy of the scheme; however, the scheme is less robust following a few attacks. Mohan et al. [22] developed a hybrid optimisation-based watermarking approach using an optimisation algorithm that enhances quality and robustness. Here, an additional level of security is provided by applying selective encryption to the host media at a low cost. In [23], the author implemented a spatial domain-based scheme using encryption and direct current coefficients. The mark is divided into different sub-watermarks and is then encrypted using MD5. Furthermore, the encrypted watermarks are concealed in the blue channel components. The presented scheme has improved robustness and the analysis ensures invisibility; however, the embedding capacity needs to be improved. Zear and Singh [24] suggested a hybrid watermarking scheme based on LWT-DCT-SVD to secure multimedia content. The security of the marked image and robustness of the text mark are improved by employing MD5 and Hamming error-correcting codes, respectively. The present technique is lacking in terms of BER and optimisation. Kumar and Singh [25] presented a colour image watermark in YCbCr where the embedding and extraction are processed through an alpha blending scheme in the LWT domain. Here, security is enhanced via Arnold's cat map (ACM). This scheme needs to be improved against median filter attacks. Loan et al. [26] designed a watermarking method that is applicable to both grey and colour images using DCT. The present technique uses a double layer of security by employing chaotic encryption and ACM for watermarked images. From the experimental results, it is noted that the method provides better performance in terms of security, quality and robustness; however, the complexity and cost are high. Haghghi et al. [27] implemented LWT, DCT and a feed-forward neural network-based semi-fragile scheme for temper detection and recovery. Using the inverse halftoning technique, the tempered regions are identified in the recovery stage.

Table 1
Summary of some related approaches

Scheme	Technique used	Domain	Color model	Limitations
Sharma et al. [18] scheme	Chaotic map, ABC optimization, DWT, SVD	transform	RGB	Tested with only single type watermark
SU et al. [19] scheme	Schur, Arnold transforms	Spatial	RGB	Lower Embedding capacity.
Sharma et al. [20] scheme	LWT, DCT, ABC optimization, Arnold transforms	transform	RGB	Watermark Security analysis not confirmed
Singh [21] scheme	LWT, DCT, message-digest (MD5)	transform	YIQ	Less robust against rotation and Histogram Equalization
Mohan et al. [22] scheme	DWT, SVD, HD, step space-filling curve, HPSOF	transform	YIQ	Computational analysis not confirmed
Su and chen [23] scheme	DC coefficients	Spatial	RGB	Lower embedding capacity
Zear and singh [24] scheme	LWT, DCT, SVD Hamming Error Encoder,	transform	RGB, YIQ, YCbCr	scaling factor could be determined through optimization.
Kumar and singh [25] scheme	LWT, alpha blending, Arnold cat map	transform	YCbCr	Less robust against Median-filtering attack
Loan et al. [26] scheme	DCT, Arnold transforms, chaotic encryption	transform	YCbCr	High complexity and computation.
Haghighi et al. [27] scheme	LWT, DCT, feed-forward neural network, halftoning	transform	YUV	false-positive rates for compression attack and less robust against average and median filters

3. Proposed Algorithm

In this section, the proposed algorithm, including computation of the embedding factor, the embedding and extraction phases of multiple marks, and the denoising process of recovered mark data, are described in detail. Figure 1 shows the block diagram of the proposed approach.

3.1 Watermark embedding and extraction procedure

In the embedding process, the colour host image, 'cover_img', is initially converted into red, green and blue components represented by 'Rc', 'Bc' and 'Gc', respectively.

This algorithm subsequently utilises DWT to decompose the 'Rc' component into a different sub-band and conceals the PAN number, 'PAN', in the 'HHR' sub-band of the image. Next, the account number, 'Account', is concealed in the green

channel, 'Gc', using the magic cube, 'm_cube', algorithm. Following this, the watermark image, 'w_image', is scrambled using the improved SIE scheme and is followed by the T-SVD decomposition. The blue component, 'Bc', is decomposed using the fusion of LWT, Schur and T-SVD. The resultant singular matrix, 'Sb', is altered using the scrambled watermark, 'enc_wimg', and the optimised scaling factor value, 'opt_α'. Lastly, the final watermarked image is formed by combining all three marked channels (wat_R, wat_G, wat_B). The watermark extraction procedure is the inverse of the embedding process. The complete embedding and extraction processes are explained in Algorithm 1 and Algorithm 2, respectively. Table 2 lists the specifics of the notations used in the algorithms.

Table2. Description of the notations used in the algorithms

Notation	Explanation	Notation	Explanation
cover_img	Cover image	inv_schur	Inverse schur of Inv_tsvd
w_image	watermark image	e_watermark	Extracted watermark
PAN	Permanent Account Number used for embedding as Text1 watermark	e_PAN	Extracted PAN
Account	Account Number used for embedding as Text2 watermark	e_Account	Extracted Account
opt_sf	Optimized Scaling Factor value	Rw, Gw, Bw	Red, Green and Blue channel of marked image
watermarked_img	Watermarked image	LLrw, HLrw, LHrw, HHrw	DWT coefficients of Rw channel
Rc, Gc, Bc	Red, Green and Blue channel of cover image	LLbw, HLbw, LHbw, HHbw	First level of LWT coefficients of Bw channel
LLr, HLr, L Hr, HHr	DWT coefficients of Rc channel	LLbw2, HLbw2, LHbw2, HHbw2	Second level of LWT coefficients of Bw channel
bin_PAN	Binary form of PAN	Ubw, Tcw	Schur coefficients of LLbw2 of blue channel watermarked image
wat_R, wat_G, wat_B	Watermarked Rc, Watermarked Gc and Watermarked Bc channel	Ubw, Sbw, Vbw	TSVD coefficients of Tcw
m_cube	Magic cube	ext_wS	Extracted Sw
d_wat	Decimal form of Account number	rec_img	Extracted enc_w
LLb, HLb, LHb, HHb	First level of LWT coefficients of Bc channel	e_img	Extracted encrypted image
LLb2, HLb2, LHb2, HHb2	Second level of LWT coefficients of Bc channel	Total	Number of attacks considered
Ub, Tc	Schur coefficients of LLb2 blue channel cover image	PSNR, NC, BER	Performance objective scores in ideal condition
Ub, Sb, Vb	TSVD coefficients of Tc	attack	Array of considered signal processing attacks
enc_wimg	Encrypted image of w_image	(NC [1], BER [1]), (NC [2], BER [2]) (NC [T], BER [T]))	Score of NC and BER
Uw, Sw, Vw	TSVD coefficients of enc_wimg	opt_sfv	Optimized of scaling factor value
inv_tsvd	Inverse TSVD of wat_coeff	T	Number of attacks tested
Algorithm1: Embedding algorithm		Algorithm2: Extraction algorithm	
Input: cover_img, w_image, PAN, Account, opt_sfv		Input: watermarked_image, opt_sfv	
Output: watermarked_img		Output: e_watermark, e_PAN, e_Account	
begin		begin	
Step 1: Red, Green and Blue Channels Separation of cover image		Step 1: Red, Green and Blue Channels Separation of marked image	

Notation	Explanation	Notation	Explanation
1. Rc	\leftarrow cover_img (:, :, 1);	1. Rw	\leftarrow watermarked_img (:, :, 1);
2. Gc	\leftarrow cover_img (:, :, 2);	2. Gw	\leftarrow watermarked_img (:, :, 2);
3. Bc	\leftarrow cover_img (:, :, 3);	3. Bw	\leftarrow watermarked_img (:, :, 3);
Step 2: Embedding in Red channel		Step 2: Extraction from Red channel	
4. [LLr, HLr, LHr, HHr]	\leftarrow DWT (Rc, 'Haar');	4. [LLrw, HLrw, LHrw, HHrw]	\leftarrow DWT (Rw, 'Haar');
5. bin_PAN	\leftarrow Binary (PAN);	5. e_PAN	\leftarrow Text_Extract (HHrw, len);
6. for i=1: Length (bin_PAN)	do	Step 3: Extraction from Green channel	
7. if bin_PAN [i] = 0		6. e_Account	\leftarrow extract_MagicCube (Gw, sz, NN, seed, rx, ry, rz);
8. bin_PAN [i]	\leftarrow -1;	7. e_Account	\leftarrow Decimal 2Char (e_Account);
9. end if		Step 4: Extraction from Blue channel	
10. end for		8. [LLbw, HLbw, LHbw, HHbw]	\leftarrow LWT (Bw, 'Haar');
11. len	\leftarrow Length (bin_PAN);	9. [LLbw2, HLbw2, LHbw2, HHbw2]	\leftarrow LWT (LLbw 'Haar');
12. wat_HHr	\leftarrow Embed (HHr, bin_PAN, opt_sfv, len);	10. [Ubw, Tcw]	= schur (LLbw2).
13. wat_R	\leftarrow IDWT (LLr, HLr, LHr, wat_HHr, 'Haar');	11. [Ubw, Sbw, Vbw]	\leftarrow TSVD (Tcw);
Step 3: Embedding in Green channel		12. ext_wS	\leftarrow (Sbw -Sw)/ opt_sfv;
14. d_wat	\leftarrow Char2Decimal (Account);	13. rec_img	\leftarrow Uw \times ext_wS \times Vw;
15. m_cube	\leftarrow MagicCube (θ , [rx, ry, rz]);	14. e_img	\leftarrow decrypt (rec_img);
16. wat_G	\leftarrow Text_Embedding (Gc, d_wat, m_cube);	15. e_watermark	\leftarrow DnCNN (e_img);
Step 4: Embedding in Blue channel		return e_watermark, e_PAN, e_Account	
17. [LLb, HLb, LHb, HHb]	\leftarrow LWT (Bc, 'Haar');		
18. [LLb2, HLb2, LHb2, HHb2]	\leftarrow LWT (LLb, 'Haar');		
19. [Ub, Tc]	= schur(LLb2);		
20. [Ub, Sb, Vb]	\leftarrow TSVD (Tc);		
21. enc_wimg	\leftarrow encrypt (w_image);		
22. [Uw, Sw, Vw]	\leftarrow TSVD (enc_wimg);		
23. wat_embd	\leftarrow Sb + opt_sfv \times Sw;		
24. wat_coeff	\leftarrow Ub \times wat_embd \times Vb;		
25. inv_tsvd	\leftarrow iTSVD (wat_coeff);		
26. inv_schur	\leftarrow i schur (Inv_tsvd);		
27. wat_B	\leftarrow i LWT(Inv_schur);		
28. watermarked_img	\leftarrow combine (wat_R, wat_G, wat_B);		
return watermarked_img			

3.2 Determination of optimal embedding factor value

To determine the ideal optimal embedding factor value for the embedding of multiple watermarks, the HPSOF optimisation scheme is used, which provides a well-balanced trade-off between invisibility and robustness. PSO and Firefly are swarm intelligence-based metaheuristic methods inspired by nature. To minimise the cost of complex numerical problems, Aydilek used a fusion of PSO and Firefly [15] optimisation techniques. Table 3 includes the parameters used for controlling the algorithms to produce optimal outcomes. Also, the fitness value objective function is defined as:

$$F_v = \lfloor \gamma \times \left(\frac{1}{PSNR} \right) \rfloor + \left[\left(\frac{1}{N} \times \sum_{i=1}^N \frac{1}{NC(w_image, e_watermark)} \right) \right]$$

1

Where, ' γ ' is a stabilizing factor which balances the quality and robustness effects. Algorithm 3 summarizes the complete process of determining the best scaling factor ('opt_sfv') for watermark embedding.

Algorithm3: Optimization of scaling factor
Input: cover, w_image, PAN, Account
Output: opt_sfv
begin
1 T ← Count (attack);
2 [PSNR] ← embedding_procedure (cover_img, w_image, PAN, Account);
3 [NC, BER] ← Extraction (watermarked_img);
4 for j ← Total do
5 [NC[j], BER[j]] ← extraction_procedure (watermarked_img, attack[j]);
6 end for
7 fitnessValue ← objectivefunction ((PSNR, NC, BER), (NC [1], BER [1]), (NC [2], BER [2]) (NC [T], BER [T]));
8 opt_sfv ← HPSOF (fitnessValue);
return opt_sfv

Table 3. Regulating parameter for fast convergence

Regulating Parameter	Value
Swarm count	15
Iteration's cycle	10
Lower bound (LB) value	0.005
Upper bound (UB) value	0.06
Acceleration coefficient1 value	0.5
Acceleration coefficient2 value	0.5
Dimensions	1
employed bees and Onlooker	Swarm count/ 2
Scout bees	Variable

3.3 De-noising process

DnCNN is employed to enhance the robustness and quality of the recovered watermark. To apply a pre-trained denoising convolutional neural network, the Deep Learning Toolbox is utilised. The denoising procedure for recovered data is summarised in Algorithm 4.

Algorithm4: De-noising process
Input: e_img
Output: e_watermark
Begin
1 Net=denoisingnewtork (DnCNN)
2 e_watermark =denoisingnewtork (e_img, Net)
return e_watermark

4 Experiments And Analysis

In this section, we present the performance of our proposed watermarking algorithm from several perspectives. The experiment was carried out on a 64-bit, 2.50 GHz and 8GB RAM workstation with MATLAB version R2019a. For the validation of the proposed algorithm, the Kodak [28] and USI-SIPI datasets [29] were used and are shown in Figure 2. Each test was performed on colour host images of 512×512 pixels, user PAN and account details of 80 and 96 bits, respectively, and a grey mark image of 128×128 pixels. The mark details are presented in Figure 3. To evaluate and test the proposed algorithm, we have carried out an invisibility analysis using PSNR and SSIM [2], a robustness analysis using NC and BER [2] and a differential analysis using NPCR and UACI [17].

The invisibility, robustness and security performance of the suggested method on the Kodak and USI-SIPI datasets are shown in Table 4. It is noted that the average PSNR value obtained for 40 test images is 57.7124 dB, with the highest value among them being 59.5111 dB. Additionally, the value of NC and BER is approaching 1 and 0, respectively, in all cases. The average NPCR reaches 0.9956, and the average UACI score reaches 0.2747, demonstrating the encryption

scheme's high security capabilities. Therefore, the results shown in this table are indicative of the suggested method's positive potential.

Table 4
Performance evaluation on Kodak and USI-SIPI dataset

Data set	Performance Evaluation					
Kodak dataset (15 test image)	PSNR	SSIM	NC	BER	NPCR	UACI
	56.7785	0.9912	1	0	0.9952	0.2789
	59.3307	0.9979	1	0	0.9957	0.2795
	59.0104	0.9969	1	0	0.9962	0.2692
	57.8019	0.9949	1	0	0.9960	0.2703
	58.0731	0.9941	1	0	0.9952	0.2719
	59.5111	0.9959	1	0	0.9965	0.2786
	58.5381	0.9931	1	0	0.9958	0.2707
	58.0537	0.9973	1	0	0.9962	0.2701
	57.1474	0.9900	1	0	0.9954	0.279
	58.7135	0.9949	1	0	0.9960	0.2798
	59.5084	0.9949	1	0	0.9954	0.2705
	58.3774	0.9936	1	0	0.9952	0.2713
	57.3104	0.9931	1	0	0.9953	0.2707
	58.7151	0.9929	1	0	0.9959	0.2700
58.6988	0.9961	1	0	0.9974	0.2700	
USI-SIPI dataset (25 test image)	56.8853	0.9909	1	0	0.9943	0.2773
	56.6119	0.9930	1	0	0.9954	0.2712
	57.6696	0.9964	1	0	0.9954	0.2793
	57.708	0.9930	1	0	0.9960	0.2692
	57.9544	0.9926	1	0	0.9960	0.2794
	58.2774	0.9945	1	0	0.9946	0.2782
	56.0407	0.9916	1	0	0.9948	0.2794
	57.5052	0.9954	1	0	0.996	0.2705
	56.8698	0.9931	1	0	0.9958	0.2712
	57.6771	0.9937	1	0	0.9958	0.2797
	56.7700	0.9915	1	0	0.9965	0.2791
	57.9248	0.9946	1	0	0.9955	0.2785
	58.7132	0.9954	1	0	0.9960	0.2792
	57.2670	0.9941	1	0	0.9960	0.2798
	56.8517	0.9912	1	0	0.9956	0.2703

Data set	Performance Evaluation					
	57.5918	0.9937	1	0	0.9958	0.2716
	57.2689	0.9939	1	0	0.9958	0.2700
	56.8311	0.9955	1	0	0.9960	0.2714
	58.0288	0.9935	1	0	0.9961	0.2704
	56.7045	0.9930	1	0	0.9957	0.2793
	57.9820	0.9930	1	0	0.9954	0.2796
	57.1083	0.9927	1	0	0.9953	0.2777
	57.9307	0.9952	1	0	0.9958	0.2787
	55.8526	0.9898	1	0	0.9946	0.278
	56.9056	0.9907	1	0	0.9949	0.2705
Average score of 40 test images	57.7124	0.9937	1	0	0.9956	0.2747

Furthermore, to quantify the results, the NC and BER are evaluated for different kinds of attacks, and the average scores are shown in Figure 4 and Table 5, respectively, for 40 test images using the Kodak and USI-SIPI datasets. From Figure 4, it is noted that the satisfactory score of NC, i.e. $NC \geq 0.7863$, is achieved for all considered attacks except the cropping attack. Similarly, the average BER is shown in Table 5 for the same set of dataset images. The average BER score achieved is zero, except for a few attacks (i.e. median filtering, resize and cropping).

Table 5
Average BER score on Kodak and USI-SIPI dataset

Attack	Average BER
No attack	0
Speckle (0.01)	0
Salt and Pepper (0.005)	0
Salt and Pepper (0.01)	0
Median filter [1, 1]	0
Median filter [2, 2]	41.6192
Histogram Equalization	0
Gaussian attack (0.001)	0
Sharpening Mask (0.1)	0
JPEG Compression (QF=90)	0
Resize [512-1024-512]	0
Resize [512-256-512]	42.3123
Cropping [20 20 400 480]	40.4333

PSNR and NC scores are recorded in Table 6 and Figure 5, respectively, and, compared with several other related methods, it can be observed from Table 6 that the achieved PSNR score outperforms the recent methods. Similarly, from Figure 5, it can be noted that our average NC performs well apart from the cropping attack.

Table 6
Comparison in terms of PSNR

PSNR (in dB)					
<i>Xu et al.</i> [13]	<i>Sharma et al.</i> [18]	<i>Swaraja et al.</i> [30]	<i>Mohan et al.</i> [31]	<i>Sinhal et al.</i> [32]	Average PSNR score (Proposed algorithm)
39.09	47.6391	36.99	55.1471	40.13	57.7124

Additionally, to validate the embedding capacity and quality of our proposed method, PSNR scores are recorded in Table 7. It can be observed that the PSNR score of > 51 dB is achieved after embedding up to 80,000 characters at different gain factor values. The average time cost evaluation for 40 test images is recorded in Table 8. The average embedding and extraction overhead are 0.177687 and 0.087648 seconds, respectively. Similarly, the average encryption time cost is 0.013705, and the average decryption time cost is 0.00485 seconds. Table 8 clearly indicates that the execution overhead of the proposed method is acceptable.

Table 7
The PSNR results using different character length

Gain factor	PSNR (in dB)							
	500 characters	1000 characters	2000 characters	5000 characters	10000 characters	20000 characters	40000 characters	80000 characters
0.01	57.9955	57.908	57.751	57.3017	56.6525	55.5715	54.0235	51.9423
0.05	57.8527	57.7616	57.6296	57.1808	56.5522	55.5032	53.9494	51.9106
0.1	57.4713	57.3899	57.2425	56.8392	56.2462	55.2739	53.7900	51.8026
0.06	57.7939	57.6976	57.5643	57.1250	56.5097	55.4612	53.9274	51.8993

Table 8
Average execution overhead

Process	Time (in seconds)
	Cover/Watermark size [512 x 512]/ [128 x 128]
Embedding	0.177687
Extraction	0.087648
Encryption	0.013705
Decryption	0.00485

5. Conclusions

A secure colour image watermarking algorithm with improved invisibility, robustness and capacity has been proposed in this paper. In the suggested algorithm, embedding is performed in the spatial and transform domains. Initially, the host colour image is divided into red, green and blue channels. Then, multiple-mark information is concealed in all three channels for different purposes. A trade-off between invisibility and robustness was analysed by fusing PSO and Firefly algorithms. To evaluate the performance of the proposed work, invisibility, robustness and security analyses were performed against various attacks. A detailed comparison was also made, demonstrating how the proposed research is better than the existing algorithms. In the future, we would like to explore the concepts of encryption and compression-based watermarking, thereby making our system more efficient for other media applications.

Declarations

Authors' contribution Both authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by both authors. The first draft of the manuscript was written by Dhiran Kumar Mahto and Amit Kumar Singh commented on previous versions of the manuscript. Both authors read and approved the final manuscript.

Funding This work has no funding resource.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Consent of publication Not applicable.

References

1. Sun W, Zhou J, Li Y, Cheung M, She J (2020) Robust High-Capacity Watermarking over Online Social Network Shared Images. *IEEE Transactions on Circuits and Systems for Video Technology*
2. Mahto DK, Singh AK (2021) A survey of color image watermarking: State-of-the-art and research directions. *Computers & Electrical Engineering*, 93, p.107255
3. Urquhart L, McAuley D (2018) Avoiding the internet of insecure industrial things. *Computer law & security review* 34(3):450–466
4. Anand A, Singh AK (2020) Watermarking techniques for medical data authentication: a survey. *Multimedia Tools and Applications*, pp 1–33
5. Singh AK, Kumar B, Singh G, Mohan A (eds) (2017) "Medical image watermarking: techniques and applications". Springer
6. Singh OP, Singh AK, Srivastava G, Kumar N (2020) "Image watermarking using soft computing techniques: A comprehensive survey," *Multimed. Tools Appl.* pp.1–32,
7. Cheema AM, Adnan SM, Mehmood Z (2020) A Novel Optimized Semi-Blind Scheme for Color Image Watermarking. *IEEE Access* 8:169525–169547
8. Pandey MK, Parmar G, Gupta R, Sikander A (2020) Lossless robust color image watermarking using lifting scheme and GWO. *International Journal of System Assurance Engineering and Management* 11(2):320–331
9. Moosazadeh M, Ekbatanifard G (2019) A new DCT-based robust image watermarking method using teaching-learning-based optimization. *Journal of Information Security and Applications* 47:28–38

10. Ahmadi SBB, 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(3):1701–1732
11. Verma VS, Jha RK, Ojha A (2015) Significant region based robust watermarking scheme in lifting wavelet transform domain. *Expert Syst Appl* 42(21):8184–8197
12. Mohan BC, Swamy KV (2010) On the use of Schur decomposition for copyright protection of digital images. *International Journal of Computer and Electrical Engineering* 2(4):1793–8163
13. Xu H, Jiang G, Yu M, Luo T (2018) A color image watermarking based on tensor analysis. *IEEE Access* 6:51500–51514
14. Ranjani JJ, Zaid F (2021) Pseudo magic cubes: A multidimensional data hiding scheme exploiting modification directions for large payloads. *Comput Electr Eng* 89:106928
15. Aydilek IB (2018) A hybrid firefly and particle swarm optimization algorithm for computationally expensive numerical problems. *Appl Soft Comput* 66:232–249
16. Kumar S, Bhatnagar G (2019) SIE: An application to secure stereo images using encryption. *Handbook of Multimedia Information Security: Techniques and Applications*. Springer, Cham, pp 37–61
17. Singh OP, Singh AK (2021) Data hiding in encryption–compression domain. *Complex & Intelligent Systems*, pp 1–14
18. Sharma S, Sharma H, Sharma JB, Poonia RC (2021) A secure and robust color image watermarking using nature-inspired intelligence. *Neural Computing and Applications*, pp 1–19
19. Su Q, Yuan Z, Liu D (2018) An approximate Schur decomposition-based spatial domain color image watermarking method. *IEEE Access* 7:4358–4370
20. Sharma S, Sharma H, Sharma JB (2021) Artificial bee colony based perceptually tuned blind color image watermarking in hybrid LWT-DCT domain. *Multimedia Tools and Applications* 80(12):18753–18785
21. Singh AK (2019) Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image. *Multimedia Tools and Applications* 78(21):30523–30533
22. Mohan A, Anand A, Singh AK, Dwivedi R, Kumar B (2021) Selective encryption and optimization-based watermarking for robust transmission of landslide images. *Computers & Electrical Engineering*, 95, p.107385
23. Su Q, Chen B (2018) Robust color image watermarking technique in the spatial domain. *Soft Comput* 22(1):91–106
24. Zear A, Singh PK (2021) Secure and robust color image dual watermarking based on LWT-DCT-SVD. *Multimedia Tools and Applications*, pp.1-18
25. Kumar S, Singh BK (2021) An improved watermarking scheme for color image using alpha blending. *Multimedia Tools and Applications* 80(9):13975–13999
26. Loan NA, Hurrah NN, Parah SA, Lee JW, Sheikh JA, Bhat GM (2018) Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access* 6:19876–19897
27. Bolourian Haghighi B, Taherinia AH, Monsefi R (2020) An effective semi-fragile watermarking method for image authentication based on lifting wavelet transform and feed-forward neural network. *Cognitive Computation* 12:863–890
28. Kodak dataset at <https://www.kaggle.com/sherylmehta/kodak-dataset>
29. USI-SIPI dataset <http://sipi.usc.edu/database/>
30. Swaraja K, Meenakshi K, Kora P (2020) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. *Biomedical Signal Processing and Control*, 55, p.101665
31. Mohan A, Anand A, Singh AK, Dwivedi R, Kumar B (2021) Selective encryption and optimization based watermarking for robust transmission of landslide images. *Computers & Electrical Engineering*, 95, p.107385

Figures

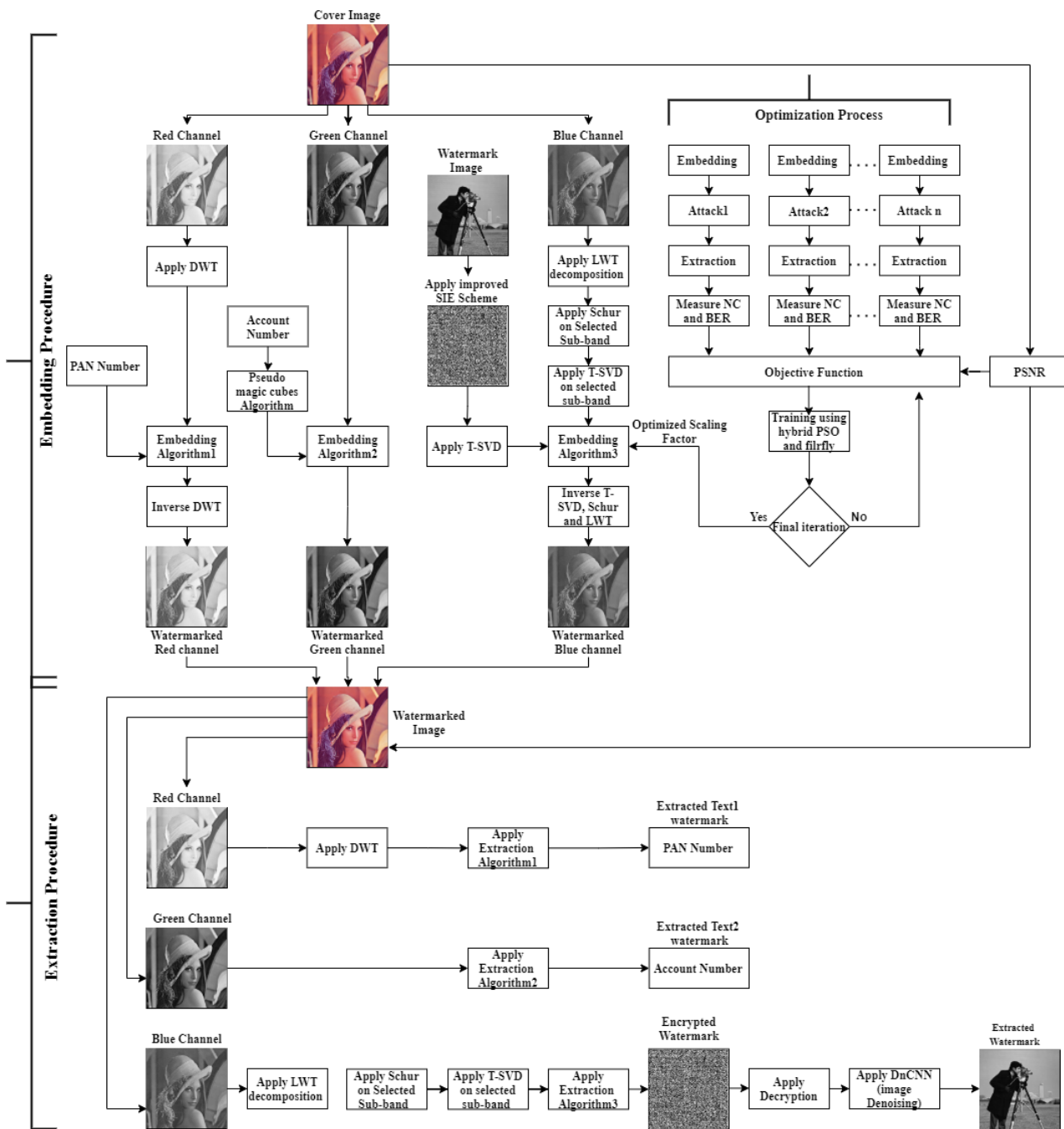


Figure 1

The proposed watermark algorithm

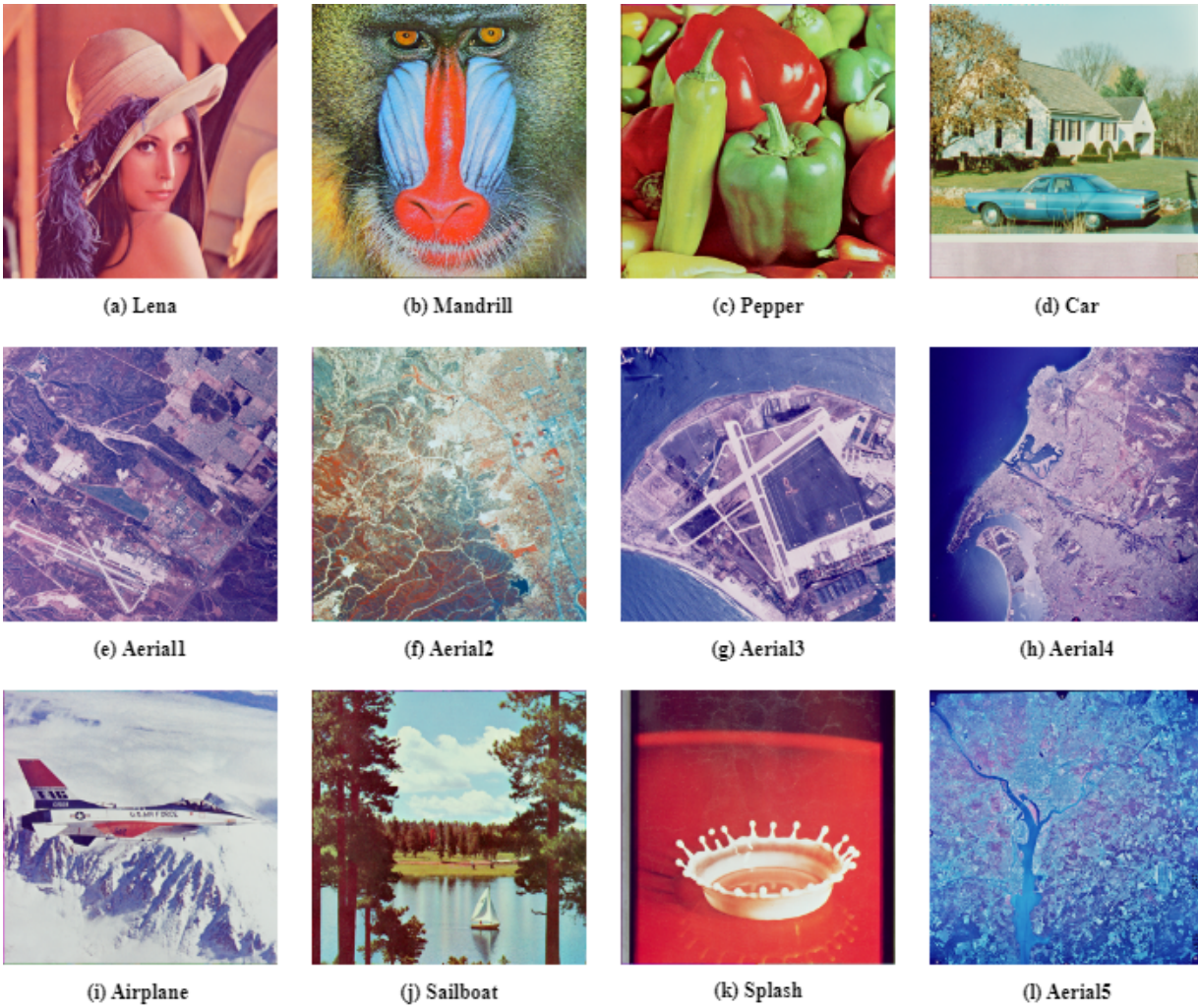


Figure 2

Used some of the test dataset Host images

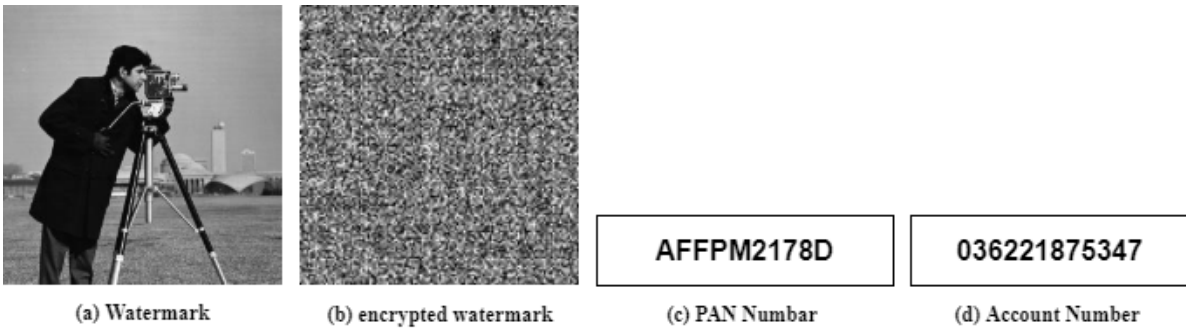


Figure 3

Used watermarks

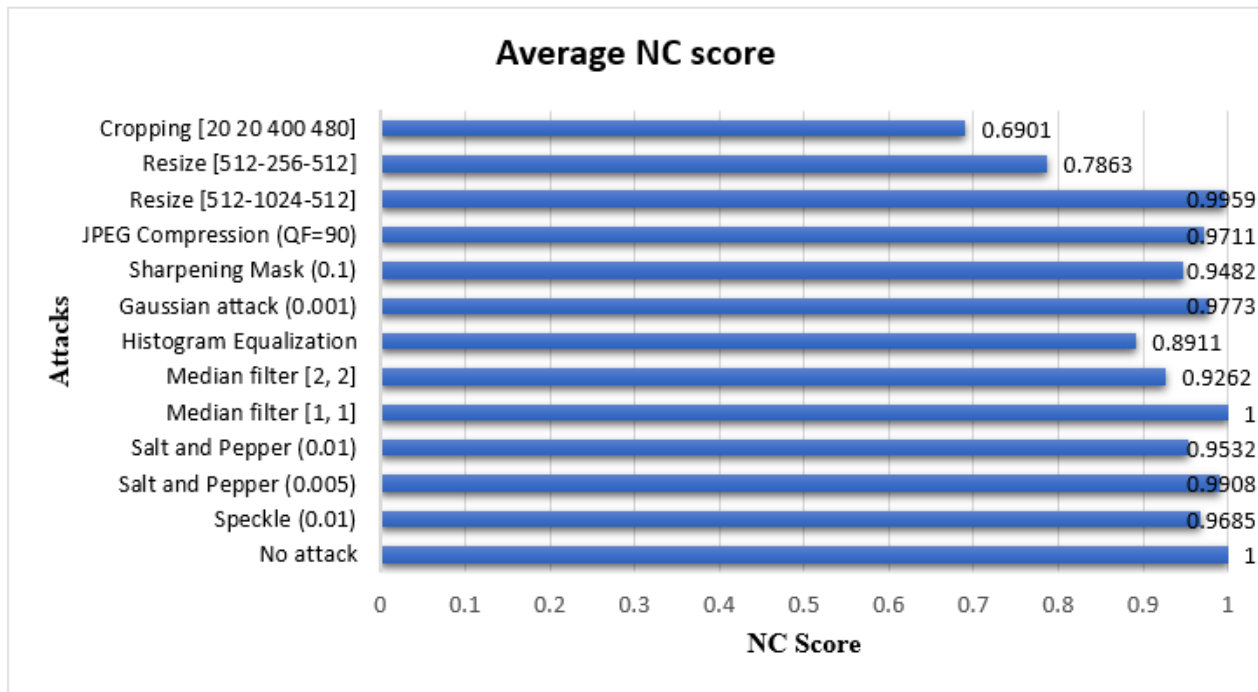


Figure 4

Average NC score on Kodak and USI-SIPI dataset