



Optimized and secure digital image watermarking technique using Henon mapping in redundant domain

Chandan Kumar¹

Received: 7 January 2022 / Revised: 16 January 2024 / Accepted: 12 February 2024

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract

Nowadays, there is huge requirement of processed data that can be transmitted from one location to another. However data transmission over open channel faces various security related threats. So securing the data is first basic need for successful communication over unsecure channel. One of trusted method to secure the content is digital image watermarking. Digital watermarking secures the contents (audio, video and images) from unauthorized user by embedding secret information inside it. So, possible attacks can be detected by checking the degradation of embedded information. This work presents an optimized digital image watermarking solution using the Dragonfly optimization algorithm for an optimum scaling factor. It employs NSCT, RDWT, and MSVD transformations on the cover image, embedding watermarks in the appropriate band. Security is enhanced using the Henon Map encryption algorithm. Evaluation across diverse cover images demonstrates superior results in invisibility, security, robustness, and embedding capacity for copyright protection.

Keywords RDWT · Non-subsampled contourlet transform · MSVD · Arnold transform · Dragon fly optimization

1 Introduction

Internet and digital image processing mutually has contributed to distribution of digital content over network. But duplication, unauthorized copying, modification and reproducing of data are some major issues lead to privacy and security problems. So protecting the content is major requirement for data security over various networks. There is urgent need to provide security of content against unauthorized users/persons [1]. Digital watermarking is confirmed to be best technique to secure digital data by embedding secret information inside it, So later it can retrieved by authorized persons/users intended to use for it. Robustness, imperceptibility and capacity are the major requirement of watermark [2]. So watermark should not be tampered or altered by any

✉ Chandan Kumar
chandansharmahmr@gmail.com

¹ Department of CSE, Career Point University Hamirpur, Hamirpur, Himachal Pradesh, India

unauthorized person [3]. To make image more secure, two different kinds of watermarks are embedded inside it so that robustness and security can be maintained. This type of scheme is known as multiple watermarking systems. Main motive to design such type of method is to provide better protection against tamper-resistance, intellectual property ownership and securing multimedia documents. Digital watermark can be in form of image, audio or video. Further watermark should wear all common watermarking attacks without losing invisibility. So based on all discussed point or need, we have introduced multiple watermarking technique by using optimization and security technique.

Here, proposed method includes following contributions:

- Using combination of NSCT, RDWT and SVD all together make the technique robust and invisible. RDWT is better than DWT due to shift invariance nature of image. Moreover NSCT provide rich directionality for better reconstruction of images [4].
- Combined embedding of different kind of watermarks together in same image provide better identity authentication [5, 6].
- Dragonfly algorithm is based on behavior of dragon fly. It starts with set of random solutions and to optimize the solutions. There are five stages in dragon fly life span, separation, alignment, cohesion, attraction towards food and disruption from the enemies [7]. Stages are as follow:

Different stages in Dragonfly algorithm are:

Alg. 1: Optimization of embedding factor

a. **Separation**

The separation of N swarms is the sum of the separation and the current individual and jthneighbor. It can be computed using equation (1).

$$R_i = - \sum_{j=1}^N X - X_j \quad (1)$$

b. **Alignment:**

The swarms align together to move forward collectively. The velocity of each swarm matches with the velocity (V) of the others.

$$A_i = \frac{\sum_{j=1}^N V_j}{N} \quad (2)$$

A_j is the velocity of jth neighbor.

c. **Cohesion: Attraction force of swarms toward the center**

$$C_i = \frac{\sum_{j=1}^N V_j}{N} - X \quad (3)$$

d. **Attraction towards food:** All the swarms get attracted towards the food (F). This is represented in Eq. (4).

$$X_i = X^+ - X \quad (4)$$

e. **The distraction outward toward an enemy is**

$$G_i = X^- + X \tag{5}$$

X^- is the position of enemy.

Using these five parameters given in Eq. (1) to (2) the exploration and exploitation can be achieved. The proper tuning of all these parameters results into the optimal solution. Thus, the step vector and position for dragon flies is computed using eq.(vi) and (vii) respectively.

$$dx_{t+1} = (rR_i + aA_i + xX_i + cC_i + gG_i) \tag{6}$$

$$X_{t+1} = X_{t+1} + dx_{t+1} \tag{7}$$

In the above equation t is the iteration count and i represent the i th fly. If a dragon fly does not has any neighbor then the levy flight is used to update the position as given in Eq. (8).

$$X_{t+1} = X_t + Levy(d) \times X_t \tag{8}$$

Where $Levy(X) = 0.01 \times \frac{u1 \times \alpha}{|u2|^{\frac{1}{\beta}}}$

$u1$ and $u2$ are randomly selected numbers in the range $[0, 1]$, β is a constant

$$\alpha = \left(\frac{\mathcal{E}(1+\beta) \times \sin\left(\frac{\pi\beta}{2}\right)}{\mathcal{E}\left(\frac{1+\beta}{2}\right) \times \beta \times 2 \left(\frac{\beta-1}{2}\right)} \right)^{\frac{1}{\beta}} \tag{9}$$

Where $\mathcal{E}(x) = (x - 1)!$ – Arnold scrambling scheme is used to provide additional confidentiality of the data [8]. Recovery of mark data is not possible even it is extracted by unauthorized persons.

- MSVD provides a replacement of wavelet filter bank. Compared to other decomposition MSVD require fewer computations. MSVD do not have basic function similar to other transformation, but its decomposition depends upon the dataset used [9].
- Finally, the suggested scheme outperforms the typical watermarking schemes in the aspect of robustness to common attacks, while it offers the invisibility, capacity and security of the media data at the same time.

Remaining paper is organized in following way: Section 2 describes the review of literature of related technique. Section 3 describes the procedure of watermark embedding, extraction, optimization for both watermarks. Result outcomes are represented in Section 4. Finally, conclusion and future plan are discussed in Section 5.

2 Literature survey

Some related watermarking schemes are discussed below.

Digital image watermarking technique using DWT, DCT and SVD is developed by Kumar et al. [10]. Firstly, reference image is calculated by finding out the contrast and threshold value of image. Further properties of original image are extracted using reference

image. Finally, mark is embedded using appropriate watermark strength which is produced by fuzzy logic system. Further, technique is also tested using Logic genetic algorithm. Scheme is noted to be robust and imperceptible due to selection of appropriate embedding strength. A hybrid robust watermarking method is introduced by Garg et al. [11]. Further, artificial bee colony (ABC) optimization is applied. Initially, DWT(1st level) decomposes cover image followed by application of DCT on cover image. Further, watermark is decomposed by DCT. Finally secret data is embedded using optimized embedding factor obtained using ABC (artificial bee colony). Performance of algorithm is calculated by various parameters. Experimental values show that PSNR is more than 40 and $NC > 0.9$ against most of common watermarking attacks. Begum et al. [12] has introduced hybridized image watermarking scheme using DCT, DFT, DWT and SVD. Further, encryption technique is applied on watermark before dividing into n-blocks. Furthermore, encrypted blocks of watermark are inserted into randomly selected n number of blocks for cover images. Finally, application of inverse transforms result into watermarked image. However, reverse of scheme leads to watermark recovery. Deeba et al. [13] has introduced a watermark method using discrete cosine transform(DCT) in sparse domain. Initially watermark is transformed by DCT. Here watermark is transformed by DCT. Further, best embedding position is find out by using K-SVD algorithm. Finally, DCT information of watermark is inserted into selected sparse coefficient of cover image. It has been observed that performance of technique is up to mark against various checkmark attacks. A stationary wavelet transform (SWT) based digital watermarking technique is described by Pourhadi et al. [14]. Further watermark is embedded based on the optimized value calculated using combine use of Bat optimization algorithm (BAT) and Speed up Robust Feature (SURF). Zhang et al. [15] introduced a robust secure watermarking method using discrete cosine transform(DCT), multi-level discrete wavelet transform(DWT) and Particle swarm optimization (PSO). Initially watermark is scrambled by Arnold transform technique. Then cover image and encrypted watermark are decomposed by multilevel DWT and DCT. Further, low and high frequency sub bands are selected to embed singular values. This technique is found to be better in term of high capacity and robustness along with imperceptibility. Amiri et al. [16] has proposed image securing method using non subsampled counterlet transform(NSCT) and stationary wavelet transform(SWT) along with singular value decomposition(SVD). Further, scaling factor is evaluated using particle swarm optimization (PSO). Firstly host image is diffused using NSCT followed by SWT. Then, SVD is applied to evaluate singular value. However watermark is decomposed by SWT before applying SVD. Finally, process of watermark embedding takes place using optimized scaling factor. A hybrid technique using DWT, DCT along with Fuzzy-BPN is introduced by Agarwal et al. [6]. Firstly, 8×8 block size of host image is selected to find out the DCT component. Next, luminance and contrast sensitivity for the same is evaluated. Permuted watermark is embedded into 3rd level DWT component of cover image. Further, robustness is measured against eight different watermarking attacks. Method is found robust against attacks. Furthermore scheme is less complex in term of watermark processing. In [17], author has developed a multiple image watermarking technique in transform domain. Embedding of two watermarks inside cover image result into enhanced security. Further, text watermark is encrypted before embedding process. Algorithm is found robust against various considered attacks. A watermarking method using scale invariant feature transform(SIFT) in NSCT domain is introduced by Hua et al. [18]. Initially, feature point having high variance for cover image is selected for embedding watermark into cover image. Further method is found to be better capture quality and temper resistance against common watermarking attacks. A DWT based watermarking scheme is introduced by

Meenpal [19]. Further SPIHT technique helps to detect suitable coefficients for imperceptible embedding of watermark. Further, security of technique is enhanced using Arnold transform. On the basis of obtained experiments results, it has been found that technique is robust against common watermarking attacks. Further, method provides better tradeoff against robustness, imperceptibility and security. Wang et al. [20] has described watermarking method using bandelet transform(BT)in NSCT domain. Further, performance of method is checked under four grey scale and eight color images. Furthermore, technique is found to be imperceptible and having better visual quality. This study addresses the challenges of imperceptibility, robustness, security, and capacity in digital image watermarking. The proposed intelligent hybrid method employs Contourlet Transform (CNT) for frequency domain transfer, SVD transformation, and dynamic scaling factors determined by PSO for enhanced robustness without compromising transparency. A novel approach is introduced to bolster security and mitigate the False Positive Problem (FPP) in SVD-based watermarking. Experimental results showcase excellent imperceptibility (PSNR 57.31 dB), notable robustness against diverse attacks, ample capacity, and enhanced security, all without false positive detection errors [21]. In addressing multimedia security concerns, this paper [22] presents an efficient hybrid digital image watermarking scheme employing two stages of Singular Value Decomposition (SVD). The embedding stage utilizes SVD followed by block-based SVD (B-SVD), while the extraction stage relies on SVD on the entire image and B-SVD. The proposed scheme enhances watermarking requirements, increases capacity, and improves watermark detection, robustness, and security. Performance evaluation based on correlation coefficient (Cr) and Peak Signal-to-Noise Ratio (PSNR) demonstrates the scheme's effectiveness with Cr reaching 0.9975 and PSNR at 45.8605. Comparative analysis underscores its superiority over recent schemes in terms of security and performance under attacks. In this paper [23], the utilization of Deep Neural Networks (DNNs) has surged across various domains, prominently in Computer Vision (CV). Particularly in the realm of Medical Image Analysis, DNNs have proven instrumental. However, the susceptibility to adversarial attacks poses a substantial threat to the robustness of vision systems. This paper explores a unique facet of digital watermarking, presenting it as a potential black-box adversarial attack, and termed watermarking attacks. The study underscores the risks posed by widespread watermark use for security purposes to vision systems. The moment-based local image watermarking method is applied to MRI, CT-scans, and X-ray images. Testing on leading CV models, including DenseNet 201, DenseNet169, and MobileNetV2, reveals the proposed attack achieving over 50% success, unveiling the potential vulnerabilities in current vision systems against watermarking attacks. This paper [24] addresses the challenge of poor robustness in medical image watermarking against geometric attacks. It introduces a zero watermarking algorithm based on KAZE-DCT for enhancing the security of medical images. The approach involves extracting feature vectors using KAZE-DCT, obtaining feature sequences through perceptual hashing, and encrypting multi-watermark images using chaotic mapping. The zero watermarking technology is then applied for watermark embedding and extraction. The algorithm demonstrates effective watermark extraction and exhibits robustness against common and geometric attacks, as evidenced by experimental results. This paper [25] introduces a novel watermarking technique for digital images using convolutional neural networks (CNNs). The approach involves extracting latent features from cover and secret images through an encoder network, concatenating them to create a marked image. On the receiver side, a de-noising auto encoder network removes noise variations from the received image and extracts the secret mark image using a CNN. The proposed technique achieves imperceptible hiding of images and demonstrates superior performance in terms of visual quality

and robustness compared to state-of-the-art schemes, as evidenced by simulation results and performance comparisons.

3 Proposed method

Here, all the process is divided into three sections: Searching for optimal embedding factor, embedding and security and finally recovery and decryption process. All the process in described in alg1 to alg3 (Fig. 1).

Alg. 1: Optimization of embedding factor (α)

Optimization of scaling factor is calculated using Eq. (1-9).

Alg. 2: Embedding of marks data

Embedding procedure:

1. Segmentation applied to host image (HI) (dimension: 512×512)

$$\begin{aligned} W_1 &= R(2z - 1, 2\pi - 1) \\ W_2 &= R(2z - 1, 2\pi - 1) \\ W_3 &= R(2z - 1, 2\pi - 1) \\ W_4 &= R(2z - 1, 2\pi - 1) \end{aligned} \quad (10)$$

where $z' = 1, 2 \dots \dots, X/2$ and $\pi' = 1, 2, \dots \dots, X/2$.

2. NSCT applied on maximum entropy ('W') segment of image.

$$[W_{U1}, W_{U2}, W_{U111}, W_{U112}, W_{U121}, W_{U122}] \leftarrow \text{NSCT}[W] \quad (11)$$

Where W_{U1}, W_{U2} is low frequency sub-bands and $W_{U111}, W_{U112}, W_{U121}, W_{U122}$ are high frequency sub-bands.

3. W_{U121} is selected for RDWT 1st level transform

$$[W_{A1}, W_{H1}, W_{V1}, W_{D1}] \leftarrow \text{RDWT}[W_{S121}] \quad (12)$$

Here

W_{A1}, W_{H1}, W_{V1} and W_{D1} are the RDWT sub-bands.

4. Singular vector calculation:

$$\begin{aligned} [U_{WA1}, S_{WA1}, V_{WA1}] &\leftarrow \text{SVD}[W_{A1}] \\ [U_{WH1}, S_{WH1}, V_{WH1}] &\leftarrow \text{SVD}[W_{H1}] \end{aligned} \quad (13)$$

5. QR encoding on adhar card number watermark

$$SW2 \leftarrow \text{Rencoding}(\text{adhar card number}(\text{watermark})) \quad (14)$$

6. NSCT decomposition (1st level) on watermark SW1 & SW2

$$\begin{aligned} [P1_{T1}, P1_{T2}, P1_{B111}, P1_{B112}, P1_{B121}, P1_{B122}] &\leftarrow \text{NSCT}[SW1] \\ [P2_{T2}, P2_{B111}, P2_{B112}, P2_{B121}, P2_{B122},] &\leftarrow \text{NSCT}[SW2] \end{aligned} \quad (15)$$

7. $P1_{B121}$ and $P2_{B121}$ (1st level RDWT transform)

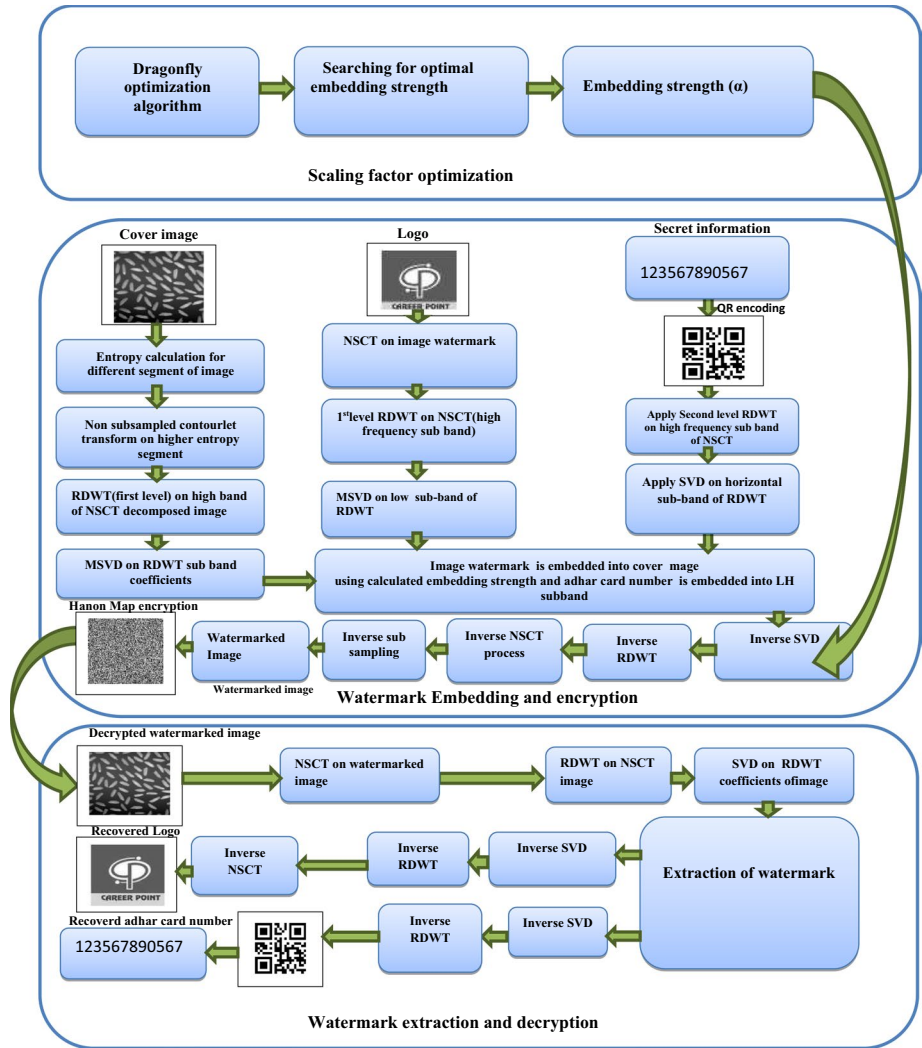


Fig. 1 Watermark (a) embedding (b) extraction process

$$\begin{bmatrix} P1_{A1}, P1_{H1}, P1_{V1}, P1_{D1} \\ P2_{A1}, P2_{H1}, P2_{V1}, P2_{D1} \end{bmatrix} \leftarrow RDWT \begin{bmatrix} P1_{B121} \\ P2_{B121} \end{bmatrix} \tag{16}$$

Where $P1_{A1}, P1_{H1}, P1_{V1}, P1_{D1}$ and $P2_{A1}, P2_{H1}, P2_{V1}, P2_{D1}$ are sub-bands of SW1 and SW2 respectively.

- Singular vector of $P1_{A1}$ and $P2_{H1}$.

$$\begin{bmatrix} U_{P1A1}, S_{P1A1}, V_{P1A1} \\ U_{P2H1}, S_{P2H1}, P_{P2A1} \end{bmatrix} \leftarrow SVD \begin{bmatrix} P1_{A1} \\ P2_{H1} \end{bmatrix} \tag{17}$$

9. Embedding process for both watermarks as

$$S_{11} = W_{MA1} + z \times S_{P1A1} \quad (18)$$

$$S_{22} = W_{MH1} + z \times S_{P2H1} \quad (19)$$

10. Inverse SVD, RDWT, NSCT and sub-sampling operation are applied which result into watermarked image (W_s).
11. Watermarked image is encrypted using Henon Map encryption.

$$W_s \rightarrow W_R$$

Alg. 3: Recovery of marks data

- Sub-image with maximum entropy (I_X) is selected from watermarked image ' W_R '.
- NSCT on I_X :

$$[I_{X1}, I_{X2}, I_{XB111}, I_{XB112}, I_{XB121}, I_{XB122}] \leftarrow \text{NSCT}[I_X] \quad (20)$$

Where

I_{X1}, I_{X2} : Low frequency sub band.

$I_{XB111}, I_{XB112}, I_{XB121}, I_{XB122}$: Sub-band with high frequency.

- 1st level RDWT decomposition

$$[I_{XA1}, I_{XH1}, I_{XV1}, I_{XD1}] \leftarrow \text{RDWT}[I_{XB121}] \quad (21)$$

- SVD for I_{XA1} and I_{XH1}

$$\begin{aligned} [U_{IXA1}, S_{IXA1}, V_{IXA1}] &\leftarrow \text{SVD}[I_{XA1}] \\ [U_{IXH1}, S_{IXH1}, V_{IXH1}] &\leftarrow \text{SVD}[I_{XH1}] \end{aligned} \quad (22)$$

- Recovery of both watermarks

$$\begin{aligned} R_{G1} &= (S_{IXA1} - S_{WA1}) / z \\ R_{G2} &= (S_{IXH1} - S_{WH1}) / z \end{aligned} \quad (23)$$

- Inverse R_{G1} and R_{G2} .

- Watermark1 (RW1) & watermark2 (RW2) recovered using inverse of RDWT and NSCT.

4 Experimental outcomes

In our work, one cover image 'rice.bmp' (https://www.bing.com/images/search?q=baboon%20watermark&qs=n&form=QBIR&qft=%20filterui%3Alicense-L2_L3_L4&sp=-1&pq=baboon%20watermark&sc=1-16&cvid=CD8F7EB89C4E4918A02268D75138377D&first=1&tsc=ImageBasicHover) of size '512 × 512'. Two watermark images 'cpuh.bmp' (<http://www.cpuh.in>) having size and Adhar card number having size '256 × 256' and '128 × 128' respectively are considered for experiment. Performance is evaluated with peak signal to noise ratio (PSNR) [26], normalized correlation (NC)

[26]. All the experiments are performed using MATLAB 16a. PSNR evaluate the alteration between original cover image and marked data. NC value finds out the robustness by measuring resemblance between the original and recovered mark images. Notation for watermarks is denoted as NC(1) and NC(2) respectively. Pictorial representation of host, watermarks and marked image is represented in Fig. 2. Encrypted and recovered marked image is shown in Fig. 3. However Extracted watermarks are shown in Fig. 4. Further, performance evaluation based on various attack is shown in Fig. 5. Experimental results are presented in Tables 1, 2, 3, 4 and 5. Performance of technique under various cover images is shown in Table 1. Highest value of PSNR is 51.2967 dB against NC, NPCR, UACI and SSIM [27] having values 0.9802, 0.9962, 0.282 and 0.999862 respectively. Performance of technique against various filters is represented in Table 2. It has been observed that the best value of NC is 1 under almost all filters. Further robustness comparison of method is represented in Table 3. Under salt and pepper attack, our best value obtained is 0.9999 as compared to techniques [27–30] having values 0.851,0.98,0.9962 respectively. Further, under Gaussian Blur attack, proposed techniques has bestvalue is 0.9988 as compared to other compared technique [27–30] having values 0.994,0.9906,0.96,0.9999respectively. Further under median filter, best value is obtained as 0.9968. Next, techniques [27–30] has obtained values as 0.883,0.9892,0.998 respectively against JPEG compression(QF=25). However, we have achieved better value ie. 0.996 against same attacks. Further, under histogram equalization we have obtained best value as 0.9958 as compared to other techniques [27–30] having values 0.9654 and 0.998. We have best NC value for cropping(12%) is 0.9999 as compared to

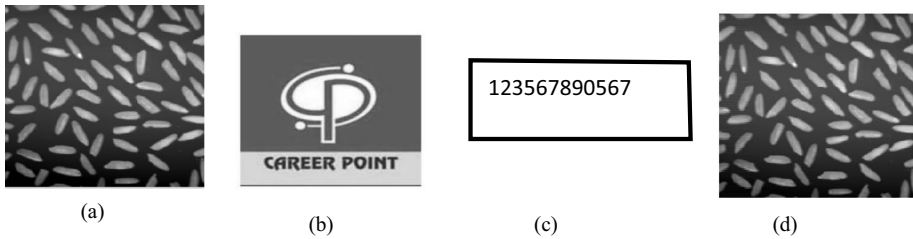


Fig. 2 a Cover image b Image watermark c adhar card number d Watermarked image

Fig. 3 a Encrypted watermarked image b Decryptedwatermarked image

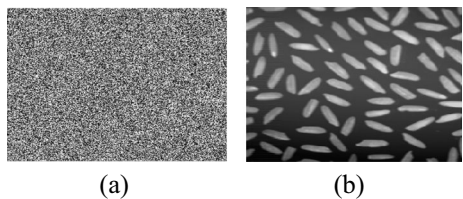
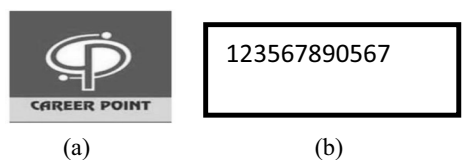


Fig. 4 Extracted (a) logo and (b) adhar card number



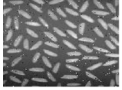


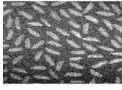


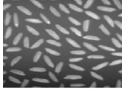


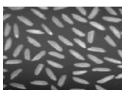


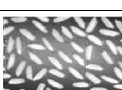





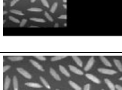
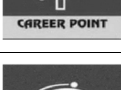

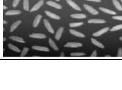
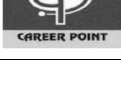




Attack	Attacked Watermarked image	Recovered Logo watermark	Secret Information	QR code for secret information
Salt and pepper noise(density=0.01)			123567890567	
Gaussian noise(mean=0,variance=0.01)			123567890567	
Median Filter Attack[2 2]			123567890567	
JPEG compression(QF=50)			123567890567	
Histogram equalization			123567890567	
Cropping(20 20 400 480)			123567890567	
Speckle noise(Density=0.05)			123567890567	
Average filtering			123567890567	
Noise and cropping			123567890567	

Fig. 5 Attacked watermarked and extracted watermarks

other compared technique [27–30] having value 0.9984. Further, we have best NC values for speckle noise and average filtering are 0.9999 and 0.9998 respectively. Under rotation attack we have value as 0.9989 as compared to other method [27–30] having NC values 0.832, 0.9973 respectively. Finally under scaling attack, we have also achieved better

Table 1 Performance of method against various cover images

Cover images	PSNR (in dB)	NC	NPCR	UACI	SSIM
MRI	45.0480	0.9905	0.9963	0.3888	0.999538
Barbara	38.5351	0.9579	0.9959	0.2935	0.998344
Baboon	39.2598	0.9762	0.9960	0.3188	0.994863
Boat	37.4686	0.9739	0.9739	0.2825	0.997180
Finger	32.6538	0.8253	0.9959	0.2783	0.985436
Bird	48.1977	0.9913	0.9961	0.2995	0.999988
Cameraman	33.7523	0.9493	0.9963	0.3459	0.998176
Coins	42.4327	0.9397	0.9961	0.3063	0.999561
Moon	47.0226	0.9899	0.9954	0.4286	0.998854
Tire	45.5276	0.9901	0.9964	0.3938	0.998753
Rice	51.2967	0.9802	0.9962	0.2823	0.999972

Table 2 Performance of method against various filters

Filters	PSNR (in dB)	NC(1)	NC(2)	SSIM
Sym4	34.63	0.9998	0.9549	0.995285
db4	34.61	1	0.9552	0.995265
Bior 4.4	36.37	0.9976	0.9547	0.997038
Coif4	34.82	0.9978	0.9575	0.995498
Bior6.8	36.16	1	0.9576	0.996742
dmey	35.45	0.9990	0.9539	0.996132
haar	35.54	0.9888	0.9423	0.996211

performance than other compared technique [27–30]. Tables 4 and 5 represent NPCR and UACI value comparison against various cover images related to other work [31–34] without optimization. Table 6, Table 7 represent NPCR and UACI value comparison against various cover images related to other work [31–34] after applying optimization. Tables 6 and 7 clearly demonstrate better value than other compared techniques. However Table 8 represent comparisons of average NPCR and UACI values with other related work [35, 36]. Result clearly represents our better value than other related techniques. Finally, Fig. 6 represents the NPCR and UACI value comparison between proposed and compared technique [27–30] after applying optimization. It is clear from the comparison that we have better range of values for NPCR and UACI than other reported techniques [27–30]

5 Conclusions

In this paper security of digital data is resolved using presented hybrid watermarking technique using NSCT-RDWT-SVD to resolve security problems. Initially, cover and watermarks are decomposed by NSCT-RDWT and SVD. Next, we find out best

Table 3 Comparison of improved robustness with related works

Attacks	Yu et al. [27]	Ali et al. [28]	Mishra et al. [29]	Thakkar et al. [30]	Proposed Technique		%age improvement
					NC(1)	NC(2)	
Salt and pepper noise	0.851	-	0.98	0.9962	0.9999	0.9593	0.14881489
Gaussian Blur	0.994	0.9906	0.96	0.9999	0.9988	0.9488	0.00360577
Median filter[2 2]	-	-	-	-	0.9968	0.9570	-
JPEG compression(QF = 25)	0.883	0.9892	-	0.998	0.9960	0.9576	0.10945382
Histogram equalization	-	0.9654	-	0.998	0.9958	0.9688	0.02632822
Cropping(12%)	-	-	-	0.9984	0.9999	0.9798	0.00140015
Speckle noise(Density = 0.05)	-	-	-	-	0.9999	0.9489	-
Average filtering	-	-	-	-	0.9998	0.9578	-
Rotation(20%)	0.832	-	-	0.9973	0.9989	0.9578	0.116598379
Scaling (50%)	0.997	0.9906	0.96	0.9999	0.9996	0.9697	0.00220104
Cropping and noise	-	-	-	-	0.9987	0.9574	-

Table 4 NPCR value comparison between proposed and compared technique (Without scaling factor optimization)

Image	Ref [31]	Ref [32]	Ref [33]	Ref [34]	Proposed method
Barbara	99.4285	99.5227	99.6092	99.6162	99.356
Boat	99.4509	99.5609	99.6102	99.6281	99.423
Cameraman	99.7335	99.5749	99.6205	99.6292	99.643
Lena	99.5177	99.5511	99.6228	99.6146	99.507
Peppers	99.5154	99.5808	99.6319	99.6092	99.504

Table 5 UACI value comparison between proposed and compared technique (Without scaling factor optimization)

Image	Ref [31]	Ref [32]	Ref [33]	Ref [34]	Proposed method
Barbara	33.6177	33.3890	33.7431	33.5776	29.35
Boat	32.4296	33.4176	33.5367	33.6143	28.25
Cameraman	32.5297	33.3691	33.7786	33.7050	34.59
Lena	33.2231	33.3461	33.7041	33.5561	30.98
Peppers	33.2263	33.3540	33.6923	33.6284	28.96

Table 6 NPCR value comparison between proposed and compared technique (Scaling factor optimization)

Image	Ref [31]	Ref [32]	Ref [33]	Ref [34]	Proposed method
Barbara	99.4285	99.5227	99.6092	99.6162	99.665
Boat	99.4509	99.5609	99.6102	99.6281	99.672
Cameraman	99.7335	99.5749	99.6205	99.6292	99.733
Lena	99.5177	99.5511	99.6228	99.6146	99.677
Peppers	99.5154	99.5808	99.6319	99.6092	99.734

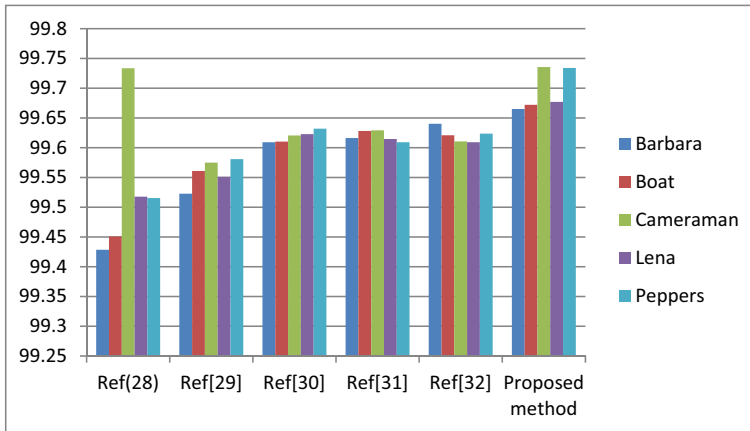
Table 7 UACI value comparison between proposed and compared technique (Scaling factor optimization)

Image	Ref [31]	Ref [32]	Ref [33]	Ref [34]	Proposed method
Barbara	33.6177	33.3890	33.7431	33.5776	33.744
Boat	32.4296	33.4176	33.5367	33.6143	33.705
Cameraman	32.5297	33.3691	33.7786	33.7050	34.751
Lena	33.2231	33.3461	33.7041	33.5561	33.981
Peppers	33.2263	33.3540	33.6923	33.6284	33.972

optimized value using Dragonfly optimization for imperceptibly embedding watermark inside cover image. Furthermore, watermarked data is secured using Henon Map. Performance of our method is evaluated using different parameters. Moreover, experimental outcomes based on various images clearly confirm the better

Table 8 Average UACI and NPCR value comparison between proposed and compared technique (after scaling factor optimization)

S No	Techniques	Average NPCR value	Average UACI value
1	Ref [35]	99.623	33.4935
2	Ref [36]	99.6680	19.1495
3	Proposed technique	99.6962	33.5367

**Fig. 6** Comparison of UACI value with other compared techniques (scaling factor optimization)

performance in term of robustness and imperceptibility. Further best value of PSNR and NC is 51.2967 dB and 1 respectively. Future plan is to check the performance for various color images against different distortions and parameters.

Data availability The datasets generated during and/or analyzed during the current study are available in the [Microsoft Bing] repository [WEB LINK TO DATASETS, CPUH].

Declarations

Conflict of interests The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. The author has no financial or proprietary interests in any material discussed in this article.

References

1. Begum M, Uddin MS (2020) Digital image watermarking techniques: a review. *Information* 11(2):110
2. Cheddad A, Condell J, Curran K, McKevitt P (2010) Digital image steganography: Survey and analysis of current methods. *Signal Process* 90(3):727–752
3. Potdar VM, Han S, Chang E (2005) A survey of digital image watermarking techniques. In *INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.* (pp. 709–716). IEEE

4. Mohammed AA, Salih DA, Saeed AM, Kheder MQ (2020) An imperceptible semi-blind image watermarking scheme in DWT-SVD domain using a zigzag embedding technique. *Multimed Tools Appl* 79(43):32095–32118
5. Bhatnagar G, Raman B (2009) A new robust reference watermarking scheme based on DWT-SVD. *Comput Stand Interfaces* 31(5):1002–1013
6. Charu A, Anurag M, Arpita S (2015) A novel gray-scale image watermarking using hybrid fuzzy-BPN architecture. *Egypt Inform J* 16:83–102
7. Mirjalili S (2016) Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems. *Neural Comput Appl* 27(4):1053–1073
8. Tang Z, Zhang X (2011) Secure image encryption without size limitation using Arnold transform and random strategies. *J Multimed* 6(2):202–206
9. Yao Q, Shao Z, Shang Y, Ding H, Liu X, Zeng R, Tong Q (2020) Color image encryption based on discrete trinomial Fourier transform and random-multiresolution singular value decomposition. *Multimed Tools Appl* 79(37):27555–27581
10. Kumar A, NarayanaRao TV (2016) Digital image watermarking using fuzzy logic and genetic algorithm. *Int J Comput Trends Technol* 41(2):101–105
11. Garg P, Kishore RR (2022) An efficient and secured blind image watermarking using ABC optimization in DWT and DCT domain. *Multimed Tools Appl* 81(26):36947–36964
12. Begum M, Uddin MS (2020) Analysis of digital image watermarking techniques through hybrid methods. *Adv Multimed* 2020:1–12
13. Deeba F, Dharejo FA, Zhou Y, Memon PA, Memon H, Khan SA, Larik NA (2022) Digital image watermarking in sparse domain. *Inf Secur J: Global Perspect* 31(2):237–250
14. Pourhadi A, Mahdavi-Nasab H (2020) A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain. *Multimed Tools Appl* 79:21653–21677
15. Zhang L, Wei D (2019) Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization. *Multimed Tools Appl* 78(19):28003–28023
16. Amiri A, Mirzakuchaki S (2020) A digital watermarking method based on NSCT transform and hybrid evolutionary algorithms with neural networks. *SN Appl Sci* 2(10):1–15
17. Sharma S, Chauhan U, Khanam R, Singh KK (2020) Digital Watermarking using Dragonfly Optimization Algorithm. *J Inf Technol Manag* 12(Special Issue: Deep Learning for Visual Information Analytics and Management):36–47
18. Hua KL, Dai BR, Srinivasan K, Hsu YH, Sharma V (2017) A hybrid NSCT domain image watermarking scheme. *EURASIP J Image Video Process* 1:10
19. Meenpal T (2018) DWT-based blind and robust watermarking using SPIHT algorithm with applications in tele-medicine. *Sādhanā* 43(1):4
20. Wang X, Chen W, Gao J, Wang C (2018) Hybrid image denoising method based on non-sampled contourlet transform and bandelet transform. *IET Image Process* 12(5):778–784
21. Hatami E, RashidyKanan H, Layeghi K, Harounabadi A (2023) An optimized robust and invisible digital image watermarking scheme in Contourlet domain for protecting rightful ownership. *Multimed Tools Appl* 82(2):2021–2051
22. Eldaoushy AF, Desouky MI, El-Dolil SA, El-Fishawy AS, El-Samie FEA (2023) Efficient hybrid digital image watermarking. *J Opt* 1–15
23. Apostolidis KD, Papakostas GA (2022) Digital watermarking as an adversarial attack on medical image analysis with deep learning. *J Imaging* 8(6):155
24. Zeng C, Liu J, Li J, Cheng J, Zhou J, Nawaz SA, ... Bhatti UA (2022) Multi-watermarking algorithm for medical image based on KAZE-DCT. *J Ambient Intell Hum Comput* 1–9
25. Singh HK, Singh AK (2024) Digital image watermarking using deep learning. *Multimed Tools Appl* 83(1):2979–2994
26. Gupta B, Agrawal DP, Yamaguchi S, (Eds) (2016) Handbook of research on modern cryptographic solutions for computer and cyber security. IGI global
27. Yu C et al (2019) An adaptive and secure holographic image watermarking scheme. *Entropy* 21(5):460
28. Ali M, Ahn C (2014) An optimized watermarking technique based on self-adaptive DE in DWT-SVD transform domain. *Signal Process* 94:545–556
29. Mishra A, Rajpal A, Bala R (2018) Bi-directional extreme learning machine for semi-blind watermarking of compressed images. *J InfSecurAppl* 38:71–84
30. Thakkar F, Srivastava VK (2021) An adaptive, secure and imperceptible image watermarking using swarm intelligence, Arnold transform, SVD and DWT. *Multimed Tools Appl* 80(8):12275–12292
31. Wang X, Li L, Zhang Y (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Opt Lasers Eng* 66:10–18

32. Belazi A, Abd El-Latif AA, Belghith S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. *Sig Process* 128:155–170
33. Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. *Sig Process* 92(4):1101–1108
34. Hua Z, Zhou Y, Pun CM, Chen CP (2015) 2d sine logistic modulation map for image encryption. *Inform Sci* 297:80–94
35. Mahalingam H, Veeramalai T, Menon AR, Amirtharajan R (2023) Dual-Domain Image Encryption in Unsecure Medium—A Secure Communication Perspective. *Mathematics* 11(2):457
36. Agbedemnab PA, Akolgo M, Agebure MA (2023) A New Image Watermarking Scheme Using Genetic Algorithm and Residual Numbers with Discrete Wavelet Transform. *J Inf Secur* 14(4):422–436

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.