



Dual watermarking: An approach for securing digital documents

Chandan Kumar¹ · Amit Kumar Singh² · Pardeep Kumar¹

Received: 5 November 2018 / Revised: 31 August 2019 / Accepted: 1 October 2019 /
Published online: 23 December 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract

This paper presents a dual watermarking technique using discrete wavelet transform (DWT), singular value decomposition (SVD) and set partitioning in hierarchical tree (SPIHT). The method uses second level DWT to transform the host image into different frequency components. Next, we further transform the selected wavelet component via SVD. Before embedding, the logo watermark is secured via Arnold transform and signature watermark are encoded by hamming code. Finally, we embed both encoded watermarks into the transformed host image via an embedding approach. The watermarked image is further compressed by SPIHT scheme along with the location key. With our scheme, maximum PSNR, NC and SSIM are obtained as 36.97 dB, 0.9965 and 0.9974, respectively. However, the best obtained BER is zero. Experimental results on various images demonstrate the importance of our scheme and superior to competing methods.

Keywords Dual watermarking · DWT · SVD · Arnold transform · SPIHT · PSNR · SSIM · NC · BER · Attacks

1 Introduction

Nowadays massive amount of digital data is generated, copied, shared and transmitted as a result of growth in information and communication technology (ICT) [4, 17].

✉ Amit Kumar Singh
amit_245singh@yahoo.com

Chandan Kumar
chandansharmahmr@gmail.com

Pardeep Kumar
pardeepkumarkhokhar@gmail.com

¹ Department of CSE & IT, JUIT, Solan, India

² Department of CSE, NIT Patna, Patna, Bihar, India

Secure transmission of digital data is still one of the major issues related with it. So, some scheme is needed to secure the digital data transmission/storage/sharing via open networks. One of the popular schemes to provide security of the contents from illegal users is digital watermarking [4, 7, 17, 20, 22]. The technique used to embed secret data imperceptibly into multimedia cover for the purpose of content authentications, annotation, ownership and copyright protection. However, it has also been applied to many other applications [4, 5, 17, 20]. Digital watermarking is used for last several years and it is an emerging area of research [4]. Various remarkable watermarking schemes have been introduced for prevention of identity theft and copyright protection. However, recent researches try to optimize the balance between contradictory factors of watermarking that motivate the necessary and continuous research in this area [1, 5, 17, 20].

Further, single watermarking techniques are able to achieve limited goals such as protection of single owner. However, to achieve better security some applications require copyright protection of several owners in multiple levels. So, dual watermarking is proved to be beneficial for protection and validate the integrity of contents [17]. There are three methods for securing images using dual watermarking. In first scheme, dual-watermark (one watermark embedded into another watermark) is embedded into cover image. In second method, primary and secondary watermarked images are generated by embedding watermark one after another respectively. In third technique, multiple watermarks are embedded simultaneously into cover image. Dual watermarking is helpful in various potential applications [3, 11, 21].

In the direction described above, we propose a DWT-SVD based robust and imperceptible dual watermarking for digital image. An encoded signature and scrambled logo watermark is simultaneously placed inside the cover for copyright protection and image validation, respectively. After embedding, the watermarked image is compressed by SPIHT scheme for efficient transmission and reduces storage need. Major contributions of our work as follows:

- **Fusion of DWT-SVD:** Due to extraordinary properties of DWT [15], it is the best choice for any researchers in watermarking domain. Further, excellent energy compaction properties and good stability make the SVD more popular for watermarking applications. It is established that DWT-SVD based watermarking schemes achieved better robustness as compared to applied separately [2, 9]. Therefore, the proposed method uses fusion of DWT-SVD to improve the robustness against attacks and preserves imperceptibility.
- **Compress image via SPIHT:** Our method uses fast and efficient SPIHT compression scheme to compress the watermarked image for efficient transmission and reduce storage requirement [12]. Further, this scheme added the flexibility to improve the performance (see Table 2) by setting an appropriate bit rate.
- **Imperceptibly embeds encoded dual watermarks:** To improve the security and reduce the bandwidth need, the method imperceptibly hides multi-watermarks inside the cover image. Further, our scheme is directly embedding the image watermark (instead of singular value of the watermark) in to the cover for better visual quality of the images. In addition, before embedding, the image and signature (text) watermark is encoded using Arnold transform and Hamming code, respectively. Therefore, the scheme provides additional security and robustness.

- **Data management:** Based on the robustness requirements [15], our scheme embeds more important data at high level DWT coefficients.

2 Related works

Some remarkable watermarking techniques are discussed below.

In [4], author described a secure watermarking scheme in transform domain. The method uses multi-objective evolutionary optimizer (MEO) to balance the major conflicting factors of watermarking system. Further, the method used Fibonacci-Lucas transformation for better security than Arnold transform. In [22], author uses different technique to produce a robust and imperceptible watermarking system for the authentication of medical images. Further, watermarked image is secured by using 2-D logistic map based chaotic encryption. Simulation results clearly confirmed that the method is robust, imperceptible and secure against various watermarking attacks. In similar way, Kumar et al. [7] also combined different techniques to provide a robust watermarking system. The method used SPIHT and Arnold transform for better robustness and security of the digital contents. Experimental study on different images proved that the scheme is robust and secure against various attacks. Author [13] developed imperceptibly embedding of multi-watermarks in the cover image. Before embedding, the method uses an encryption scheme to encrypt the text watermark. It is noticed that this encryption method minimize the encryption-decryption time while preserves security. The results studies indicate that technique is robust against considered attacks.

In [9], Author uses DWT-SPIHT-Arnold transform to develop a robust watermarking for medical data. The scrambled data, as a watermark image, is placed inside the appropriate wavelet coefficients of the cover. Before embedding, SPIHT scheme uses to determine the suitable coefficients of the cover image. In [6], Kumar et al. also introduced the embedding of scrambled version of watermark is placed inside the transformed coefficients of the cover images. The method uses the SPIHT scheme to compress watermarked image for efficient transmission on the network. Result study indicates the usefulness of the scheme in terms of objective and subjective evaluations. In [10], to improve the security of the medical data, a secure watermarking scheme is proposed, where encrypted version of the medical watermark is placed inside the cover image. Through experiments, the method is imperceptible and achieves good robustness against various kinds of attacks. In [18], Singh et al. developed the embedding of multi-watermark in the DWT-DCT-SVD coefficients of the cover image. Before embedding, text watermark is encoded via error correction code. Further, the selective encryption method is used to encrypt the watermarked image. In addition, the robustness of the scheme is further improved via neural networks. The robustness and imperceptibility of the scheme investigated through objective and subjective metrics. Various simulations confirm that the scheme provide a good trade-off between major parameters of the watermark systems. In similar way, Author of [23] introduced a BPNN based watermarking in DWT-DCT-SVD domain. The method imperceptibly embeds three encoded watermarks in the cover image. Lossless compression scheme and hamming code is used to compress and encode the symptom and signature text watermark, respectively. The test resultsfor considered

image showed the usefulness of the scheme. In [19], author introduced embedding of logo and QR code in selected DWT coefficient of the cover image. Results demonstrations indicate that, the method is robust for popular image processing attacks.

In [8], Liu et al. developed a dual watermarking scheme in wavelet domain. The method uses DWT to transform the ‘Y’ channel of the ‘YCbCr’ cover image and the robust logo watermark placed inside the resulting cover image. Further, fragile watermark is embedded in the RGB model of the watermarked image through spatial domain scheme. Test analysis on eight different color images indicates that the method is highly imperceptible and robust and suitable for copyright protection and authentication of image. In [14], a dual watermarking scheme is also proposed by Singh et al., in which different type of watermark is placed inside the DWT-SVD cover image. Before embedding, the method uses error correction code to encode the text watermark. Further, author investigated the performance of three well know code. Detail analysis of the work indicates the importance of the method in medical applications. In [16], a robust dual watermarking scheme in LWT-DCT domain is proposed. The method uses color image as cover and two encoded watermarks are imperceptibly embedded for authentication purpose. According to the result’s study, the method not only improved the robustness, but also computationally low.

3 Proposed method

Embedding and extraction procedure of our scheme is clearly presented in Fig. 1. The process is divided into three phases: 1) imperceptibly embedding of dual watermarks, 2) compress the watermarked image via SPIHT scheme, and 3) robustly extract both watermarks. After the second level DWT decomposition of the cover, apply the SVD on selected sub-band to obtain the singular vector for watermarking. Next, security of logo watermark is enhanced by Arnold encryption. Encrypted logo watermark is divided into two sub-images (both having equal size). Sub-image 1 and sub-image2 are embedded into ‘LH’ and ‘HL’ sub-band of 1st level DWT of cover image, respectively. However, text watermark is encoded by hamming code and placed inside the ‘HH’ sub-bands of second level DWT. Further inverse SVD and DWT are applied on watermarked image. Finally, the watermarked image is compressed via SPIHT scheme. In extraction process, all presented steps are implemented in reverse order to extract both watermarks from respective bands. Further, encrypted parts of watermark is combined together to recover the watermark image. At last, inverse Arnold is applied to decrypt original watermark image and hamming decoder is implemented to recover signature watermark.

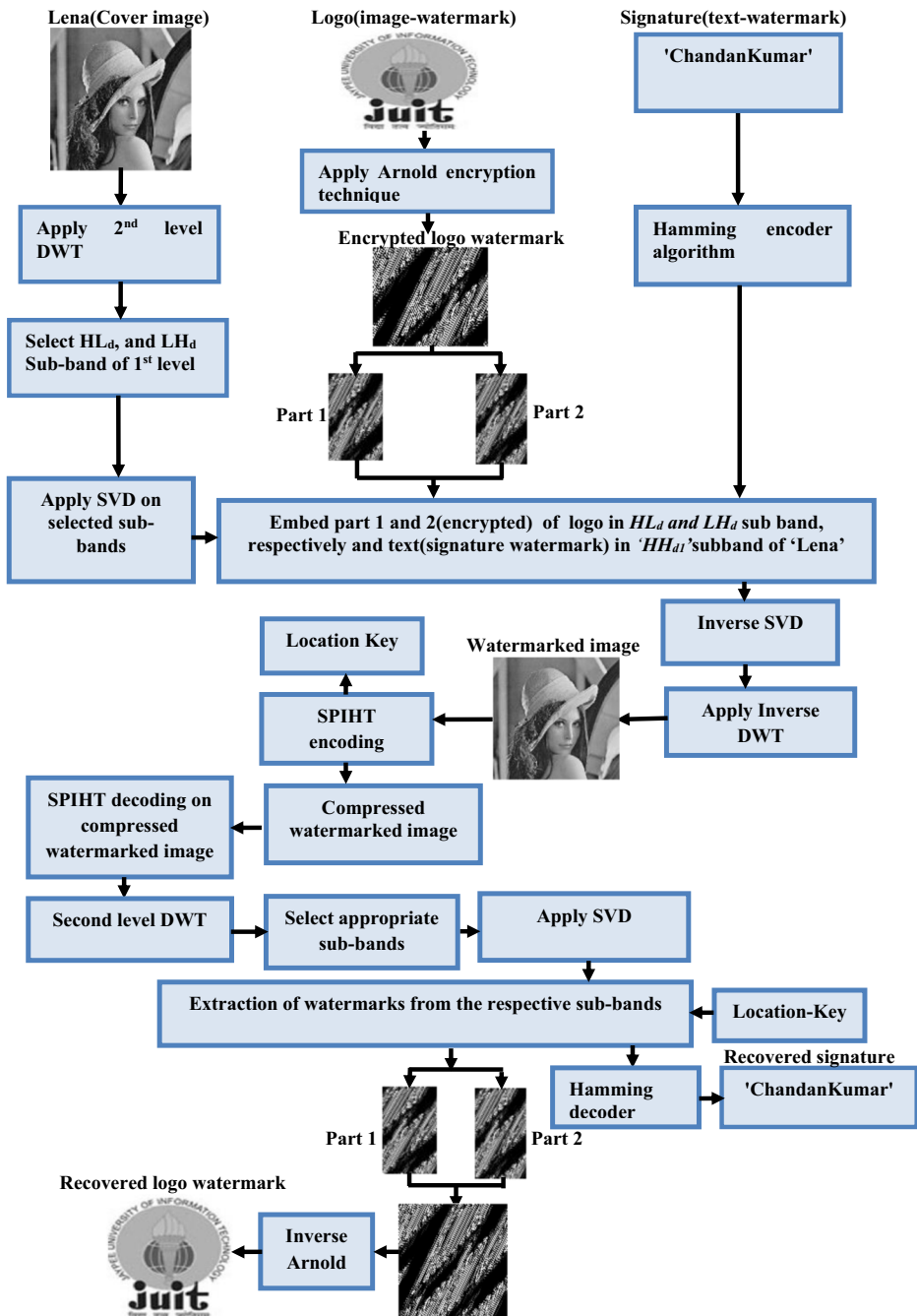


Fig. 1 Embedding and extraction procedure for watermarks (Logo and signature)

3.1 Algorithm for watermarks embedding

Step 1: Declared variables are

Lena(C_g) : Input cover image

Juit(K_g): Input 'logo' watermark

μ: Scale factor

DWT &SVD: Transform domain techniques

Wavelet filters:Haar

LL_d,HL_d,LH_d, HH_d: DWT coefficients for cover image(1st level)

LL_{d1},HL_{d1},LH_{d1}, HH_{d1}: DWT coefficients for cover image (2nd level)

Sd₁: diagonal matrix for HL_d

Sd₂: diagonal matrix for LH_d

U_{d1} and V_{d1}^T : Orthonormalmatrix for HL_d

U_{d2}andV_{d2}^T:Orthonormalmatrix for LH_d

μ:Scale factor

G_g^a: modified values of S_{dk}

U_{dg}^aand V_{dg}^{aT}: Orthonormal matrices for G_g^a

S_{dg}^a: Diagonal matrix for G_g^a

G_{amodi}: DWT coefficient(modified)

G_d: Watermarked image

G_c: Compressed watermarked image

G_r:Uncompressedwatermarked image

G_g : Encrypted watermark image

Step 2: Read cover and watermark image

$C_g \leftarrow$ Lena.bmp (Size :512×512)

$K_g \leftarrow$ Juit.bmp (Size:256×256)

Step3: Apply arnold encryption technique on watermark image

//Arnold transform is applied on text (signature) watermark.

$G_g \leftarrow$ Arnold_transform(K_g)

Step4: 'Lena' image transform by second level DWT

$[LL_d, HL_d, LH_d, HH_d] \leftarrow$ DWT (C_g , wavelet filter); //First level DWT decomposition

$[LL_{d1}, HL_{d1}, LH_{d1}, HH_{d1}] \leftarrow$ DWT (LL_d , wavelet filter); //Second level DWT decomposition

Step5: Apply SVD on selected sub- band of cover image

//Select sub band HL_d and LH_d from cover image

If (SVD on HL_d)

$U_{d1} S_{d1} V_{d1}^T \leftarrow$ SVD(HL_d) //SVD on sub-band HL_d

Endif;

If (SVD on LH_d)

$U_{d2} S_{d2} V_{d2}^T \leftarrow$ SVD(LH_d) //SVD on sub-band LH_d

Endif;

Step6: Change 'string/text' to binary bits

$Stxt \leftarrow$ binary(Chandankumar); // Stxt is number of bits generated using string

Step7: Binary watermark bits ($Stxt$) is encoding by Hamming

$G_b \leftarrow$ error correcting code ($Stxt$)

Where G_b is encoded binary watermark bits.

Step8: For watermarking bits Replace '(0,1)' by '(-1,1)'

//If L is length of string then bit stream is changed to $G(1) G(2) \dots G(L)$ by changing 0 by -1 & 1 by 1

Step9: Watermark (s) embedding

// Encrypted image watermark is divided into two parts $G = G_1 + G_2$, singular values is modified in HL_d and LH_d sub band with half of the watermark image

For $\mu \leftarrow 0.01:0.1$

$S_{da} + \mu G_a = G_g^a, a, g = 1, 2$

End;

//text watermark is embeds into HH_{d1} sub-band

For $\mu \leftarrow 0.01:0.1$

$f'(p, q) = f(p, q)(1 + \mu \times G_b)$; // $f(p, q)$ and $f'(p, q)$ are DWT coefficients before and after embedding process

end;

Step10: Calculate singular value for SVD(G_g^a) and modified coefficients for DWT.

If (SVD on G_g^a) then

$[U_{dg}^a S_{dg}^a V_{dg}^{aT}] \leftarrow$ SVD(G_g^a)

Endif;

//modified DWT coefficient

$G_{amodi} \leftarrow U_{da}^a S_{dg}^a V_{da}^T$

Step11: Obtained G_d (watermarked image)

$G_k \leftarrow$ InverseDWT [$LL_{d1}, HL_{d1}, LH_{d1}, G_b$, wavelet filter];

$G_d \leftarrow$ InverseDWT($G_k, G_1^1, G_2^2, HH_{d1}$, wavelet filter); //Watermarked image reconstruction

Step12: Apply SPIHT technique on watermarked image

$G_c \leftarrow$ SPIHT (G_d) // G_c is compressed watermarked image

3.2 Extraction algorithm for watermark

Step 1: Declared variable are:

μ : Scale-factor

LL_d, HL_d, LH_d, HH_d : Sub-bands(Watermarked image)

S_{d1} : Matrices (Orthonormal) for sub-band HL_d

S_{d2} : Orthonormal matrices for LH_d

U_{dg1} and V_{dg1}^T : Orthonormal matrices for HL_d

U_{dg2} and V_{dg2}^T : Orthonormal matrices for LH_d

DG: changed singular value (for selected sub-bands of cover image)

Ga: Recovered watermark

$a=1 \& 2$

Step 2: Apply SPIHT decompression and perform DWT on decompressed watermarked image (possibly distorted)

SPIHT (G_c) \rightarrow G_r //SPIHT decompression

$[LL_d, HL_d, LH_d$ and $HH_d, \text{wavelet filter}] \leftarrow$ DWT ($G_r, \text{wavelet filter}$)//DWT on decompressed watermarked image.

Step 3: Compute the singular values for HL_d, LH_d sub-bands

//Apply SVD to HL_d, LH_d subbands

If (SVD on HL_d) then

$U_{dg1} S_{dg1} V_{dg1}^T \leftarrow$ SVD(HL_d)

Endif;

If (SVD on LH_d) then

$U_{dg2} S_{dg2} V_{dg2}^T \leftarrow$ SVD (LH_d)

Endif;

Step 4: Calculate inverse SVD

DG $\leftarrow U_{dg}^g S_{dga} V_{dg}^{aT}; g=1,2$

Step 5: Recover and combinesub-image 1 and 2 of watermark image from each sub-band

$G_a = \frac{DG - S_{da}}{\mu}; a=1,2$

end;

//Text watermark extraction

$G_{rb} = \frac{f'_{r(p,q)} - f(p,q)}{\mu f(p,q)}; f'_{r(p,q)}$ represents DWT coefficients

$G_e b \leftarrow$ Positive or negative sign ($G_r b$);

Where $G_e b$ is extracted text watermark bits

Step6: Compute error correcting codes of $G_e b$

// Final watermark is obtained by replacing '(-1, 1)' by '(0, 1)'.

$G_r b \leftarrow$ Ecc($G_e b$)//Error correcting code on extracted watermark bits

Step7: Convert the watermark bits into text to get the original watermark

Originaltext \leftarrow binary to text(watermarkbits)

Step 8: Apply inverse Arnold transform to decrypt logo watermark

end:



Fig. 2 (I) cover image, (II) logo watermark, (III) signature watermark, and (IV) watermarked image

4 Experimental results

Our experiments are performed via MATLAB version 2013b. In this, ten different types of cover image (dimensions: 512×512), two watermarks as ‘logo’ (dimensions: 256×256), ‘signature’ watermark (96 bits) and ten important attacks are used for evaluation purpose. We used Peak signal to noise ratio (PSNR), normalized correlation (NC), Bit error rate (BER) and structured similarity index (SSIM) as standard performance metric to evaluate the performance of proposed scheme. These performance metrics are well defined in [17]. The Lena (cover image), watermarks (logo & signature) and watermarked images are shown in Fig. 2. Figure 3 shows extracted logo and signature watermarks. Extracted watermarks and watermarked (attacked) images are depicted in Fig. 4. We analyzed the performance of our proposed scheme in Tables 1, 2, 3, 4, 5, 6 and 7.

Table 1 summarizes the performance in terms of PSNR, NC, BER and SSIM of our proposed method at different gain and bit rate. In Table 1, the best value of PSNR, NC and SSIM are 36.97 dB (at gain = 0.01 and bit rate = 3), 0.9965 (at gain = 0.1 and bit rate = 2), and 0.9969 (at gain = 0.01 and bit rate = 3), respectively. However, BER is zero in all considered cases.

The performance of our method at different bit rates and gain = 0.05 are shown in Table 2. In this Table, the best value of PSNR, NC and SSIM are 33.15 dB (at gain = 0.05 and bit rate = 1), 0.9950 (at gain = 0.05 and bit rate = 3), 0.9929 (at gain = 0.05 and bit rate = 1), respectively. However, BER is zero in all considered gain and bit rate values. From Table 2, it is observed that the best performance is obtained at bit rate = 3 and gain = 0.05. Hence, these values are selected for further investigation. Table 3 lists the PSNR, NC, BER and SSIM values of our method for different cover images under bit rates = 3 and gain = 0.05. From this table, best value of PSNR, NC and SSIM is 33.20 dB (for ‘Moon’ image), 0.9962 (for ‘Tire’ image) and 0.9974 (for ‘Moon’ image), respectively.

Table 4 lists the NC, BER and SSIM values with gain = 0.05 & bit rate = 3 under various attacks. From Table 4, best value of NC is 0.9999 for average filtering attack, BER is zero for most of the considered attacks, and SSIM is 0.9966 under median filter [33]. However, maximum BER = 4.76 under cropping attack. Table 5 shows the NC, BER and SSIM for

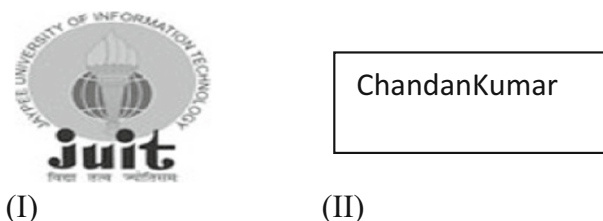


Fig. 3 Extracted watermarks, (I) logo and (II) Signature



Type of attack	watermarked images(after attack)	Recovered Logo watermark	Recovered Signature watermark
Salt and pepper noise(having density=0.01)			ChandanKumar
Gaussian noise(having mean=0,variance=0.01)			ChandanKumar
Median-Filter [2 2]			ChandanKumar
Jpeg-compression(with QF=50)			ChandanKumar
Histogram Equalization			ChandanKumar
Cropping-attack(20 20 400 480)			ChandanKumar
Speckle noise(having density=0.05)			ChandanKumar
Average filtering attack			ChandanKumar

Fig. 4 Watermarked (attacked) and watermarks (extracted)

varying size of text watermark at bit rate = 3. By considering this Table, we noticed that greater size of watermark affect the performance of our approach.

Tables 6 and 7 lists the NC value's comparison with other approaches under popular attacks. From these tables, our scheme achieves a better robustness in compare to the competing methods [6, 12, 16]. As shown in these tables, it is established that the proposed scheme presented up to 77.40% enhancement in NC value over competing methods at low BER value.

Therefore, with the above discussion, the proposed scheme offers the optimal performance and superiority. Consequently, our scheme offers a better trade-off between conflicting factors of watermarking.

Table 1 PSNR, NC, BER and SSIM values at different bit rates and gain

Bit rate values	Gain factors (μ)	PSNR (dB)	NC	BER	SSIM
1	0.01	36.79	0.8904	0	0.9968
	0.04	35.11	0.9935	0	0.9957
	0.05	34	0.9939	0	0.9946
	0.1	30.21	0.9936	0	0.9864
2	0.01	36.93	0.8828	0	0.9944
	0.04	35.32	0.9925	0	0.9959
	0.05	34.37	0.9935	0	0.9949
	0.1	30.25	0.9965	0	0.9865
3	0.01	36.97	0.8818	0	0.9969
	0.04	35.35	0.9919	0	0.9959
	0.05	34.39	0.9931	0	0.9909
	0.1	30.27	0.9963	0	0.9866

Table 2 PSNR, NC, BER and SSIM values at different bit rates and gain = 0.05

Bit rate	PSNR	NC	BER	SSIM
1	33.15	0.9950	0	0.9929
2	32.49	0.9775	0	0.9924
3	32.52	0.9777	0	0.9925

Table 3 PSNR, NC, BER and SSIM values for different cover images at bit rates =3 and gain = 0.05

Cover images	PSNR (dB)	NC	BER	SSIM
MRI	32.52	0.9777	0	0.9925
Barbara	28	0.9838	0	0.9926
Baboon	29.6	0.9246	0	0.9533
Boat	29.91	0.9482	0	0.9567
Finger	28.90	0.9428	0	0.9622
Bird	32.45	0.9935	0	0.9834
Cameraman	29	0.9936	0	0.9913
Coins	30.69	0.9947	0	0.9913
Moon	33.20	0.9804	0	0.9974
Tire	32.79	0.9962	0	0.9955

Table 4 NC, BER and SSIM values against different attacks using ‘Lena’ as cover

Attacks applied	NC values	BER	SSIM
Salt & pepper noise attack (with density = 0.01, 0.08, 0.001)	0.5377, 0.5175, 0.9914	0	0.9481, 0.9462, 0.9933
Gaussian noise-attack (mean = 0, variance = 0.01, 0.001, 0.002)	0.3765, 0.7171, 0.5065	0	0.8944, 0.9822, 0.9687
Median filter [2, 2], [3, 3]	0.8981, 0.8132	0.9432	0.9938, 0.9966
JPEG compression (QF = 50 & QF = 80)	0.9871 & 0.9959	0	0.9936 & 0.9938
Histogram equalization	0.6357	1.4286	0.4363
Cropping (20, 20, 400, 480)	0.7891	4.76	0.2290
Speckle noise attack (at density = 0.01, 0.02 & 0.005)	0.7421, 0.6119 & 0.8709	0	0.9857, 0.97750 & 0.9899
Average filtering	0.9999	0.9485	0.9932

Table 5 PSNR, NC, BER and SSIM values for varying size of text watermark

Gain factor (μ)	24 characters				15 characters			
	PSNR	NC	BER	SSIM	PSNR	NC	BER	SSIM
0.01	36.8822	0.9320	0	0.9964	37.72	0.9180	0	0.9969
0.05	34.1801	0.9958	0	0.9939	34.61	0.9960	0	0.9945
0.1	29.3564	0.9918	0	0.9855	29.49	0.9916	0	0.9859

Table 6 Robustness comparison results of related watermarking schemes

Attacks	NC [12]	NC [6]	NC (Proposed technique)	% Enhancement in NC value
Salt & pepper (noise density = 0.5)	0.7208	0.5810	0.9914	37.54
Gaussian (mean = 0, Var = 0.02)	–	0.7906	0.8329	5.35
Scaling attacks ($\times 1.5$)	–	0.5227	0.9273	77.40
Histogram equalization	0.5415	0.6736	0.9384	39.31
Cropping	0.7158	–	0.7891	10.24
Sharpening	0.5034	–	0.6985	38.76
Invert-attack	0.9771	–	0.9821	0.51

Table 7 NC Comparison results of related watermarking scheme [16] and proposed scheme

Attacks	Technique [16]		Proposed method		% Enhancement in NC value
	NC	BER	NC	BER	
JPEG Compression attack at (QF=100, 60&20)	0.9950,0.9325,0.9653	0	0.9969,0.9852, 0.9704	0	0.19
Sharpening mask attack under threshold = 0.1, 0.3, 0.5, 0.7 & 0.9	0.6073,0.6257, 0.6390,0.6486,0.6556	0	0.6705, 0.6815, 0.6948, 0.6985	0	6.54
Median filtering [2 2] and [3 3]	0.9116,0.8885	0	0.8991,0.8132	0	-1.37
Scaling factor 2&2.5	0.7075,0.6500	0.1,0.126	0.7445, 0.6850	0.2,3810	5.23, 5.38
Gaussian-LPF having standard deviation value = 0.6	0.8780	0	0.8789	0	0.1
Gaussian noise Under mean = 0 & Var = 0.001,0.05	0.7012,0.3150	0,8.5714	0.7171,0.4257	0, 2.381-0	2.27, 35.14
Salt & pepper noise with (Density = 0.001,0.1)	0.7553,0.3011	0	0.9914, 0.4158	0	31.26
Histogram equalizationattack	0.5880	1.4286	0.6357	2.3810	8.11
Cropping attack(20,20 400,480)	0.7451	4.5714	0.7891	4.7619	5.9

5 Conclusions

In this work, a robust technique for multiple watermarking techniques based on DWT, SVD, SPIHT and Arnold transform is proposed. We have embedded multi-watermarks inside cover image for purpose of authentication and integrity. Arnold transform provides extra level of security. Due to spatio-frequency localization properties of DWT, watermark location can be easily detected. However, visual-perception of cover image remains unchanged if there is slight change in singular values due to mathematical property of SVD. Further, presence of SPIHT provides bandwidth efficient transmission of data. Experimental results reveal that the scheme is secure and robust for different attacks and found superior to competing approaches. In future, proposed scheme can be further improved and expanded to other multimedia watermarking schemes such as audio and video.

References

1. Bhatnagar G, Raman B (2009) A new robust reference watermarking scheme based on DWT-SVD. *Computer Standards & Interfaces* 31(5):1002–1013
2. Chang CC, Tsai P, Lin CC (2005) SVD-based digital image watermarking scheme. *Pattern Recogn Lett* 26(10):1577–1586
3. Elhoseny M, Ramírez-González G, Abu-Elnasr OM, Shawkat SA, Arunkumar N, Farouk A (2018) Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access* 6:20596–20608. <https://doi.org/10.1109/ACCESS.2018.2817615>
4. Gunjal BL, Mali SN (2015) MEO based secured, robust, high capacity and perceptual quality image watermarking in DWT-SVD domain. 4(1), pp. 126
5. Kumar C, Singh AK, Kumar P (2018) A recent survey on image watermarking techniques and its application in e-governance. *Multimed Tools Appl* 77(3):3597–3622
6. Kumar C, Singh AK, Kumar P (2018) Improved wavelet-based image watermarking through SPIHT. *Multimed Tools Appl*:1–14. <https://doi.org/10.1007/s11042-018-6177-0>
7. Kumar C., Singh A. K., Kumar P., Singh R. and Singh S.(2018) SPIHT based multiple image watermarking in NSCT domain, *Concurrency and Computation: Practice and Experience*, <https://doi.org/10.1002/cpe.4912>
8. Liu XL, Lin CC, Yuan SM (2018) Blind dual watermarking for color images' authentication and copyright protection. *IEEE Transactions on Circuits and Systems for Video Technology* 28(5):1047–1055
9. Meenpal T (2018) DWT-based blind and robust watermarking using SPIHT algorithm with applications in tele-medicine. *Sādhanā* 43(1):4
10. Sharma A, Singh AK, Ghrrera SP (2017) Robust and secure multiple watermarking for medical images. *Wirel Pers Commun* 92(4):1611–1624
11. Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H, Hou G (2018) Secure and robust fragile watermarking scheme for medical images. *IEEE Access* 6:10269–10278. <https://doi.org/10.1109/ACCESS.2018.2799240>
12. Shivani J. L.andSenapati R. K. (2017) Robust Image Embedded Watermarking Using DCT and Listless SPIHT. *Future Internet* 9(3):1–16
13. Singh AK (2017) Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimed Tools Appl* 76(6):8881–8900
14. Singh AK (2019) Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image. *Multimed Tools Appl*:1–11. <https://doi.org/10.1007/s11042-018-7115-x>
15. Singh AK, Dave M, Mohan A (2014) Wavelet based image watermarking: futuristic concepts in information security. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences* 84(3):345–359
16. Singh AK, Kumar B, Dave M, Mohan A (2015) Robust and imperceptible dual watermarking for telemedicine applications. *Wirel Pers Commun* 80(4):1415–1433
17. Singh AK, Kumar B, Singh G, Mohan A (2017) *Medical Image Watermarking: Techniques and Applications*, book series on Multimedia Systems and Applications, Springer, USA, ISBN: 978–3319576985
18. Singh, A.K., Kumar, B., Singh, G. and Mohan, A.(2017). Secure Multiple Watermarking Technique Using Neural Networks. In: Singh et al. (eds.) *Medical Image Watermarking: Techniques and Applications* (pp. 175–194). Springer, Cham.

19. Singh RK, Shaw DK, Jha SK, Kumar M (2017) A DWT-SVD based multiple watermarking scheme for image based data security. *J Inf Optim Sci* 39(1):67–81. <https://doi.org/10.1080/02522667.2017.1372153>
20. Singh L, Singh AK, Singh PK (2018) Secure data hiding techniques: A survey. *Multimed Tools Appl*:1–21. <https://doi.org/10.1007/s11042-018-6407-5>
21. Thakur S, Singh AK, Ghrera SP, Elhoseny M (2018) Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-018-6263-3>
22. Thakur S, Singh AK, Ghrera SP, Mohan A (2018) Chaotic based secure watermarking approach for medical images. *Multimed Tools Appl*:1–14. <https://doi.org/10.1007/s11042-018-6691-0>
23. Zear A., Singh A.K. and Kumar P.(2016). A proposed secures multiple watermarking techniques based on DWT, DCT and SVD for application in medicine. *Multimedia Tools and Applications*, pp. 1–20.

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



Chandan Kumar received B.Tech. in Computer Science and Engineering from H.P. University Shimla in 2003. He has done M.Tech. in Computer Science from Singhania University Rajasthan in 2011. He is currently pursuing Ph.D. from J. P. University Waknaghat (H.P). His research interest includes Data Hiding Techniques, Image Processing and Computer networks.



Amit Kumar Singh is currently an Assistant Professor with the Computer Science and Engineering Department, National Institute of Technology Patna (An Institute of National Importance), Patna, India. He has authored over 90 peer-reviewed journal, conference publications, and book chapters. He has authored three books entitled

Medical Image Watermarking: Techniques and Applications, Springer, in 2017, and Animal Biometrics: Techniques and Applications, Springer, in 2018, Intelligent Wavelet Based Techniques for Advanced Multimedia Applications, Springer, in 2019. He has also edited fourbook entitled Handbook of Multimedia Information Security: Techniques and Applications, Springer, in 2019, Security in Smart Cities: Models, Applications, and Challenges, Springer, in 2019, the Proceedings of 4th IEEE International Conference on Parallel, Distributed and Grid Computing, in 2016, and the Proceedings of 4th International Conference on Image Information Processing, in 2017. He currently serves on the Associate Editor of IEEE ACCESS and Former member of the editorial board of Multimedia Tools and Applications (Springer). He has edited various international journal special issues as a Guest Editor, such as IEEE Consumer Electronics Magazine, IEEE Access, Multimedia Tools and Applications, Springer, International Journal of Information Management, Elsevier, Journal of Ambient Intelligence and Humanized Computing, Springer, Int. J. of Information and Computer Security, InderScience, International Journal of Grid and Utility Computing, Inderscience and Journal of Intelligent Systems, Walter de Gruyter GmbH & Co. KG, Germany. His research interests include data hiding, biometrics, & Cryptography.



Pardeep Kumar is currently working as Assistant Professor (Senior Grade) in the Department of Computer Science & Engineering at Jaypee University of Information Technology (JUIT), Wakanaghat and he has 10 years of extensive experience in Academics. Prior to joining Jaypee Group, he has associated with Mody University of Technology & Science (Formerly known as Mody Institute of Technology & Science) Laxmangarh, Sikar, Rajasthan. He has completed his Ph.D. (Computer Science and Engineering, Nov. 2012) from Uttarakhand Technical University, Dehradun. Dr. Kumar is also serving as Professional Member of ACM (Association for Computing Machinery), Life Member of IAENG (International Association of Engineers) and IAENG society of computer science and society of Data Mining. Dr. Kumar has published around 22 papers in peer reviewed Journals and Conferences of National and International repute.