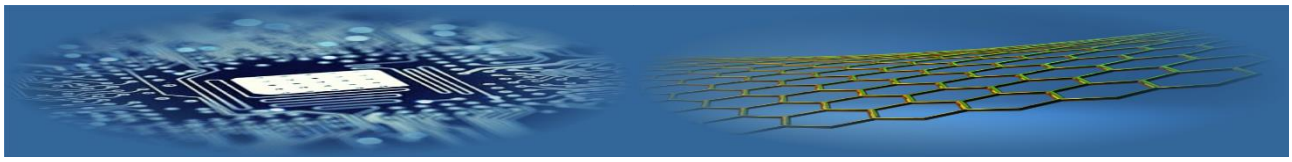

A new hybrid blind image watermarking technique for content authentication based on LWT & SVD

Pratibha Singh*, R R Tewari

Department of Electronics and Communication, University of Allahabad, Allahabad, India

**Corresponding author's e-mail: pratibha2238@gmail.com*

Received 27 September 2017, www.cmnt.lv

Abstract

This paper proposes, a robust digital watermarking technique based on LWT (Lifting wavelet transform) and Singular value decomposition (SVD) for the protection of intellectual rights. The singular values of watermark logo are embedded into the singular values of HH subband which is obtained by 1-level LWT on original image and then SVD. In this scheme, a Digital signature is generated by using secret key and the orthogonal matrices (U & V) which is achieved by performing SVD on watermark image for the security purpose. In the next step, the generated digital signature is embedded into the modified LL_3 and HH_3 subband which is obtained after further decomposition of LL subband by N-level LWT. On the receiver side, before extracting watermark, the digital signature is used for the ownership authentication: If the extracted signature is matched with the generated signature then the process of watermark extraction goes on otherwise is stopped. Thus, the proposed scheme achieves the high robustness against various attacks is analyzed.

Keywords:

Lifting Wavelet Transform (LWT),
SVD (Singular value decomposition),
Image watermarking,
Digital signature

1 Introduction

Today, a large number of digital documents can be stored, transmitted and copied easily which raise the concern towards the security and privacy of these digital data from its illegal copying, duplication, distribution and tampering. Sharing of digital data over the internet causes direct and severe economic loss to the copyright owner which reduces the actual value of the content. Therefore, protection of multimedia becomes a serious demanding issue. In this case digital watermarking is being used as a potent tool for preventing the intellectual properties. Insertion of some data into the media, in such a way that no one is able to differentiate between the original one and the image after its embedding is said to be Digital Watermarking [1]. The two main process of watermarking schemes are embedding and an extraction. In embedding, a watermark which is a secret message is inserted into the original medium (host) whereas extraction process tries to obtain the watermark from the cover medium. The main essential characteristic which defines the watermarking technique qualities are [1]:

a) Robustness: The watermark must be capable to remaining alive after various attacks which may be image processing or geometrical attacks like cropping, noise, filtering, rotation and compression. Robustness means the watermark image should not be destroyed after applying these several attacks.

b) Imperceptibility: The presence of secret data should not be detectable from the naked human eyes. In other words, it becomes quite difficult to distinguish between these two images for human visual system. It means after inserting the confidential message, the originality of the cover image should not degraded.

c) Capacity: It refers to how many numbers of bits can be hidden in a host image without losing its imperceptibility and is totally dependent on the application.

There are two broad categories of digital watermarking process for embedding the watermark i.e. spatial domain and Transform domain. In spatial domain, embedding is executed by a simple logic i.e. by reorganizing the image pixels and the easiest example is to alter the LSB of the original image pixels and the watermark is embedded on these modified LSB. On the other hand, in transform domain, we find out all the frequency coefficients of an image by using any of these transformation techniques like DCT, DWT, DFT and embedding is performed on these frequency coefficients.

From the review of literature, it is found that numerous watermarking schemes have been developed for improving the two main features i.e. imperceptibility and robustness which can be achieved by using different transform methods as well as by their combinations. Recently, SVD based watermarking receives valuable importance due to its various properties means the singular values obtained by SVD possess a stability factor due to which a minute change in singular values doesn't affect the transparency of the original image. Liu & Tan et al, (2002), have used SVD in their scheme, where they find out the singular values of host image and then change these obtained values by summing the watermark, this technique perform better robustness against geometric attacks. Ganic & Eskicioglu et al, (2004) proposed a blind watermarking algorithm where singular values are obtained from all the subband of the host media obtained by DWT. SVD is also perform on visual watermark and then these obtained values of host image and watermark image are summed up. This technique is remarkably not robust to geometric attacks. Gaurav et al, (2012) developed a technique based on wavelet transform for protecting the data. In their proposed technique,

embedding is done on the selected blocks of the subband obtained by the l-level DWT and Zig-Zag scan. Blocks for embedding are selected by finding the variances which is normalized to the threshold values. The experimental results show better visual perceptibility against attacks. Gaurav et al, (2012) proposed another technique using fractional wavelet packet transform (FRWPT) and SVD for improving the fidelity. Another watermarking scheme introduced by Musrrat Ali et al, (2015) using DWT, SVD & artificial bee colony (ABC). In this researcher keep choosing the blocks for embedding on the basis of human visual system. The simulations result shows that this scheme achieves high robustness against several intentional and unintentional attacks. Xiaojun Qi et al, (2015) proposed a new approach for generating a watermark by using Mersenne Twister algorithm and a secret key. By using Singular values, the original image is JPEG quantized into blocks of 4 X 4 (IW) and another content dependent watermark is generated (CW) and finally the watermark is generated by performing Xor operation between CW & IW. And this watermark is embedded into the randomly chosen non-overlapping blocks 4 X 4 of host image and shows high robustness with attacks. Makbol et al, (2014) proposed a digital signature based watermarking scheme with integer wavelet transform & SVD to achieve high security against malicious attacks and to defeat the false positive problem. The embedding of watermark is done directly into the singular values of the all the sub band of original image which is achieved by 1-level IWT and SVD and the digital signature is embedded into the obtained watermarked image. This scheme solve out the false positive problem. Recently, Vivek et al, (2015) proposed a significant region (SR) based image watermarking via LWT where they decompose the host image by 3-level LWT. By using a key, the coefficients of subbands obtained are randomly shuffled and grouped into the block and these blocks again shuffled using a secret key. Set all coefficients from each block into ascending order and find out the maximum and minimum coefficients. The watermark is embedded into the blocks having maximum coefficient differences. This method maintains a satisfactory result for imperceptibility.

For enhancing the security, a new watermarking technique which is based on LWT and SVD is proposed in this research paper. LWT is preferred due to its several advantages from the traditional wavelet transform as it reduces number of operations nearly by a factor of two. In this paper, the host image is gray image (512 X 512) and watermark is a binary logo (64 X 64), which is resized according to the host image before inserting. Watermark is embedded by replacing the singular values of host image by watermark. Digital signature using a secret key is generated by the orthogonal matrices U & V of watermark image which is embedded in modified LL_{3} and HH_{3} subband, obtained after further decomposition of LL subband by 3-level LWT. The proposed scheme is semi-blind watermarking where we require a watermark image for the signature generation for authentication purpose. If the generated signature is matched with the extracted one then the extraction process will keep on otherwise is stopped. The center of attraction of this research paper is to achieve high robustness from various attacks such as geometrical and non geometrical specially noise, rotation and compression.

The remaining paper is organized as follows: Section 2 introduces the basic theory on which the watermarking scheme is based on. Section 3 presents the generation of digital signature, embedding and extraction from the watermarked image and the proposed watermarking scheme is also explained. Experimental outcomes and Conclusion are briefly discussed in section 4 and 5.

2 Preliminaries

2.1 LIFTING WAVELET TRANSFORM (LWT)

Wim Swedens introduced the concept of lifting wavelet transform (1998) to reduce the computational time as it allows a faster and easier implementation of wavelet transform. This lifting scheme is a modus operendi to implement reversible integer wavelet transform which is not possible in the conventional transform methods means it is just to solve out the problem which we have in integer domain [12]. There are mainly three basic steps for constructing wavelet using lifting scheme i.e. splitting, prediction and update.

Split phase: Also known as lazy wavelet transform, where the input signal is X (n) is split into two part, one is even and the other is odd X (2n) and X(2n +1) and is expressed as:

$$\text{Split}(X(n))=[(X_{even}(n)), (X_{odd}(n))]. \quad (1)$$

Prediction phase: Here, we use unchanged even samples to predict odd sets $X_{odd}(n)$ and the difference between the real values and the prediction values $P[X_{even}(n)]$ is generated as:

$$S(n)=X_{odd}(n) - P[X_{even}(n)], \quad (2)$$

where, P[.] = prediction operator and S(n) is the detail signal which represent the high frequency part of the real signal and this prediction phase is represented as a high pass filter.

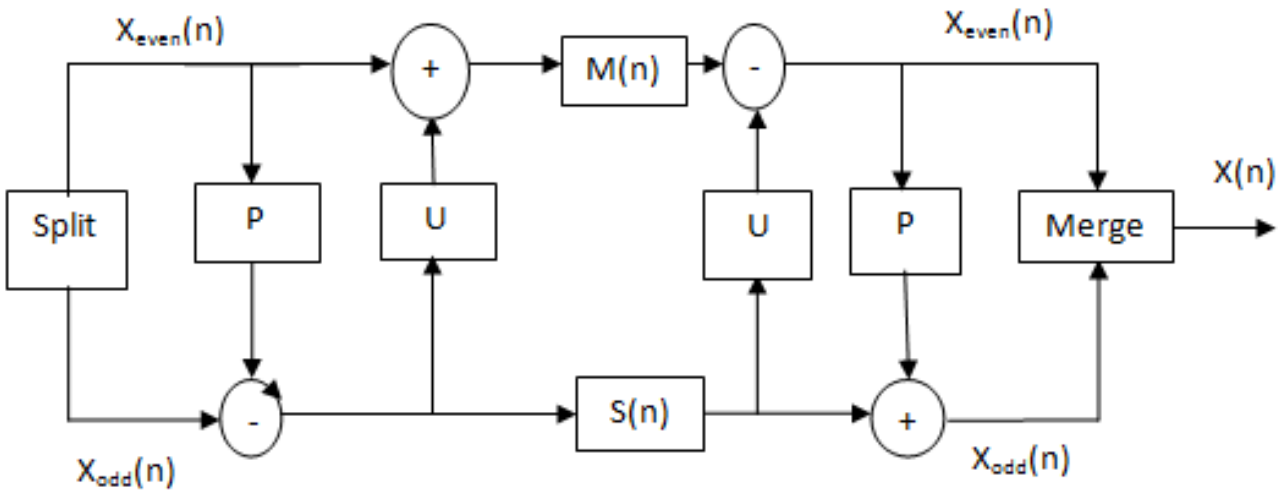

FIGURE 1 Decomposition and reconstruction of lifting wavelet

Update: In this step, even samples $X_{even}(n)$ are updated by using detail signal S(n), obtained by the update operator U[.] and a approximate signal M(n) represent the low frequency component of the original signal and it can be viewed as in Equation (3)

$$M(n) = X_{even}(n) + U[S(n)]. \quad (3)$$

Reconstruction of the lifting wavelet transform is an inverse process of decomposition and both of the process is shown in Figure 1.

$$A=U_A*S_A*V_A{}^T=\begin{bmatrix} U_{1,1} & \cdots & U_{1,M} \\ \vdots & \ddots & \vdots \\ U_{M,1} & \cdots & U_{M,M} \end{bmatrix}\begin{bmatrix} S_{1,1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & S_{M,N} \end{bmatrix}\begin{bmatrix} V_{1,1} & \cdots & V_{1,N} \\ \vdots & \ddots & \vdots \\ V_{N,1} & \cdots & V_{N,N} \end{bmatrix}^T, \quad (4)$$

where, U_A and V_A are called as the left and singular vectors of matrix A. SVD is widely used in watermarking due to its unique features i.e. the slight modification in singular values will not affect the transparency of the original image. Singular values define the luminance of an image, whereas singular vectors (U_A & V_A) define the geometric properties of an image. From the first row to the last row, the components of the diagonal matrix S_A should be arranged in a specified manner i.e. from highest value to the lowest one means in descending order and satisfy the relation 5,

$$S_{1,1} \geq S_{2,2} \geq \ldots\ldots\ldots\ldots\ldots\ldots\ldots S_{r,r} > S_{r+1,r+1} = S_{M,N}, \quad (5)$$

where r = rank of the matrix

3 The proposed scheme (LWT-SVD)

In this segment, the proposed LWT-SVD scheme is demonstrated which consist of two basic steps: Digital signature as well as watermark embedding into the host image and extraction of watermark as described in Figure 2 and Figure 3, respectively. For enhancing the security, a signature based watermarking technique has been implemented where the orthogonal matrices of the watermark image U, V and secret key has been used for signature generation. For owner validation, the process is segmented into two general steps: Generation of Digital signature, embedding of signature then extraction of signature is performed and lastly authentication steps. Firstly, the signature is generated and then embedding is done as explained in subsection 3.1 and 3.2. At the time of decoding the signature is extracted from the watermarked image which is compared by the signature which has been generated at the owner side. If the signature matches then the watermark extraction process is carries on otherwise the extraction of watermark comes to an end and no watermark will be extracted.

2.2 SINGULAR VALUE DECOMPOSITION

On Linear algebra theory, SVD is totally based where the factorization is performed on any rectangular real or complex matrix. This is the method of converting correlated variables into uncorrelated sets due to which different connections between the original data is exposed in better manner [2]. It is used as multimedia gadget as it becomes a very beneficial in analysis of data and in signal processing applications.

According to the SVD theory, a rectangular matrix A, can be sub divided into matrices; an orthogonal matrix U, a diagonal matrix S and the transpose of an orthogonal matrix V and is represented as in (4),

3.1 SIGNATURE GENERATION STEPS

Digital signature is the peculiar binary digits, which is generated by the use of secret key and U, V matrices. The important condition of signature is that it should be random in nature so that the attacker will find some difficulty from predicting it. Steps for the generation of digital signature are listed below:

1. We have taken the orthogonal matrices (U_w & V_w) of watermark image for generating the signature.
2. Find the sum and then median of both orthogonal

matrices U_w and V_w.

3. Transform both matrices into their corresponding binary bits under the conditions as follows.

$$If = \begin{cases} U_{w,sum} > U_{w,sum}\,(median) = 1 \\ otherwise = 0 \end{cases}$$

$$If = \begin{cases} V_{w,sum} > V_{w,sum}\,(median) = 1 \\ otherwise = 0 \end{cases}$$

4. Perform XORing between both the binary outputs and save as R_1 (n).
5. Secret key is also transformed into binary bits i.e R_2 (n).

$G(n) = R_1(n) \oplus R_2(n)$

where $\oplus$ is XOR operation. The result obtained G(n) is a generated signature. This generated signature is embedded into the host image.

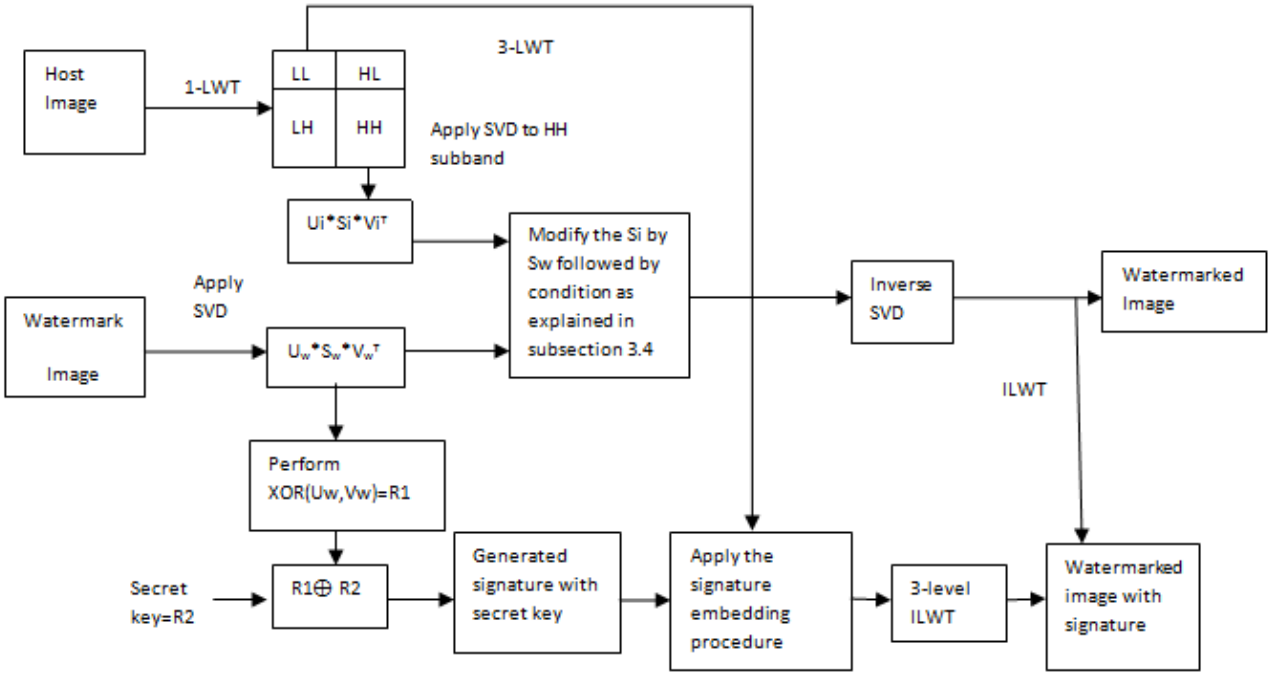

FIGURE 2 Proposed watermarking technique

3.2 SIGNATURE EMBEDDING

One of the important conditions that should be kept in mind before inserting the digital signature into the original media is that the signed watermarked image should be robust and the quality of an image may not be degraded. 4-level LWT is applied on the host image which decompose it into subbands i.e. $LL_{\_3}$, $LH_{\_3}$, $HL_{\_3}$ and $HH_{\_3}$. $LL_{\_3}$ and $HH_{\_3}$ subbands are modified for embedding the digital signature and the procedure of embedding the signature are illustrated as follows:

1. Perform 1-level LWT on original media i.e. an image.
2. Again apply 3-level LWT on LL subband and the obtained subands are, $LL_{\_3}$, $LH_{\_3}$, $HL_{\_3}$, $HH_{\_3}$.
3. Reshape $LL_{\_3}$ and $HH_{\_3}$ subband into a single row vector after squaring all the elements present in these two subbands, as follows:

$$LL_{\_3}^{m\ odified} = [1: (LL_{\_3})\ \hat{}2]$$

$$HH_{\_3}^{modified} = [1: (HH_{\_3})\ \hat{}2]$$

4. Concatenate all the elements of above row vectors into larger row vectors and the resultant rows we obtain are of size 1 X 512.

$$D_{\_modified} = [LL_{\_3}^{modified}\ HH_{\_3}^{modified}]_{1X512}$$

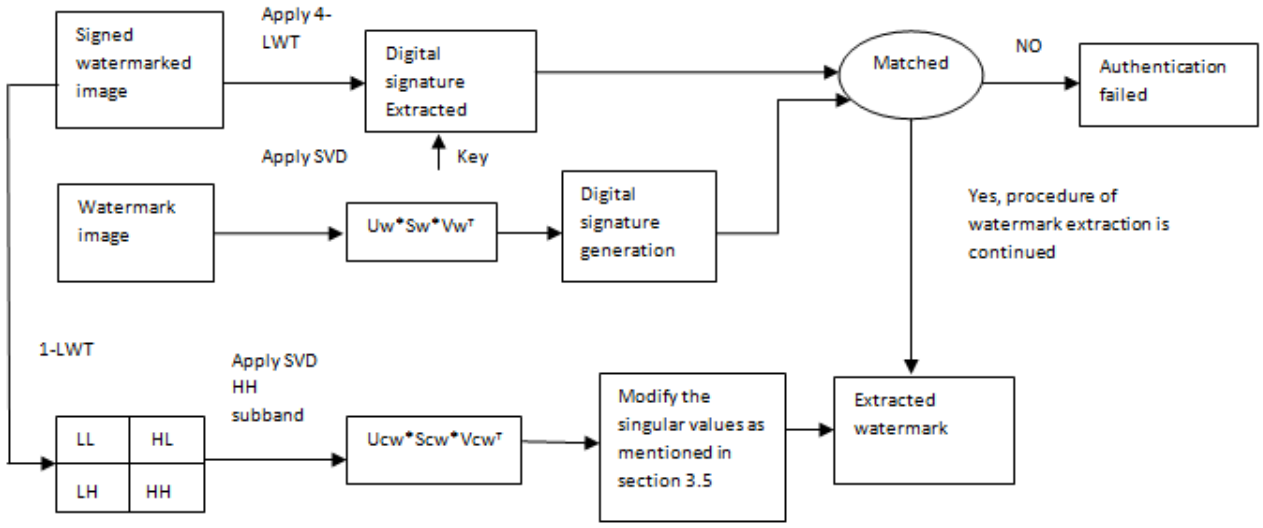

FIGURE 3 Procedure of watermark extraction

5. Divide $D_{\_modified}$ into two sections i.e. integer part and decimal fraction, by returning absolute value of each element in an array and rounds each elements towards zero, as follows

$K_{\_new}^{modified}$ = abs [$D_{\_modified}$]

Integer_ part = fix [$K_{new}^{modified}$]

Fraction part = abs ($K_{new}^{modified}$ - Integer_ part)

Then, convert integer elements into binary bits of length N=16.

6. Substitute the 10th bit position of coefficient by the generated signature bit and then transform binary code into its decimal number.
7. Reconstruct the original array from integer and fraction parts.
8. Perform Inverse LWT to obtain the signed watermarked image

A **B**

FIGURE 4 **(A)** Standard benchmark Images **(B)** Obtained Watermarked Images

3.3 SIGNATURE EXTRACTION

1. Using 1- LWT, decompose the watermarked image into four subbands.
2. Further decompose the LL subband by 3-level LWT.
3. Extract the signature from LL_{w_3} & HH_{w_3} bands by following procedure:

a) Select all the coefficients from LL_{w_3} and HH_{w_3} band and reshape them to a row vector

$LL_{\_3}^{modified}$ = [1: (LL_{w_3}) ^2]

$HH_{\_3}^{modified}$ = [1 :(HH_{w_3}) ^2]

b) Concatenate the above row vector as illustrated below

$D_{w\_modified}$ = $[LL_{\_3}^{modified}\ HH_{\_3}^{modified}]_{1\ X\ 512}$

4. Separate integer part from the fractional one then converted it into its binary code of L bits i.e. 16 bits.
5. Extract the 10th bit from the selected coefficients then comparison between the signatures extracted and generated is proceed.
6. If the signature bits are identical then authentication is successful and watermark extraction process is carried out but if authentication is failed then the procedure of extraction is stopped.

3.4 WATERMARK EMBEDDING

The block diagram of proposed algorithm is shown in Figure 2 and the corresponding steps are explained below:

1. 1-level LWT is applied for transforming the original image into subbands, namely LL, HL, LH and HH.
2. SVD is performed on HH subband as well as on the watermark logo and obtain the Singular Values as follows:

A_i (HH) = $U_i S_i V_i^T$

3. Exchange singular values (Si) by the Singular values (S_w) by using following conditions as follows.

If (length (watermark logo)) => 256)

S_i_diagonal (1: length (S_i), :) = S_w_diagonal (1:length(S_i) , :) ;

elseif (length (watermark logo) < 256)

S_i_diagonal (1: length (watermark),:) = S_w_diagonal(1: length(watermark), :) ;

4. Apply again 3- level LWT and further decompose LL subband.
5. Embed the digital signature generated into modified $LL_{\_3}$ and $HH_{\_3}$ subband as already explained in section 3.2.
6. The watermarked signed image is obtained after applying inverse LWT.

3.5 THE WATERMARK EXTRACTION PROCEDURE

Firstly, signature is extracted from the output watermarked image. If this extracted signature value is matched with the generated signature, then the watermark extraction procedure will be proceed otherwise, get stopped. The watermark extraction procedure is as follows:

1. Apply the 1-level LWT on watermarked image (A_W) and divide it into different subbands (LL, LH, LH and HH).
2. SVD is applied on HH subband as follows:

$Aw = U_{cw} S_{cw} V_{cw}^T$

3. Extract the watermark using conditions as follows:
4. Generate a zeros matrix of length of watermark image and select the diagonal values(S_{hw})

if length(watermark logo) >= 256

Shw_diagonal(1:length(Scw), :) = Scw_diagonal;

elseif length(watermark logo) < 256

Shw_diagonal(1:length(watermark logo), :) = Scw_diagonal(1:length(watermark logo), :);

End

5. Extract the singular values and build the watermark logo by utilizing extracted singular elements and orthogonal matrices.

4 Experimental setup and results

Matlab tool is used for simulation, evaluating the performance of the proposed LWT via SVD watermarking scheme. Ten different standard gray host images of size 512 X512 and watermark image of size 64 X 64 has been used to perform the experiments, shown in Figure. 4(A) and resultant watermarked images are given in Figure. 4(B).The two important characteristics that any watermarking scheme should posses are robustness and imperceptibility. The obtained simulation outcomes show the proposed scheme achieved high robustness and imperceptibility against different attacks which has been investigated by PSNR (Peak Signal to noise ratio) and NC (Normalized correlation coefficient). The PSNR is employed for evaluating imperceptibility i.e. the resemblance between the host image and the watermarked image according to the human visual system and is given as,

$$PSNR\ (dB) = 10 \log_{10} .(255^2 / MSE)_{HVS}, \quad (6)$$

$$MSE(\text{Mean Square error}) = \frac{1}{m.n} \sum\sum \|\boldsymbol{I}(\boldsymbol{i},\boldsymbol{j}) - \boldsymbol{K}(\boldsymbol{i},\boldsymbol{j})\|^2, \quad (7)$$

where I(i,j) = intensity pixels of original image
K(i,j) = intensity value of watermarked image and m,n are the dimentions of the image.

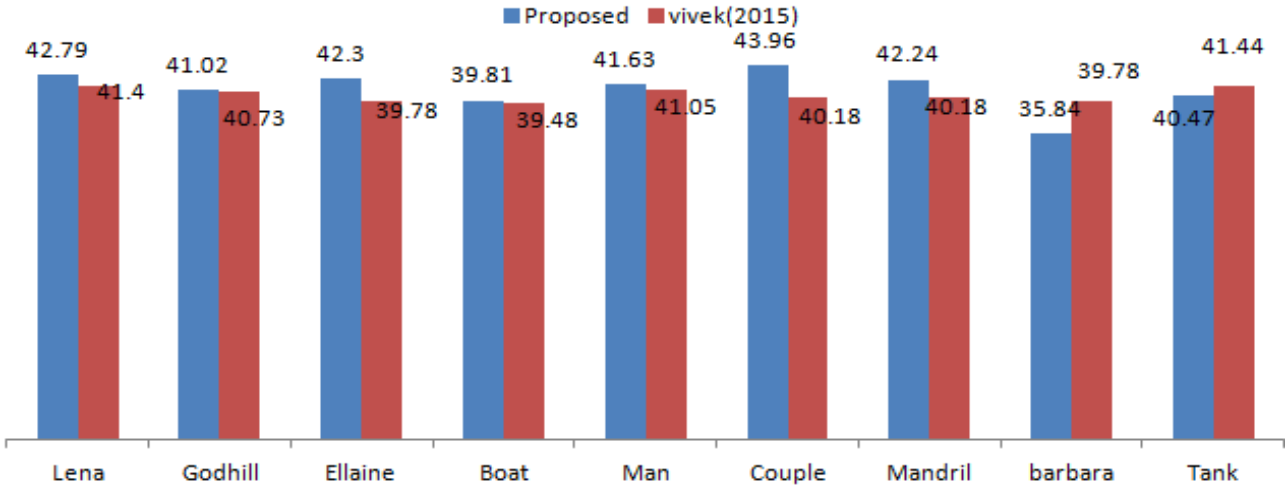

FIGURE 5 PSNR values of nine watermarked images as compared with the result of Vivek, et. al, 2015

Robustness of any watermarking technique is analysed on the basis of comparison between the original watermark and the extracted watermark image. To verify this NC is used and is given by eq.8.

TABLE 1 NC values of extracted watermark for different attacks over 10 standard images

Images	Attacks														
	Gs (0.01)	Sp (0.01)	Slp (0.05)	Rt(10°)	Rt(5°)	GaC (0.02)	Gu blr (13x13)	Mt blr (13,45°)	Avg (3x3)	Avg (5x5)	Md (5x5)	Md (7x7)	Shr -0.02	Cut (1/4)	Shrp (1.5,0.8)
Lena	0.966	0.9685	0.9072	0.9081	0.9069	0.875	0.8842	0.8893	0.8775	0.8791	0.8778	0.8802	0.9074	0.9474	0.8892
Godhill	0.9647	0.97	0.9145	0.898	0.879	0.9647	0.9625	0.9725	0.9667	0.9699	0.9702	0.9731	0.957	0.9776	0.9395
Barbara	0.9702	0.97	0.9167	0.8979	0.9073	0.9264	0.9334	0.9531	0.943	0.948	0.9476	0.953	0.9449	0.9626	0.9107
Man	0.951	0.946	0.9012	0.8941	0.8984	0.9116	0.9113	0.9402	0.915	0.918	0.9222	0.9281	0.9097	0.9482	0.9012
Boat	0.9737	0.9696	0.9083	0.8968	0.8886	0.9091	0.8911	0.9287	0.8963	0.8981	0.8889	0.9002	0.9123	0.9217	0.895
Zelda	0.9627	0.9695	0.9139	0.9015	0.889	0.9395	0.9345	0.9304	0.9401	0.9431	0.9405	0.9415	0.8969	0.9613	0.9323
Couple	0.9801	0.9834	0.8917	0.8951	0.9587	0.9565	0.962	0.984	0.9783	0.9812	0.9843	0.9757	0.9504	0.9682	0.9465
Mandril	0.9654	0.9685	0.9009	0.8938	0.8912	0.8815	0.9331	0.9143	0.9008	0.9016	0.9	0.8959	0.8923	0.945	0.895
Elaine	0.968	0.9702	0.9145	0.8799	0.8993	0.9095	0.9461	0.9703	0.9378	0.9417	0.9413	0.9446	0.9355	0.9678	0.9166
Tank	0.9662	0.9714	0.9245	0.8799	0.8993	0.9095	0.9461	0.9702	0.9352	0.9672	0.9725	0.9803	0.9081	0.9854	0.9205

$$NC = \frac{\sum_i \sum_j W(i,j).W'(i,j)}{\sum_i \sum_j [W(i,j)]^2} \quad (8)$$

where W (i,j) = Watermark image, W′ (i,j) = Extracted watermark image

4.1 (I). IMPERCEPTIBILITY

Ten different gray images are taken for evaluating the performance in terms of imperceptibility

a) When no attacks has been applied on these 10 benchmark images, the average of PSNR values comes to be above 35 dB which is considered to be a high perceptible value. It may be observed from the Figure 4(B) that the proposed scheme shows a good performance in terms imperceptibility. The compared result for PSNR value of proposed scheme with **vivek et. al (2015)** for 9 images are presented in Figure 5.

ii) Robustness test: The key feature of any watermarking technique is robustness. Table 1. presents the NC values for the extracted watermark when the watermarked images are subjected to different kinds of open attacks such as salt and pepper noise(Slp), Speckle noise(Sp), Gaussian noise(Gs), median filtering(Md), Average filtering(Avg), cropping(Cr), rotation(Rt), Gauss blur(Gu br), Motion Blur(Mt br), shearing attack(Sh), Gamma correction(GaC), Sharpening(Shrp), Cutting(Cut), compression(JPEG) and Table 2 presents the comparison of the proposed scheme with the existing technique (**vivek et.al,2015**) by comparing the NC values.

There are several attacks for manipulating an image and one of the well known attacks is addition of noise and from Figure 6 it can be observed that after adding the noise, watermarked image is degraded but the watermark is still recognized.

TABLE 2 The comparison results with **vivek et.al (2015)** for common image processing attacks. (NC)

Images → / Attacks ↓	Lena		Elaine		Boat		Man		Mandril	
	vivek	Proposed	vivek	Proposed	Vivek	Proposed	Vivek	Proposed	Vivek	Proposed
Avg(5X5)	0.7383	**0.8791**	0.6914	**0.9417**	0.6523	**0.9063**	0.5938	**0.918**	0.5	**0.9008**
Md(3X3)	0.9570	0.8794	0.9492	0.9421	0.9063	0.8937	0.9258	0.9159	0.875	**0.9005**
Gs(0.01)	0.9727	0.966	0.9414	**0.968**	0.9648	**0.9737**	0.957	0.951	0.9375	**0.9654**
Gs(0.02)	0.8555	**0.9553**	0.8594	**0.9557**	0.9141	**0.9515**	0.8711	**0.9282**	0.8984	**0.9445**
Slp(0.01)	0.7539	**0.9662**	0.8203	**0.9668**	0.7539	**0.9667**	0.7852	**0.9518**	0.8438	**0.9625**
Rt(0.1°)	0.8594	**0.8842**	0.8867	**0.9368**	0.7305	**0.8911**	0.707	**0.9113**	0.582	**0.9003**
Rt(0.2°)	0.4531	**0.8875**	0.457	**0.9345**	0.3047	**0.8894**	0.3203	**0.9054**	0.2891	**0.8995**
Cr(1/4)	0.9336	**0.9454**	0.9727	0.9339	0.9336	**0.9489**	0.9102	**0.9494**	0.9258	**0.9617**
Sp(0.01)	0.7461	**0.9685**	0.7734	**0.97**	0.8633	**0.9696**	0.8164	**0.946**	0.8008	**0.9685**
JPEG(10)	0.8789	**0.975**	0.8516	**0.9514**	0.7422	**0.9353**	0.7461	**0.9768**	0.6797	**0.9776**
JPEG(20)	0.9414	**0.9756**	0.9258	**0.9505**	0.918	**0.9427**	0.9297	**0.9781**	0.9063	**0.9754**
JPEG(30)	0.9922	0.9758	0.9805	**0.9882**	0.9883	0.9339	0.9727	**0.9771**	0.9766	**0.9773**
JPEG(40)	1	0.9761	0.9883	**0.9903**	0.9922	0.933	1	**1**	0.9961	0.977
JPEG(50)	1	**1**	1	**1**	1	**1**	1	**1**	1	**1**
JPEG(60)	1	**1**	1	**1**	1	**1**	1	**1**	1	**1**
JPEG(70)	1	**1**	1	**1**	1	**1**	1	1	1	**1**
JPEG(80)	1	1	1	**1**	1	1	1	**1**	1	**1**
JPEG(90)	1	1	1	1	1	1	1	**1**	1	1

The bold values specifies that this scheme shows better performance against the scheme (vivek et. al., 2015) under different attacks

The proposed algorithm also tested for rotation, sharpening, motion blur, shear attack, average filtering and median filtering as shown in Figure 7, Figure 8, Figure 9, Figure 10, Figure 12, Figure 13. The watermarked image is also tested with JPEG compression as shown in Figure 11.

A B

FIGURE 6 Result of salt & pepper noise (0.05)

A B

FIGURE 7 Result of rotation (10°)

A B

FIGURE 8 Result of sharpening (r=1.5, s=0.8)

A B

FIGURE 9 Result of motion blur (len=13, angle=45)

A B

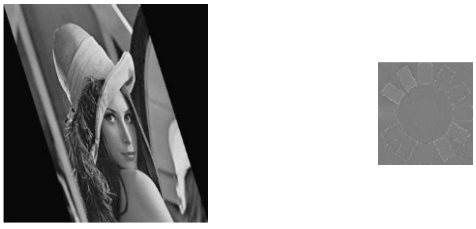

FIGURE 10 Result of shear attack (0.02)

A B

FIGURE 11 Result of Compression attack (QF=60)

A B

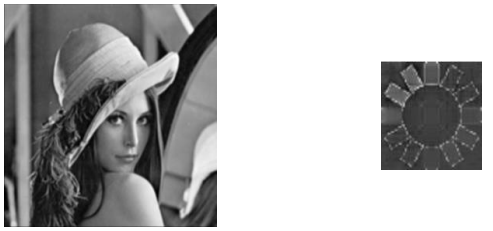

FIGURE 12 Result of average filtering (5x5)

A B

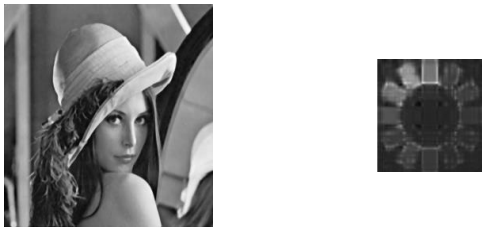

FIGURE 13 Result of median filtering (5x5)

A) Attacked image; B) Extracted watermark

5 Conclusion

This paper proposes a new watermarking technique based on LWT and SVD. For enhancing the security and robustness digital signature and secret key is used and embedded in the host image where the watermark image is already embedded into the subband which are achieved by N- level LWT and SVD. During the watermark extraction, first the extracted signature is matched with the original signature: if both the signature match then the extraction of watermark is continued otherwise it shows that the authentication failed and no watermark will be extracted. This scheme has been compared with the existing technique and it proves that the proposed technique is good enough on the basis of imperceptibility, robustness and security. Simulation result verified that the proposed scheme is robust against common image processing attacks.

References

[1] Cox I J, Kilian J, Leighton F, Shamoon T 1997 Secure Spread spectrum watermarking for multimedia *IEEE transaction on image processing* **6** 1673-87

[2] Liu R, Tan T 2002 An SVD based watermarking scheme for protecting rightful ownership *IEEE Trans. Multimed* **4** 121-8

[3] Ganic E, Eskicioglu A M 2004 *Robust DWT-SVD domain* image watermarking: embedding data in all frequencies In *Proceedings of ACM multimedia and security workshop, Magdeburg, Germany* 166-74

[4] Bhatnagar G, Jonathan Q, Wu M, Raman B 2012 A new robust adjustable logo watermarking scheme *Computer & security* **31** 40-58

[5] Bhatnagar G, Jonathan Q M Wu, Raman B 2012 Robust gray-scale logo watermarking in wavelet domain *Computers and Electrical Engineering* **38** 1164-76

[6] Ali M, Ahn CW 2014 An optimized watermarking technique based on self adaptive DE in DWT-SVD transform domain *Signal Processing* **94** 545-56

[7] Ali M, Ahn C W, Pant M, Siarry P 2015 An image watermarking scheme in wavelet domain with optimized compensation of Singular Value Decomposition Via artificial bee colony *Information Science* **301** 44-60

[8] Qi X, Xin X 2015 A singular value based semifragile watermarking scheme for image content authentication with tamper localization *J. Vis. Commun. Image R.* **30** 312-27

[9] Makbol N M, Khoo B E 2014 A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition *Digital signal processing* **33** 134-47

[10] Verma V S, Jha R K, Ojha A 2015 Significant region based robust watermarking scheme in lifting wavelet transform domain *Expert System with Applications* **42** 8184-97

[11] Dadkhah S, Manaf A A, Hori Y, Hassanien A E, Sadeghi S 2014 An efficient SVD-based image tampering detection & self recovery using active watermarking *Signal Processing: Image communication* **29** 1197-210

[12] Verma V S, Jha R K 2014 Improved watermarking technique based on significant difference of lifting wavelet coefficients *Signal, Image and Video Process* 1-8

[13] Barni M, Bartolini F, Piva A 2001 Improved wavelet based watermarking through pixel wise masking *IEEE Trans Image Process* **10**(5) 783-91

[14] Chandra D 2002 Digital image watermarking using singular value decomposition *In Proceedings of the IEEE 45th Midwest symposium on circuits & systems, Oklahoma state university, USA* 264-7

[15] Mohammad A M, Alhaj A, Shaltaf S 2008 An improved SVD-based watermarking scheme for protecting rightful ownership *Signal processing* **88** 2158-80

[16] Run R S, Horng S J, Lai J L, Kao T W, Chen R J 2012 An improved SVD based watermarking technique for copyright protection *xpert System with Applications* **39** 673-89

[17] Mishra A, Aggarwal C, Sharma A, Bedi P 2014 Optimized gray scale watermarking using DWT-SVD and firefly algorithm *Expert System with Applications* **41** 7858-67

[18] Keyvanpour M R, Bayat F M 2011 Robust dynamic block based image watermarking in DWT domain *Procedia computer science* **3** 238-42

[19] Lu W, Sun W, Lu H 2009 Robust watermarking based on DWT and non-negative matrix factorization *Computers and Electrical Engineering* **35** 183-8

[20] Hwang M S, Chang C C, Hwang K F 1999 A watermarking technique based on one way hash functions. *IEEE transactions on customer electronics* **45**(2) 286-94

[21] Alexander S, Scott D, Ahmet ME 2005 Robust DCT-SVD image watermarking for copyright protection: Embedding data in all frequencies *In proceedings of the 13th European signal processing conference (EUSIPCO2005), Turkey*

[22] Lagzian S, Soryani M, Fathy M 2011 A new robust watermarking scheme based on RDWT-SVD *Int. J.Intell.Inf.Process* **2**(1) 22-9

[23] Tay P, Havlicek J P 2002 Image watermarking using wavelets *IEEE* 258-61

[24] Kundur D, Hatzinakos D 1999 Digital watermarking for Telltale tamper proofing and authentication *In Proceedings of IEEE* 1167-80

AUTHORS

Pratibha Singh

Current position: Research Scholar, Department of Electronics and Communication, University of Allahabad, Allahabad, India
University studies: M. Tech from Department of Electronics and Communication, University of Allahabad, Allahabad, India
Scientific interest: Digital Communication, Image processing and Image watermarking.
Publications: 2 papers
Experience: 1 year of experience in Teaching

R.R.Tewari

Current position: Professor, Department of Computer Science, University of Allahabad, Allahabad, India
University studies: University of Allahabad, Allahabad, India
Scientific interest: Real Time systems, Wireless sensor Network, Mobile ad-hoc network, computer network and advanced computer architecture
Experience: 35 years