

A fast watermarking algorithm with enhanced security using compressive sensing and principle components and its performance analysis against a set of standard attacks

Falgun N. Thakkar¹ · Vinay Kumar Srivastava¹

Received: 31 March 2015 / Revised: 25 February 2016 / Accepted: 30 June 2016 /

Published online: 30 September 2016

© Springer Science+Business Media New York 2016

Abstract An algorithm for watermarking of digital images is proposed in this paper which utilizes Compressive Sensing (CS) with Principle Components (PCs) to achieve robustness, speed and security. CS is applied on PCs of watermark image to get the CS measurements. The singular values of these CS measurements are embedded with a scale factor into the HL subband of the cover image. The generated watermarked image contains three-layer security: one from PCs and other two from CS measurements. To recover PCs from CS measurements, a convex optimization tool, namely, the Orthogonal Matching Pursuit (OMP) is employed. Experiments are performed on both types of cover images; one with more low frequency components and another with more high frequency components. The algorithm offers state-of-the art values of robustness and security in presence of different checkmark attacks like geometrical, non-geometrical and JPEG compression. A comparison of robustness of proposed algorithm with existing algorithms reveals that the proposed algorithm outperforms for most of the noise attacks. The performance of proposed algorithm with different wavelet families (e.g., orthogonal, biorthogonal, symmetric and asymmetric) are compared in terms of robustness and execution time. Such comparison may be helpful in selecting a suitable wavelet for a class of cover images in presence of checkmark attacks. The Haar wavelet performs better for geometric noise attack whereas Bior6.8 and Sym8 for non-geometric and JPEG compression type of noise attacks. The execution time of proposed algorithm with Haar wavelet is found to be minimum for all checkmark attacks. Moreover, it is quite less as compared to Optimization based methods and close to the other watermarking technique used for H.264 video standard.

✉ Falgun N. Thakkar
falgunget@gmail.com

Vinay Kumar Srivastava
vinay@mannit.ac.in

¹ Electronics and Communication Engineering Department, Motilal Nehru National Institute of Technology, Allahabad 211004 Uttar Pradesh, India

Keywords Principle Component Analysis (PCA) · Compressive Sensing (CS) · Orthogonal Matching Pursuit (OMP) · Fast watermarking · Orthogonal and biorthogonal wavelet analysis · Checkmark attacks · Watermarking execution time

1 Introduction

In recent years, watermarking has become a very important part of multimedia communication through internet [11, 13, 14, 19, 21–23, 34, 37, 39]. In the absence of copyright protection, anyone can misuse the copyright material available through internet from any corner of the world [21]. The watermarking technology has its own advantages with which it can provide such protection to multimedia data. According to working domains, watermarking schemes can be divided into two categories, i.e. spatial domain and frequency domain. Frequency domain watermarking scheme can provide better robustness and embedding capacity as compare to spatial domain watermarking schemes [13]. In this paper, a frequency domain watermarking technique is proposed. A good watermarking scheme should carry the security of copyright content with sufficient robustness against geometric, non-geometric and compression types of attacks [14]. Singular Value Decomposition (SVD) based watermarking techniques [13, 14] have good robustness but fail in protecting rightful ownership [22, 34, 37]. Based on Principle Components (PCs) and wavelet transform, several improved SVD based models have been proposed [11, 19, 23, 39]. PC based watermarking techniques [11] provide assurance for rightful ownership but are very sensitive to any attack [21]. Thus, in the presence of attacks, robustness of such techniques becomes poor. In this technique, the scalar scale factor is not sufficient because of higher sensitivity of PCs against noise attacks and, therefore, each and every pixels of watermark image need individual scale factor. The scale factor required in this technique is two dimensional (2D) with same size as watermark image. Tuning of the scale factor matrix can be performed by using various optimization techniques such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and Differential Evolution (DE) [2, 8, 12, 21, 29, 31]. This scale factor is used to embed the PCs into the cover image to improve the robustness of the algorithm. Although the watermarking scheme based on combination of PCs and optimization technique are able to fulfill the requirements of good watermarking algorithms like robustness and rightful ownership, most of these optimization techniques are iterative in nature and require several iterations to obtain the optimum value of scale factor matrix. As a result, these iterative techniques require large computation time [21].

Candes and Donoho have given the Compressive sensing (CS) algorithm [3, 5], which becomes the breakthrough in sampling technique based on Nyquist theorem [25]. CS based watermarking algorithm is used for temper detection in [27] whereas this algorithm is applied to increase robustness with reduced set of measurements of watermark image in [18]. CS based technique has many desirable features like less computational complexity, security and robustness [32, 36, 38]. The computationally efficient CS based watermarking technique with different scrambling algorithm is implemented in [7, 28, 38]. Performance of CS based watermarking technique under additive white Gaussian noise and impulsive noise attack is mentioned in [35]. Better robustness and rightful ownership of CS based watermarking algorithm is presented in [6]. The watermarking for biometric data protection with CS is implemented in [25]. Double encrypted digital watermarking against Gaussian and shearing

attacks is proposed in [15] with two layer security. It is mentioned in [1] that, the non-blind watermarking scheme is more robust than blind watermarking scheme and required in applications such as automated search of original media.

From the above discussion it is clear that the CS based watermarking technique can reduce computational complexity and increase robustness of algorithm. Thus, in this paper, a CS based non-blind watermarking algorithm is proposed which focuses on robustness, computational complexity reduction and rightful ownership with multiple levels of security.

Literature depicts that, better robustness and rightful ownership is offered by combination of PCs and optimization technique like PSO or GA based algorithm [8, 12, 21, 29, 31]. But these algorithms provide only single level of security with large execution time burden due to scale factor matrix. To overcome the time burden in algorithms [10, 21, 24], lesser number of iterations have been chosen which may not always allow to reach to the global solution. So, their proposed scheme may not give better response in terms of robustness and imperceptibility. Therefore, to remove the drawbacks of PSO or GA based watermarking algorithm, a novel CS-PCs based technique is proposed in this paper. In this algorithm, CS is applied on PCs of watermark image to generate the CS measurements. Singular values of CS measurements modify the singular values of HL subband of cover image to obtain watermarked image. Proposed CS-PCs (CS measurement of PCs) based scheme offers state-of-the-art results in terms of execution time of watermarking algorithm, security and robustness. Moreover, use of scalar scale factor without any requirement of its optimization reduces the computational complexity of algorithm. In proposed algorithm CS is applied on the PCs of the watermark image which are to be embedded inside the cover image. In the proposed CS based algorithm, Gaussian random matrix Φ with circular shaped kernel [16] is applied on the PCs of watermark image to get linear CS measurements. These CS measurements can resist geometrical attacks.

The effectiveness of algorithm is also analyzed with cover images containing either more low frequency or more high frequency components. As the Orthogonal Matching Pursuit (OMP) algorithm is fast [25] as compared to recovery algorithms like l_1 minimization, it is used in this paper to recover the PCs from its CS measurements.

In [5], Brannock et al. found that while watermarking with non-colored watermark image, the simpler wavelet transform like Haar performs better. In this paper, the performance analysis of proposed watermarking technique with orthogonal and biorthogonal wavelets including Haar transform is carried out. Analysis shows that, the effectiveness of wavelet family does not depend on the type of watermark but depends on the wavelet transform that is used in the watermarking scheme. In the proposed algorithm, study shows that in addition to the Haar wavelet other wavelet families also perform better for non-colored watermarks. Moreover, the performance also varies with change in type of cover image and different group of attacks.

The remaining paper is organized as follows: In section 2, a brief preliminary on compressive sensing (CS), singular value decomposition (SVD) with PCs and wavelet transform is presented. The security aspect of proposed algorithm is given in section 3. Section 4 contains the implementation of CS-PCs based proposed algorithm with a variety of cover images and its performance is tested in the presence of checkmark attacks. Moreover the experiment also includes execution time analysis with different wavelet family. The result and discussion for robustness, computational complexity and performance under various noise attacks are given in section 5. Finally the conclusions are mentioned in section 6.

2 Preliminaries

2.1 Compressive sensing

A signal x in R^N can be defined in terms of basis vectors with dimension $N \times I$. It can become sparse signal when only k entries of x are non-zero, where $k < M$ and $M < N$. The signal has k number of nonzero coefficients, so to remove this redundancy the x can be represented as

$$S = \varphi x \quad (1)$$

where signal S is the column vector of weighed coefficients in the φ domain with dimension $N \times I$. φ is basis matrix having dimension $N \times N$ [3]. The sparse representation of data x can be defined by equation

$$x = \varphi^T S \quad (2)$$

The sampling of data in an unconventional way is known as compressive sensing, which is represented by the following equation [33]

$$y = \Phi S \quad (3)$$

where Φ is known as the random measurement matrix having dimension $M \times N$ with $M < N$ and y is measurement vector with dimension $M \times I$.

The Eqs. (1) to (3) can be combined in following consolidated form

$$y = \Phi S = \Phi \varphi x = Cx \quad (4)$$

where $C = \Phi \varphi$ is the matrix with dimension $M \times N$, φ is a matrix for creating sparse data set and matrix Φ is the random measurement matrix.

It is necessary for matrix Φ to satisfy restricted isometric property (RIP) with order k to recover signal x perfectly from M measurements which is given by following equation

$$(1 - \delta_k) \|x\|_2^2 \leq \|\Phi x\|_2^2 \leq (1 + \delta_k) \|x\|_2^2 \quad (5)$$

where $\delta_k \in (0, 1)$ and $x \in \Sigma_k$, where $\Sigma_k = \{x : \|x\|_0 \leq k\}$

To recover the signal from random measurements a greedy algorithm is used which is theoretically and empirically given by Tropp et al. [26]. This algorithm is known as orthogonal matching pursuit (OMP). As this algorithm is faster and simpler to implement, it is used in this paper for the recovery of sparse signal set from measurement vectors. The OMP is a technique to find the solution of least square problem which can be defined mathematically by the following equation

$$\hat{x} = \underset{x}{\operatorname{argmin}} \|y - \Phi x\|_2 \quad (6)$$

where \hat{x} is the unique solution of least square problem which provides the recovery of signal from the random measurement vector y .

2.2 Discrete wavelet transform

The discrete wavelet transform (DWT) decompose the signal into different frequency subbands. In image processing algorithms, it plays a vital role because its decomposition

follows the anisotropic properties of human visual system (HVS) [4]. DWT offer multiple levels [12] of decomposition which gives freedom to embed data at desired position. DWT is mainly used in the watermarking schemes to increase its robustness. In watermarking, components of watermark can be embedded in selected subbands of cover image in such a way that they can be protected from different kinds of noise attacks. The different wavelet filters are used to decompose the signal into different frequency subbands. Popular wavelet filters are Haar, Daubechies, Coiflet, Bior and Symlet. Wavelet filters can also classified with different properties like orthogonal, biorthogonal, symmetrical and asymmetrical. Various wavelet filters perform differently for any particular algorithm therefore, choosing suitable wavelet for various algorithms is an important research issue.

First-level wavelet decomposition of the image produces four different frequency subbands denoted by LL, LH, HL and HH. The subband LL contains the lower frequency information and remaining three contains the higher frequency information of the image. Further levels of LL subband decomposition produces more frequency subbands. The watermark image can be embedded in any of the frequency subband to get some desirable properties in the watermarking algorithm. The watermarks embed into the low frequency subband (LL) are robust in presence of various image processing attacks whereas embedding in high frequency subbands (HH) improves the perceptual quality of watermarked image. Use of intermediate frequency subbands (LH and HL) provides the tradeoff between perceptual quality of watermarked image and robustness against the range of attacks.

2.3 Singular value decomposition

In linear algebra, the singular value decomposition (SVD) is a tool which decomposes the input matrix into three matrices. The image is a matrix of pixel values which are non-negative [21]. If SVD is applied on image A with dimension $M \times N$, the three generated matrices can be define by the following equation

$$A = USV^T \quad (7)$$

In Eq. (7) the matrix ‘ S ’ is a diagonal matrix with dimension $M \times N$, which contains the singular values of image A along the diagonal and the other elements are zero. It is also known as the set of luminance values of image A . The matrix U with dimension $M \times M$ and matrix V with dimension $N \times N$ are orthogonal matrices, also known as left and right singular values respectively. Here U represents the horizontal and V represents the vertical detail of respective image [19, 21]. The matrix formulation of Eq. (7) is given as

$$A = \begin{pmatrix} U_{1,1} & \cdots & U_{1,M} \\ U_{2,1} & \cdots & U_{2,M} \\ \vdots & \ddots & \vdots \\ U_{M,1} & \cdots & U_{M,M} \end{pmatrix} \begin{pmatrix} \sigma_{1,1} & 0 & 0 \\ 0 & \sigma_{2,2} & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_{M,N} \end{pmatrix} \begin{pmatrix} V_{1,1} & \cdots & V_{1,N} \\ V_{2,1} & \cdots & V_{2,N} \\ \vdots & \ddots & \vdots \\ V_{N,1} & \cdots & V_{N,N} \end{pmatrix}^T$$

SVD is used in the watermarking due to its stability property which state that a large variation in the singular values does not occur if small perturbation is add inside the image. Moreover the properties of SVD such as invariance of non-zero singular values of a matrix under transformations like transpose, translation, flip and rotation make it more popular in various algorithms of image processing. The product of matrices US , in Eq. (7) is known as the principle components (PCs) of the image [11]. In proposed algorithm, CS is applied on PCs of

watermark image to get more layers of security. These CS measurements of PCs of watermark are named as CS-PCs measurements of watermark.

3 Three layer security – an application scenario of proposed algorithm

In this paper, a robust and imperceptible watermarking algorithm is proposed which has three layers of security. This proposed scheme can be used for different applications. One such possible application scenario of proposed algorithm is given in Fig. 1 and described below.

User A is the super user who is having all the rights of watermark content with top secret Key 1 along with key 2 and 3. This user can extract the secret watermark data by these three keys using the data received from channel. In case if the super user A receives the malicious data, secret watermark data will not be detected. Therefore, this user sends a request to the transmitter for stopping the transmission. Super user can also distribute the rights of secret watermark data to different users in the local channel with different levels of securities. Users B, C, D and E can get the secret watermark data from super user A and extract it with respective rights. Suppose, any one of the user is not able extract the watermark due to malicious attack, the user sends request signal to the super user A for stopping the transmission towards that local channel. Here, as users B and E are having only the key 3, the super user A sends the secret watermark data extracted by key 1 and 2 to these users. The users C and D are having key 2 and 3, so the super user A transmit them a secret watermark data after extracting it by the top secret key 1. These users can further transmit secret watermark data after extracting it by key 2 to the users like F, G, H and I having the key 3 through other local channel. This user will not be able to extract the secret watermark data if there is any malicious attack. As a result of this, respective users send a request signal to the user C or D for stopping the transmission. Moreover, as no one from the authenticated group of users are having top secret key 1, so they cannot bypass the super user A for extracting the secret watermark data. If user J attacks the secret watermark data and tries to retransmit over the channel; then any authenticated user, on receiving it, may send a request to super user A for stopping the transmission.

4 Proposed method

The speed of internet is increasing rapidly as it has reached to fourth generation and beyond. Therefore, the watermarking algorithms based on time consuming optimization techniques may not be suitable in high-speed applications. To achieve better performance in terms of robustness and rightful ownership, the need for watermarking algorithms employing PCs and optimization technique has been highlighted in several recent literatures [21, 29]. Such techniques inherently suffer from the problem of time burden [10, 21, 24]. Moreover, the use of single layer of security in [10, 21, 24] may not be sufficient for smart malicious attacks. Thus, the main requirements for any fast watermarking scheme are less response time, more robustness and security.

The watermarking technique based on PCs (reliable SVD) protects rightful ownership and removes the false-positive problem of SVD based watermarking algorithms [11]. PCs embedded inside the cover image makes this technique less robust as they are sensitive to any attack which may largely change these values [21]. For this PCs based algorithm, lack of proper

selection method for scale factor leads to poor robustness for smaller value of scale factor whereas the larger value of scale factor leads to poor imperceptibility [21]. Therefore, simultaneously better robustness and imperceptibility could not be achieved with PCs based watermarking algorithm alone. To solve this problem, many researchers have used 2D scale factor to embed the watermark inside the cover image which need optimization technique [21, 29]. These approach removes the problem of robustness in the PCs based watermarking algorithms, but require more execution time. The performance of algorithms [10, 21, 24], is limited as less number of iterations are selected to overcome the time burden.

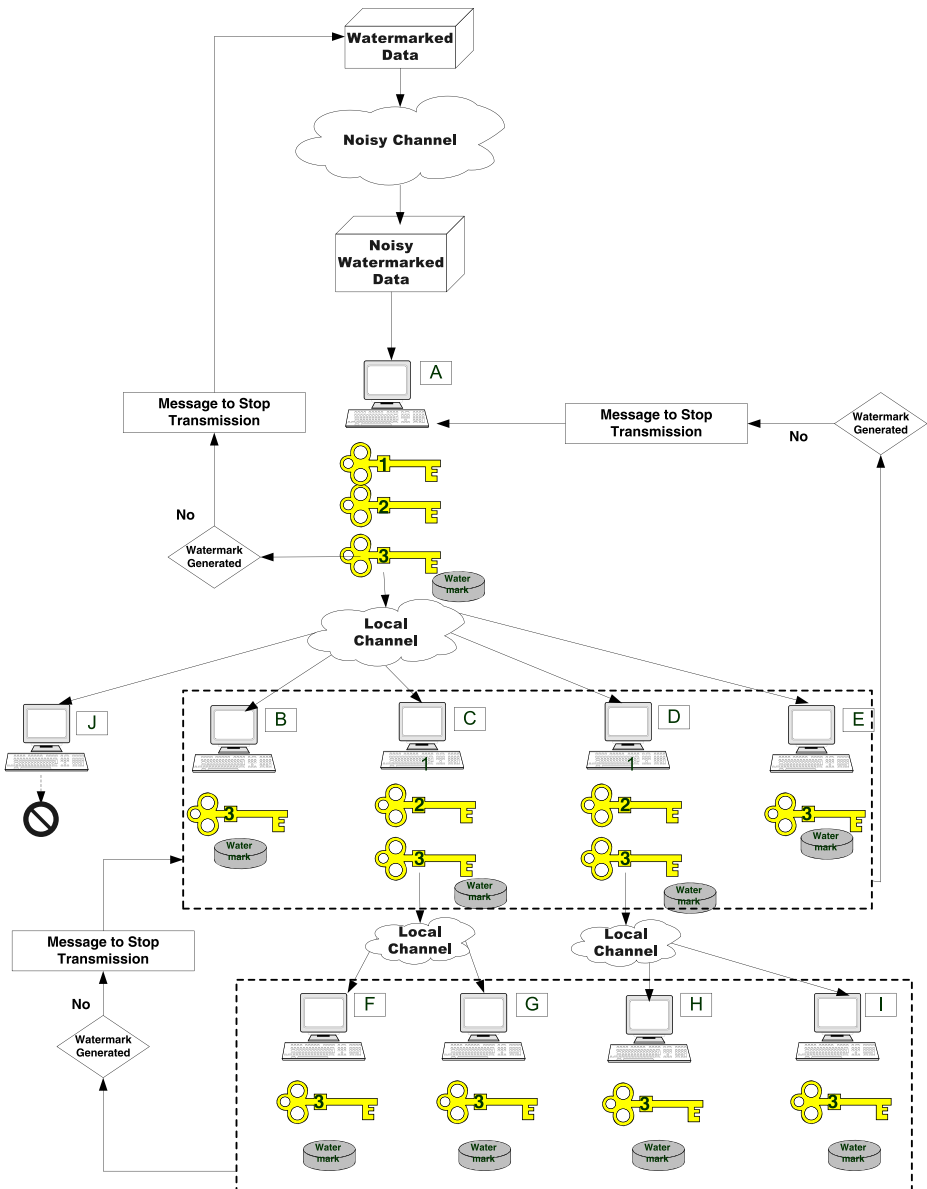


Fig. 1 Three layer security scheme for watermark data

The random sampling of the signal and sparsity are the popular approach for robustness enhancement [32]. As shown in [33], the random Gaussian matrix used in CS is capable of acquiring the information of the signal and the retrieval of clear signal is not possible without this sensing matrix. Also, it is mentioned in [36] that ‘Nowadays where security has prime significance the CS based cryptography systems are rigorously used’. Inspired by the existing works [32, 33, 36], in the proposed algorithm, CS is incorporated in the PCs based watermarking technique. This leads to better robustness and imperceptibility without increasing the execution time burden. It is demonstrated in [38] that compressive sensing can be used as a tool to achieve better robustness, imperceptibility and anti-attack capability in image watermarking algorithm. Moreover, two layer of security is achieved in image watermarking using CS measurements in [15]. Therefore to take the benefit of rightful ownership protection by PCs and to reduce execution time, CS is used with PCs in our proposed scheme. Here, the random measurement matrix is applied on the PCs of the watermark image to get linear measurements. These linear measurements carry the transformed PCs of watermark which are more robust as compared to original PCs. The singular values of these linear measurements are embedded inside the cover image which uses a scalar scale factor for any type of cover image or noise attack.

So, in the proposed algorithm CS is used with PCs which does not use any optimization technique to get suitable scale factor and hence it requires less execution time. Moreover, the use of CS not only increases the robustness of the watermarking scheme but also provides the rightful ownership protection. The conceptual diagram of proposed embedding algorithm is given in Fig. 2.

In this section, the embedding and extraction schemes of the proposed watermarking algorithm are described. Moreover, execution time and robustness analysis based on different wavelet families will be discussed in next section.

4.1 Watermark embedding process

The PCs, $U_w \Sigma_w$ of watermark image w is transformed to the domain of Random measurement matrix Φ and orthogonal matrix φ . As a result of this, linear CS measurement vector Y is generated. The singular value Σ_{wm} of the CS measurement vector Y is embedded inside the HL subband of the cover image C , which is used to provide the three layers of security in

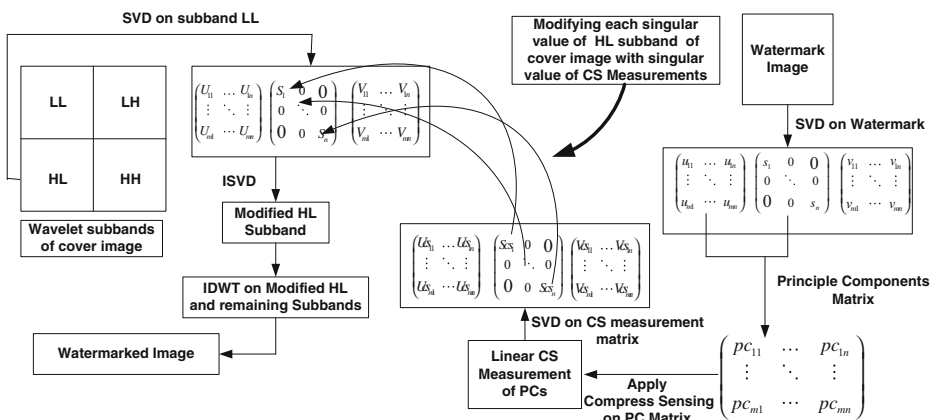


Fig. 2 The conceptual diagram of proposed embedding algorithm

watermarking scheme. Figure 3 shows the block diagram for the proposed embedding process and the mathematical steps for this scheme are as follows:

Step 1: Apply the singular value decomposition on the watermark image w , to get the principle components.

$$w = U_w \Sigma_w V_w'$$

in above equation the matrix product $(U_w \Sigma_w)$ is the PCs of the watermark image.

Step 2: Apply DCT as an orthogonal transform on the PCs of the watermark image to get the sparse data set for compress sensing

$$S = \varphi(U_w \Sigma_w) = DCT(U_w \Sigma_w)$$

Step 3: Apply Gaussian random matrix Φ on the sparse data set S of PCs of watermark image column wise, which is giving the measurement vector Y

$$Y = \Phi(S)$$

Step 4: Apply SVD on linear measurement vector Y , to generate the singular value of measurement vector Σ_{wM}

$$Y = U_{wM} \Sigma_{wM} V_{wM}'$$

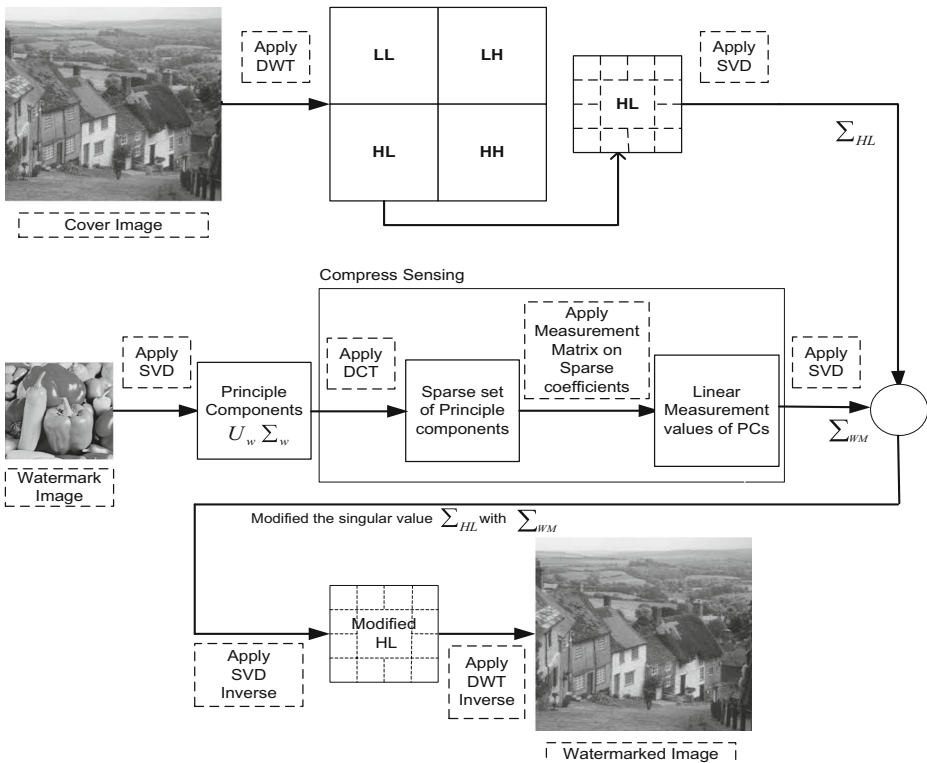


Fig. 3 Block diagram of proposed watermark embedding technique

Step 5: Apply first level of DWT on the cover image C , to get the four subbands (LL, LH, HL, HH). Apply SVD on the HL subband to get its singular values Σ_{HL}

$$C_{HL} = U_{HL}\Sigma_{HL}V'_{HL}$$

Step 6: Modify the Σ_{HL} with Σ_{wM} to embed the watermark content in the cover image

$$\overline{\Sigma}_{HL} = \Sigma_{HL} + \alpha * \Sigma_{wM}$$

Step 7: Apply inverse SVD to get the modified subband HL of cover image

$$U_{HL}\overline{\Sigma}_{HL}V'_{HL} = C^*_{HL}$$

Step 8: Apply inverse wavelet transform with modified wavelet subband HL to get the watermarked image C^*

4.2 Checkmark attacks

Unique checkmark attacks are used to achieve uniform performance comparison of various watermarking algorithms. Therefore, in this paper, unique checkmark attacks based on stirmark benchmark [20] are used. These attacks are divided in different categories like Denoising, geometrical, watermark copy, compression and de-synchronization.

Checkmark attacks like geometrical, non-geometrical and compression are applied on watermarked images. These noisy watermarked images at the receiving end are checked using security keys by user at various stages. After successful authentication, the copyright watermark is available to authorized user. The steps for the proposed extraction process are discussed in the following sub section.

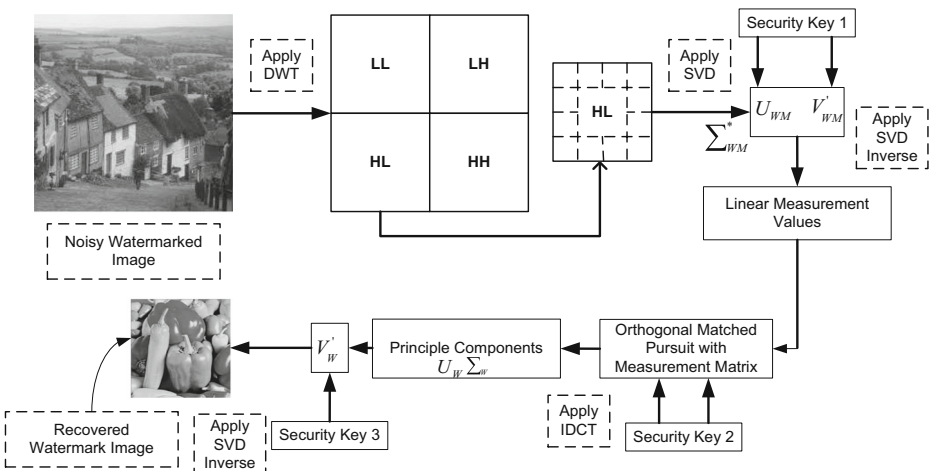


Fig. 4 Block diagram of proposed watermark extraction technique

4.3 Watermark extraction process

To recover the watermark from noisy watermarked image the orthogonal matrices of linear measurement vector, random measurement matrix and the right singular matrix of the watermark image are required. The OMP algorithm is used to recover the PCs from the linear measurement values. Figure 4 shows the block diagram for the proposed extraction process. The mathematical steps for this scheme are as follows:

Step 1: Apply wavelet transform on the noisy watermarked image and generate the modified subband HL. Perform SVD decomposition on HL subband to generate the modified singular value as $\overline{\Sigma}_{HL}^*$

$$C_{HL}^* = U_{HL}^* \overline{\Sigma}_{HL}^* V_{HL}'^*$$

Step 2: Recover the singular values Σ_{wM} of linear measurements of PCs of the watermark image using the modified singular value $\overline{\Sigma}_{HL}^*$ as

$$\Sigma_{wM}^* = \left(\overline{\Sigma}_{HL}^* - \Sigma_{HL} \right) / \alpha$$

Step 3: Generate the linear measurement vector Y using the right and left singular matrices, U_{wM} and V_{wM} (security key-1) along with recovered singular matrix Σ_{wM}^*

$$U_{wM} \Sigma_{wM}^* V_{wM}' = Y$$

Step 4: The measurement matrix, Φ which is used as security key-2 and recovered Y reproduce the sparse data set S of the PCs column wise with the help of OMP algorithm. Further apply inverse DCT on sparse dataset S to generate PCs of watermark image

$$S = OMP(\Phi, Y)$$

$$U_w^* \Sigma_w^* = IDCT(S)$$

Step 5: Apply inverse SVD on recovered PCs and right singular matrix V_w , (security key-3) to extract the watermark image w^*

$$U_w^* \Sigma_w^* V_w' = w^*$$

5 Experimental results and discussion

The experimental results for the CS-PCs based watermarking algorithm along with test images and performance measures are discussed in this section. The characteristic of various types of cover image and watermark image is discussed in subsection 5.1. The performance measures like MSE, PSNR and NC are explained in subsection 5.2. In subsection 5.3, the robustness and perceptual quality of the proposed scheme with Haar wavelet in the presence of variety of

checkmark attacks is presented. The effect of using symmetric, asymmetric, orthogonal and non orthogonal wavelets on the robustness of extracted watermark is discussed in subsection 5.4. Comparison of execution time of algorithm with different wavelets in the presence of variety of noise attacks, and its suitability with video standard H.264 is presented in subsection 5.5. The robustness of proposed algorithm is compared with the PSO based watermarking scheme in subsection 5.6.

5.1 Cover and watermark images

The performance of any watermarking algorithm may vary with the different types of input images. Therefore in this paper, the algorithm is tested for two different types of cover images. Cameraman image contains majority of low frequency components whereas Goldhill image contains high frequency components. Moreover, the analysis is also carried out with different noise attacks and wavelet families on different types of cover images.

In Fig. 5, Cameraman and Goldhill cover images having dimension 512×512 and Peppers watermark image with dimension 256×256 are shown. Use of peppers image as a watermark along with different types of cover images shows the performance of proposed algorithm under the mixture of different frequency components in the watermark image.

5.2 Performance measures

The normalized correlation (NC) is the parameter which measures the similarity between original watermark image (w) and extracted watermark image w^* . Mathematical formula [21] of NC is given in Eq. (8).

$$NC = \frac{\sum_{i=1}^N \sum_{j=1}^N (w_{ij} - \bar{w}) (w_{ij}^* - \bar{w}^*)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^N (w_{ij} - \bar{w})^2} \sqrt{\sum_{i=1}^N \sum_{j=1}^N (w_{ij}^* - \bar{w}^*)^2}} \quad (8)$$

where, $\bar{w} = \frac{1}{N^2} \sum_{i=1}^N \sum_{j=1}^N w_{ij}$ and $\bar{w}^* = \frac{1}{N^2} \sum_{i=1}^N \sum_{j=1}^N w_{ij}^*$



Fig. 5 The cover images (a) Cameraman which has low frequency majority contents (b) Goldhill which has high frequency majority contents, and the watermark image (c) Peppers which has nearly equal low and high frequency contents

Table 1 The attack analysis of proposed algorithm (with Haar wavelet) for different values of scale factor with Median filtering and Gaussian filtering in terms of NC values of extracted watermark and execution time T1 and T2

Scale Factor used for embedding	Attacks											
	Median Filter (3 × 3)			Median Filter (5 × 5)			Median Filter (7 × 7)			Gaussian Filter (3 × 3)		
	NC	Execution Time (in sec.)		NC	Execution Time (in sec.)		NC	Execution Time (in sec.)		NC	Execution Time (in sec.)	
		T1	T2		T1	T2		T1	T2		T1	T2
Cameraman Cover Image												
0.02	0.8168	0.42	4.91	0.8430	0.40	4.99	0.8753	0.38	4.87	0.9390	0.39	4.85
0.03	0.8459	0.40	4.89	0.8726	0.39	4.87	0.9079	0.39	4.85	0.9574	0.40	4.83
0.04	0.8716	0.40	5.08	0.9044	0.40	4.9	0.9262	0.39	4.86	0.9670	0.38	4.84
0.05	0.8996	0.39	4.91	0.9306	0.39	4.85	0.9395	0.39	4.83	0.9724	0.39	4.85
Goldhill Cover Image												
0.02	0.9178	0.38	4.87	0.8852	0.4	4.87	0.9157	0.4	4.85	0.9668	0.4	4.88
0.03	0.9483	0.39	4.93	0.9344	0.39	5.03	0.9452	0.4	4.86	0.9761	0.39	4.82
0.04	0.9649	0.39	4.84	0.9599	0.4	4.83	0.9609	0.39	4.85	0.9805	0.38	4.83
0.05	0.9726	0.39	4.84	0.9708	0.39	4.86	0.9680	0.38	4.82	0.9828	0.38	4.88

Table 2 The attack analysis of proposed algorithm (with Haar wavelet) for different values of scale factor with Average filtering, sharpening and Histogram equalization in terms of NC values of extracted watermark and execution time

Scale Factor used for embedding	Attacks											
	Average Filter (3 × 3)			Average Filter (5 × 5)			Sharpening			Histogram Equalization		
	NC	Execution Time (in sec.)		NC	Execution Time (in sec.)		NC	Execution Time (in sec.)		NC	Execution Time (in sec.)	
		T1	T2		T1	T2		T1	T2		T1	T2
Cameraman Cover Image												
0.02	0.8475	0.39	4.87	0.9046	0.41	4.81	0.9705	0.39	4.84	0.8583	0.38	4.78
0.03	0.8880	0.42	4.88	0.9233	0.42	5.18	0.9789	0.38	4.81	0.8605	0.36	4.80
0.04	0.9175	0.46	4.99	0.9372	0.39	4.91	0.9823	0.38	4.80	0.8578	0.38	4.80
0.05	0.9417	0.42	4.93	0.9478	0.39	4.87	0.9840	0.40	4.80	0.8554	0.38	4.80
Goldhill Cover Image												
0.02	0.9294	0.38	4.82	0.9458	0.42	4.91	0.9781	0.39	4.83	0.9621	0.40	4.78
0.03	0.9659	0.39	4.88	0.9593	0.39	4.95	0.9827	0.38	4.80	0.9516	0.37	4.80
0.04	0.9788	0.38	4.96	0.9681	0.39	4.84	0.9847	0.38	4.79	0.9393	0.37	4.80
0.05	0.9839	0.39	4.88	0.9738	0.39	4.83	0.9857	0.38	4.82	0.9312	0.36	4.81

Table 3 The attack analysis of proposed algorithm (with Haar wavelet) for different values of scale factor against Rotation and Gaussian noise in terms of NC values of extracted watermark and execution time

Scale Factor used for embedding	Attacks											
	Rotation (0.25°)		Rotation (-0.25°)		Rotation (0.2°)		Gaussian Noise (Variance = 0.01)					
	NC	Execution Time (in sec.)	NC	Execution Time (in sec.)	NC	Execution Time (in sec.)	NC	Execution Time (in sec.)				
	T1	T2	T1	T2	T1	T2	T1	T2				
Cameraman Cover Image												
0.02	0.9117	0.39	4.79	0.9566	0.38	4.78	0.9013	0.38	4.83	0.8183	0.40	4.94
0.03	0.9330	0.38	4.79	0.9739	0.37	4.79	0.9213	0.38	4.83	0.8296	0.40	4.99
0.04	0.9408	0.37	4.81	0.9792	0.38	4.85	0.9289	0.39	4.81	0.8322	0.39	4.97
0.05	0.9441	0.38	4.77	0.9810	0.38	4.80	0.9329	0.38	4.80	0.8340	0.38	4.98
Goldhill Cover Image												
0.02	0.9394	0.38	4.78	0.9840	0.38	4.80	0.9433	0.38	4.79	0.7816	0.37	4.8
0.03	0.9609	0.38	4.79	0.9850	0.38	4.79	0.9623	0.38	4.80	0.8405	0.39	4.79
0.04	0.9696	0.37	4.79	0.9849	0.37	4.80	0.9694	0.38	4.79	0.8563	0.37	4.79
0.05	0.9735	0.38	4.82	0.9846	0.38	4.81	0.9730	0.37	4.81	0.8695	0.37	4.78

The value of NC lies in between 0 and 1. The NC = 1 shows that the extracted watermark is exactly equal to the original watermark. The imperceptibility of

Table 4 The attack analysis of proposed algorithm (with Haar wavelet) for different values of scale factor with scaling, cropping and Salt & pepper in terms of NC values of extracted watermark and execution time

Scale Factor used for embedding	Attacks								
	Scaling (512-256-512)			Cropping (25 %)			Salt & Pepper Noise (0.01)		
	NC	Execution Time (in sec.)		NC	Execution Time (in sec.)		NC	Execution Time (in sec.)	
		T1	T2		T1	T2		T1	T2
Cameraman Cover Image									
0.02	0.8179	0.38	4.82	0.9509	0.38	4.82	0.8068	0.38	4.79
0.03	0.8329	0.37	4.81	0.9748	0.37	4.83	0.8225	0.37	4.88
0.04	0.8472	0.37	4.80	0.9826	0.38	4.80	0.8283	0.38	4.80
0.05	0.8596	0.37	4.82	0.9856	0.40	4.82	0.8298	0.38	4.82
Goldhill Cover Image									
0.02	0.8698	0.38	4.85	0.9767	0.40	4.81	0.7557	0.40	4.81
0.03	0.8857	0.39	4.82	0.9824	0.39	4.79	0.8226	0.37	4.83
0.04	0.8988	0.39	4.78	0.9840	0.38	4.80	0.8442	0.39	4.82
0.05	0.9102	0.37	4.82	0.9844	0.38	4.85	0.8567	0.37	4.81

Table 5 The attack analysis of proposed algorithm (with Haar wavelet) for different values of scale factor with JPEG compression in terms of NC values of extracted watermark and execution time

Scale Factor used for embedding	Quality Factor Q =10		Quality Factor Q =30		Quality Factor Q =50		Quality Factor Q =70		Quality Factor Q =90						
	Execution Time (in sec.)		Execution Time (in sec.)		Execution Time (in sec.)		Execution Time (in sec.)		Execution Time (in sec.)						
	T1	T2	NC	NC	NC	NC	NC	NC	NC	NC					
Cameraman Cover Image															
0.02	0.9394	0.40	5.03	0.9425	0.39	4.86	0.9470	0.38	4.84	0.9518	0.39	4.83	0.9568	0.39	4.83
0.03	0.9482	0.38	4.99	0.9580	0.39	4.85	0.9631	0.40	4.83	0.9668	0.38	4.83	0.9703	0.38	4.83
0.04	0.9559	0.38	4.87	0.9660	0.38	4.84	0.9710	0.38	4.84	0.9739	0.38	4.86	0.9765	0.37	4.88
0.05	0.9590	0.39	4.84	0.9718	0.39	4.84	0.9759	0.37	4.82	0.9783	0.38	4.88	0.9801	0.38	4.83
Goldhill Cover Image															
0.02	0.9806	0.38	4.82	0.9746	0.38	4.80	0.9709	0.38	4.84	0.9695	0.38	4.80	0.9723	0.39	4.87
0.03	0.9835	0.38	4.84	0.9763	0.38	4.84	0.9749	0.39	4.83	0.9760	0.39	4.82	0.9793	0.38	4.83
0.04	0.9832	0.38	4.83	0.9777	0.38	4.83	0.9772	0.38	4.83	0.9798	0.39	4.82	0.9822	0.38	4.85
0.05	0.9828	0.39	4.84	0.9788	0.37	4.85	0.9798	0.37	4.84	0.9817	0.38	4.84	0.9839	0.39	4.83

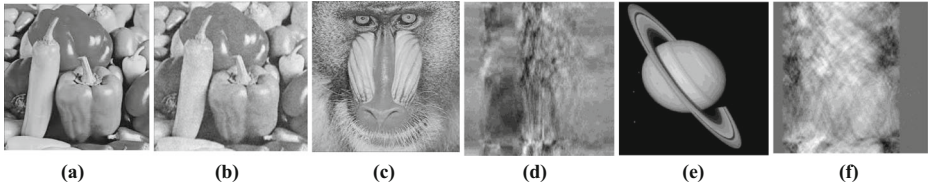


Fig. 6 Watermark images (a) Authenticate original watermark image pepper (b) Recovered watermark image pepper from orthogonal matrix of image a (c) baboon image (d) Imperceptible image display by the algorithm with the use of orthogonal matrix of image c (e) Saturn Image (f) Imperceptible image display by the algorithm with the use of orthogonal matrix of image e

watermarked image is evaluated by peak signal-to-noise ratio (PSNR) given in equation below

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \tag{9}$$

where mean square error (MSE) is defined as

$$MSE = \frac{1}{M^2} \sum_{i=1}^M \sum_{j=1}^M [H(i, j) - H^*(i, j)]^2$$

where the H and H* are the original cover image and watermarked image.

5.3 Robustness and perceptual quality analysis with copyright verification

The CS-PCs measurements of watermark image are embedded inside the HL subband of Haar wavelet transform applied on cover image. To check the robustness of watermarking

Table 6 The attack analysis of proposed algorithm (with bior6.8 wavelet) for different values of scale factor with median filtering, JPEG compression and Gaussian noise in terms of NC values of extracted watermark and execution time

Scale Factor used for embedding	Attacks								
	Median Filter (3 × 3)			JPEG (Q= 30)			Gaussian Noise (Variance = 0.01)		
	NC	Execution Time (in sec.)		NC	Execution Time (in sec.)		NC	Execution Time (in sec.)	
		T1	T2		T1	T2		T1	T2
Cameraman Cover Image									
0.02	0.8437	0.41	5.44	0.9630	0.43	5.38	0.7802	0.41	5.38
0.03	0.8699	0.40	5.41	0.9706	0.41	5.40	0.7852	0.41	5.39
0.04	0.8889	0.42	5.40	0.9743	0.42	5.38	0.7843	0.41	5.39
0.05	0.9035	0.42	5.38	0.9775	0.40	5.38	0.7831	0.41	5.39
Goldhill Cover Image									
0.02	0.9132	0.41	5.49	0.9758	0.42	5.37	0.7833	0.43	5.40
0.03	0.9339	0.41	5.41	0.9778	0.41	5.38	0.8214	0.43	5.39
0.04	0.9470	0.43	5.39	0.9793	0.42	5.37	0.8385	0.41	5.39
0.05	0.9552	0.41	5.39	0.9802	0.44	5.39	0.8393	0.41	5.39

Table 7 The attack analysis of proposed algorithm (with bior6.8 wavelet) for different values of scale factor with Rotation in terms of NC values of extracted watermark and execution time

Scale Factor used for embedding	Attacks																
	Rotation (0.25°)				Rotation (-0.2°)				Rotation (0.25°)				Rotation (-0.2°)				
	NC		Execution Time (in sec.)		NC		Execution Time (in sec.)		NC		Execution Time (in sec.)		NC		Execution Time (in sec.)		
	T1	T2	T1	T2	T1	T2	T1	T2	T1	T2	T1	T2	T1	T2			
Cameraman Cover Image						Goldhill Cover Image											
0.02	0.9324	0.42	5.41	0.9622	0.40	5.39	0.9690	0.41	5.38	0.9864	0.42	5.38	0.9870	0.43	5.36		
0.03	0.9294	0.41	5.37	0.9613	0.43	5.37	0.9706	0.41	5.36	0.9870	0.43	5.36	0.9872	0.41	5.36		
0.04	0.9272	0.41	5.40	0.9606	0.42	5.38	0.9712	0.41	5.38	0.9872	0.41	5.36	0.9875	0.43	5.38		
0.05	0.9257	0.43	5.38	0.9601	0.40	5.39	0.9716	0.41	5.37	0.9875	0.43	5.38					

algorithms the standard benchmark attacks known as checkmark attacks [20] are used. These attacks are applied on the watermarked image to verify the versatility of the algorithm against various categories of noise like geometric, non-geometric and JPEG compression.

The non-geometric group of checkmark attacks applied on watermarked image and respective robustness offered by the proposed algorithm is mentioned in Tables 1 and 2.

The attack analysis of proposed algorithm against median and Gaussian filtering attacks applied on the Cameraman and Goldhill watermarked images with different scale factors is

Table 8 The attack analysis of proposed algorithm (with symlet8 wavelet) for different values of scale factor with JPEG compression, Median filtering and Gaussian noise in terms of NC values of extracted watermark and execution time

Scale Factor used for embedding	Attacks									
	Median Filter (3 × 3)			JPEG (Q= 30)				Gaussian Noise (Variance = 0.01)		
	NC		Execution Time (in sec.)	NC		Execution Time (in sec.)		NC		Execution Time (in sec.)
	T1	T2	T1	T2	T1	T2	T1	T2		
Cameraman Cover Image										
0.02	0.8698	0.40	5.28	0.9630	0.40	5.29	0.7990	0.40	5.29	
0.03	0.8983	0.40	5.28	0.9705	0.40	5.28	0.8012	0.41	5.29	
0.04	0.9207	0.40	5.28	0.9737	0.40	5.26	0.7998	0.40	5.28	
0.05	0.9385	0.40	5.27	0.9769	0.41	5.26	0.7991	0.40	5.29	
Goldhill Cover Image										
0.02	0.9480	0.40	5.27	0.9751	0.38	5.28	0.7948	0.40	5.27	
0.03	0.9621	0.42	5.27	0.9780	0.39	5.28	0.8336	0.40	5.28	
0.04	0.9693	0.42	5.27	0.9791	0.39	5.29	0.8482	0.42	5.28	
0.05	0.9742	0.40	5.26	0.9805	0.40	5.27	0.8545	0.39	5.28	

Table 9 The attack analysis of proposed algorithm (with symlet8 wavelet) for different values of scale factor with Rotation in terms of NC values of extracted watermark and execution time

Scale Factor used for embedding	Attacks											
	Rotation (0.25°)		Rotation (-0.2°)		Rotation (0.25°)		Rotation (-0.2°)					
	NC	Execution Time (in sec.)	NC	Execution Time (in sec.)	NC	Execution Time (in sec.)	NC	Execution Time (in sec.)				
	T1	T2	T1	T2	T1	T2	T1	T2				
Cameraman Cover Image				Goldhill Cover Image								
0.02	0.9321	0.40	5.28	0.9601	0.41	5.28	0.9657	0.41	5.27	0.9863	0.41	5.27
0.03	0.9291	0.40	5.27	0.9591	0.40	5.29	0.9662	0.40	5.29	0.9869	0.40	5.32
0.04	0.9271	0.39	5.28	0.9584	0.39	5.30	0.9667	0.38	5.27	0.9871	0.40	5.27
0.05	0.9260	0.40	5.26	0.9579	0.40	5.26	0.9667	0.41	5.27	0.9873	0.40	5.28

tabulated in the Table 1. The execution time analysis of the algorithm will be discussed in subsection 5.4. In case of median filtering attack, increasing the size of window from 3×3 to 7×7 , the robustness of algorithm also increases for cameraman cover image. In the influence of Gaussian filtering attack the algorithm performs well for both the types of cover images as NC values are above 0.9 for all scale factors. The robustness against sharpening, histogram equalization and average filtering attacks are mentioned in the Table 2. The NC is above 0.97 in case of sharpening attack for both the types of cover image. Unlike all other types of attacks the robustness against histogram equalization decreases as the value of scale factor increases.

The performance analysis of proposed algorithm against geometric attacks like Gaussian noise, salt & pepper noise, rotation, scaling and cropping is given in Tables 3 and 4.

Robustness of algorithm is much better against the rotation attacks with various degrees like 0.25° , -0.25° and 0.2° as the NC values are above 0.9 for both the types of cover images which is given in Table 3. The correlation is above 0.8 for each of the cover image at most of the scale factors against the Gaussian noise attack with variance 0.01. The performance against scaling, cropping and salt & pepper noise attacks is shown in Table 4. With 25 % cropping on both the watermarked images, the proposed scheme is giving NC value above 0.95. In scaling, the dimension of watermarked image is reduced to half, i.e. from 512×512 to 256×256 , the

Table 10 The PSNR value of watermarked images with different value of scale factor for Different wavelets

Scale Factor used for embedding	PSNR					
	Haar Wavelet	Bior6.8 Wavelet	Sym8 Wavelet	Haar Wavelet	Bior6.8 Wavelet	Sym8 Wavelet
Cameraman Cover Image			Goldhill Cover Image			
0.02	34.7353	35.1753	35.4439	34.1023	33.7613	33.9876
0.03	33.4671	33.7052	33.8962	32.8083	32.5136	32.6881
0.04	35.3459	32.7945	32.9276	31.9512	31.7203	31.8564
0.05	32.0512	32.1592	32.2520	31.3360	31.1541	31.2740



Fig. 7 Watermarked images (a) Low frequency image Cameraman (b) High frequency image Goldhill

algorithm offered NC value above 0.81 with Cameraman as cover image and above 0.86 for Goldhill as cover image. Salt and pepper noise with noise density 0.01 the NC value obtained is above 0.8.

JPEG compression is used in many applications like video streaming, telemedicine and live conferences. Image quality requirement for various applications is different e. g. medical imaging requires high quality of image whereas high image quality is not needed for the applications such as video streaming or live conferences which can reduce the data rate or the transmission bandwidth. The proposed watermarking technique can also work well with variations of quality level of JPEG compression indicated in terms of quality factor. In this paper, the algorithm is tested with different quality factors which are varied from 10 to 90.

The proposed algorithm performs well for both high and low values of quality factors. Table 5 shows the performance of the algorithm under JPEG compression for the span of compression values in terms of various quality factors. High values of NC are obtained under high as well as low values of quality factors with Goldhill and cameraman cover images.

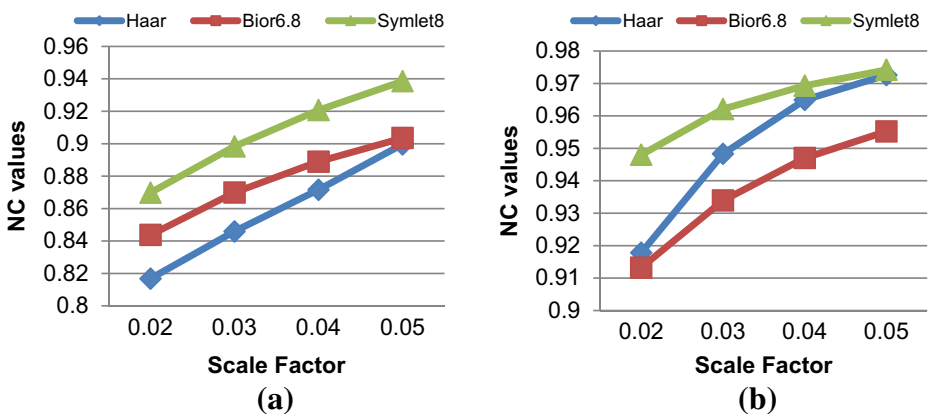


Fig. 8 Effect of non-geometric Checkmark attack: Median Filter (3×3) applied to watermarked images generated with different wavelets such as Haar, Bior6.8 and Symlet8 applied on (a) Low frequency Cameraman Cover image and (b) High frequency Goldhill Cover image

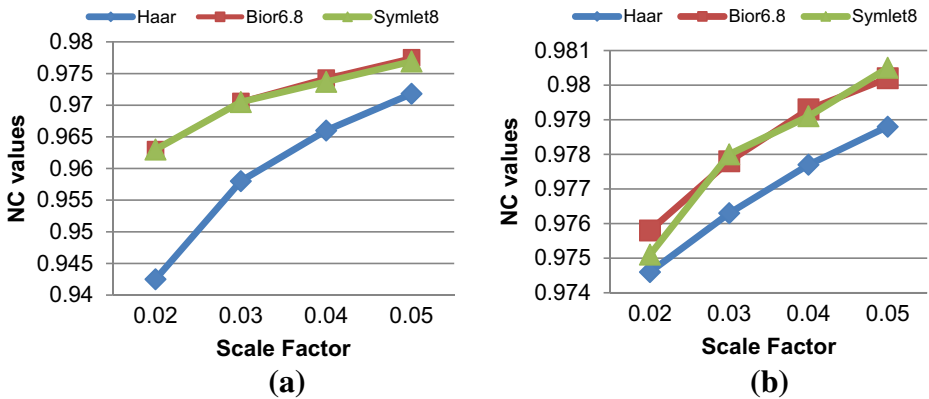


Fig. 9 Effect of JPEG compression (QF = 30) attack: applied to watermarked image generated with different wavelets such as Haar, Bior6.8 and Symlet8 applied on (a) Low frequency Cameraman Cover image and (b) High frequency Goldhill Cover image

To check the rightful ownership ability of proposed algorithm, SVD decomposition is applied on the watermark image to generate the orthogonal matrix V^T . Inverse SVD is applied on this orthogonal matrix V^T of claimed watermark and received PCs to extract the watermark image. Pepper is embedded in the cover image as the watermark image as shown in Fig. 6a which is the authentic watermark. If orthogonal matrix V^T is generated with the same embedded watermark image then inverse SVD of its combination with the received PCs generate the watermark shown in Fig. 6b. If the Baboon image shown in Fig. 6c is used to generate the orthogonal matrix V^T in place of authenticate watermark, the algorithm generates the imperceptible image as shown in Fig. 6d. The orthogonal matrix V^T is used of Saturn image in Fig 6e, then the recovered image generated by the algorithm is given in Fig 6f. When any malicious person or systems tries to extract the watermark this kind of imperceptible image will be generated by proposed algorithm which indicates that the user is unauthorized.

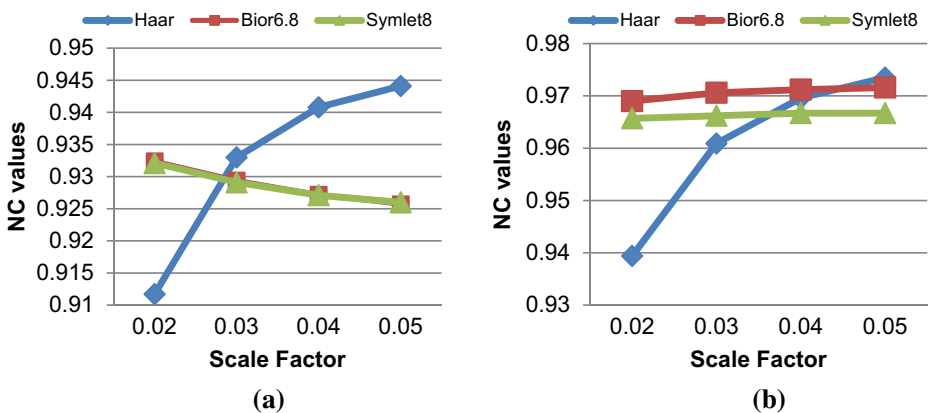


Fig. 10 Effect of geometric Checkmark Rotation (0.25°) attack: applied to watermarked image generated with different wavelets such as Haar, Bior6.8 and Symlet8 applied on (a) Low frequency Cameraman Cover image and (b) High frequency Goldhill Cover image

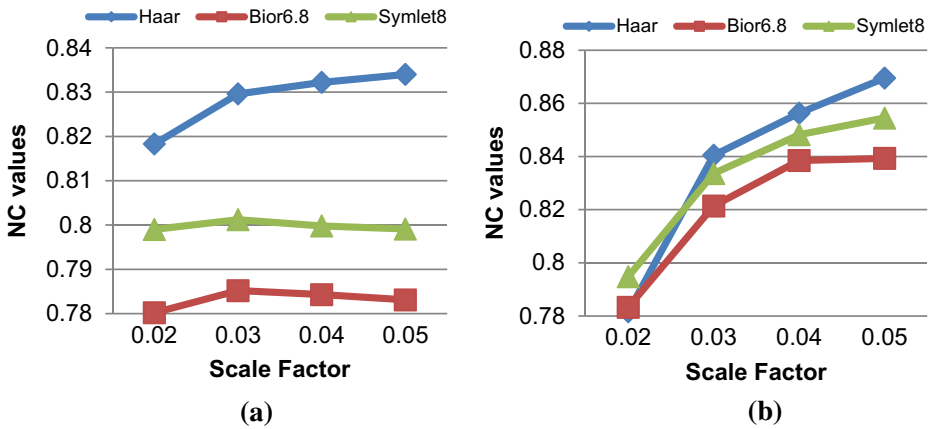


Fig 11 Effect of Checkmark Gaussian noise (variance=0.01) attack: applied to watermarked image generated with different wavelets such as Haar, Bior6.8 and Symlet8 applied on (a) Low frequency Cameraman Cover image and (b) High frequency Goldhill Cover image

5.4 Effect of wavelet families on robustness of proposed algorithm

In [5], different families of wavelet are used in watermarking algorithm where the watermark is embedded inside the HL and LH subbands of cover image. Here, the robustness of algorithm was compared with different wavelet filters like Haar, Daubechies, Bior, Symlets, coiflets, and reversible Bior for non-colored watermark images. The analysis shows that the simpler wavelet like Haar wavelet transform outperforms over any of the complicated wavelet transforms.

In this paper, the robustness analysis of the proposed algorithm is carried out with three wavelets: Haar, Bior 6.8, and Symlet8. The Haar wavelet is asymmetric, orthogonal, and biorthogonal. Robustness analysis with this wavelet is given in Tables 1, 2, 3, 4, and 5. For selected types of noise attacks, the experiment is carried out with bior6.8, which is symmetric and biorthogonal, as shown in Tables 6 and 7. The Symlet8 wavelet is near symmetric, orthogonal, and biorthogonal, for which the analysis is given in Tables 8 and 9.

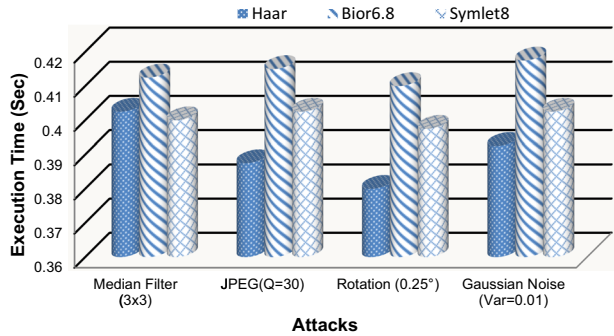
The quality of the watermarked image is verified by calculating PSNR, which is above 30 dB for both cover images. The PSNR is calculated for both types of cover images with different wavelets, as given in Table 10. The analysis shows that the value of PSNR is more than 31 dB for all scale factors. The value of PSNR is larger for the low-frequency cover image (Cameraman) as compared to the high-frequency cover image (Goldhill). The visual quality of the watermarked image is shown in Fig. 7.

To compare the performance of the proposed algorithm with different wavelet families, some attacks are chosen from the geometric, non-geometric, and JPEG compression

Table 11 Computational time comparison among proposed and existing methods

Method	Proposed Method	False positive free-SVD based method [9]	Reliable SVD based method [11]
Watermark Embedding time	0.36 s	0.39 s	1.0764 s
Watermark Extraction time	0.06 s	0.2496 s	1.3884 s

Fig. 12 Embedding and extraction time comparison of proposed algorithm for low frequency Cameraman cover image against various attacks like Median filtering (non-geometric), JPEG compression, Rotation (geometric) and Gaussian noise (removal)



group. From geometric type of attacks, the rotation and Gaussian noise are selected. The median filtering with window size 3×3 and Gaussian noise with variance 0.01 are taken from non-geometric cluster of attack. For JPEG compression the quality factor $Q = 30$ is chosen. In Figs. 8, 9, 10 and 11 the graphical analysis is presented to compare the robustness of proposed algorithm for various wavelets families. In Fig. 8, the non-geometric median filtering attack is applied to verify the performance of different wavelets in which the Symlet8 wavelet outperforms over other wavelets for both the cover images. For JPEG compression attack ($Q = 30$), both the Bior6.8 and Symlet8 wavelets perform better as compare to Haar wavelet with Cameraman and Goldhill cover images which is shown in Fig. 9a and b respectively. In the presence of rotation geometric attack (0.25°) the robustness of algorithm improves gradually with increasing the value of scale factor with Haar wavelet for both the cover images shown in Fig. 10. In Fig. 11a it is shown that the Haar wavelet performs better as compared to other complex wavelets for cameraman cover image in presence of Gaussian attack (variance = 0.01) whereas for Goldhill cover image also the Haar wavelet performs better except for the scale factor 0.02. For Goldhill cover image, the performance with Bior6.8 and Symlet8 wavelets are close to Haar wavelet as shown in Fig. 11b.

The analysis shows that, the Haar wavelet is suitable against geometric type of noise attacks whereas Sym8 and Bior6.8 perform better against the non-geometric noise and JPEG compression types of attacks for different classes of cover images.

Fig. 13 CS measurement generation and recovery comparison of proposed algorithm for low frequency Cameraman cover image against various attacks like Median filtering (non-geometric), JPEG compression, Rotation (geometric) and Gaussian noise (removal)

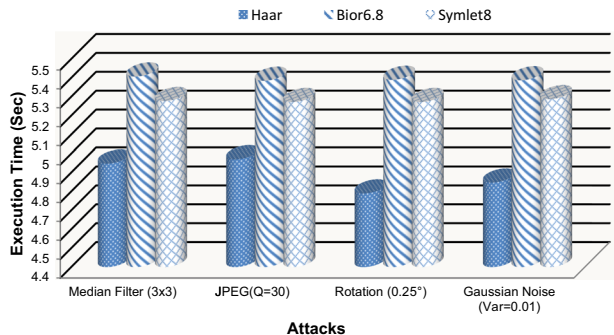
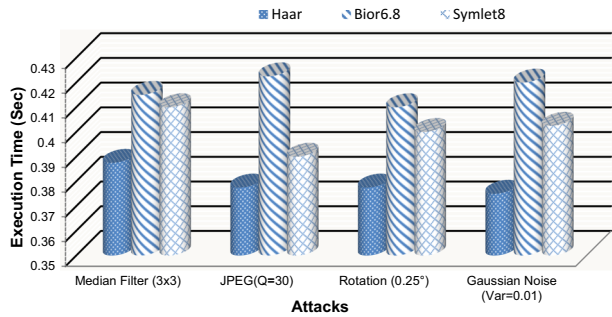


Fig. 14 Embedding and extraction time comparison of proposed algorithm for high frequency Goldhill cover image against various attacks like Median filtering (non-geometric), JPEG compression, Rotation (geometric) and Gaussian noise (removal)



5.5 Execution time analysis of proposed scheme and comparison with existing methods

The execution time is an important parameter for any watermarking algorithm, particularly when it is used as a part of application like content identification and protection of video content, forensic, piracy deterrence and content filtering. The execution time can be divided into four parts post processing time, watermark embedding time, watermark extraction time and post processing time. The extraction and embedding time have prime importance because they are the part of a continuous process. In this paper, the time analysis is divided in two parts one part contains embedding and extraction time of algorithm whereas second part contain CS measurement generation and recovery time analysis. In [9], it is noted that the embedding time is 0.39 s and extraction time is 0.2496 s which is better than the algorithm proposed in [11] where these values are 1.0764 and 1.3884 s respectively.

In Tables 1, 2, 3, 4, 5, 6, 7, 8 and 9, the column “T1” shows the embedding and extraction time, whereas column “T2” shows the CS measurement generation and recovery time of proposed algorithm. The PSNR values for different watermarked image with different scale factors are given in Table 10. In Table 11, the average value of embedding and extraction time T1 of proposed algorithm is compared with existing methods [9, 11] which demonstrate that the algorithm is computationally efficient. In [17] the time analysis of fast watermarking scheme for H.264 video standard is given, in which the embedding and extraction time are 5.578 s and 5.448 s respectively with payload around 3 K bytes. These embedding and extraction time are much larger as compared to the proposed algorithm even with higher payload of around

Fig. 15 CS measurement generation and recovery time comparison of proposed algorithm for high frequency Goldhill cover image against various attacks like Median filtering (non-geometric), JPEG compression, Rotation (geometric) and Gaussian noise (removal)

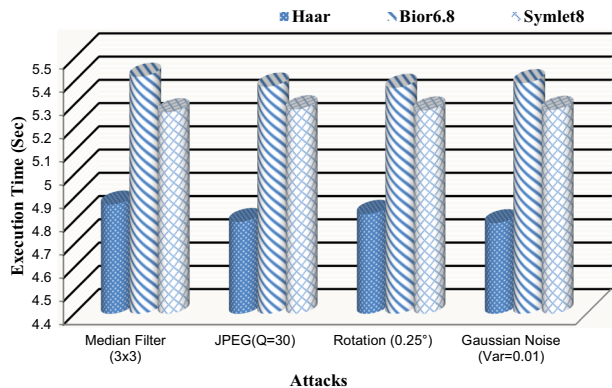


Table 12 The comparative analysis of NC values of proposed work with the existing algorithms [9, 30]














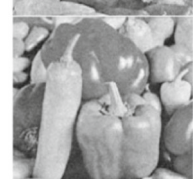
Noise Attack	Extracted Watermark Image using proposed Algorithm	Normalized Correlation		
		Proposed Algorithm	Wang et al. [30]	Guo et al. [9]
JPEG (Q=10)		0.9828	0.43	NA
JPEG (Q=30)		0.9788	0.91	NA
JPEG (Q=80)		0.9798	1	0.9886
Median Filter (3 x 3)		0.9726	0.94	0.9395
Median Filter (5 x 5)		0.9708	0.85	NA
Median Filter (7 x 7)		0.9680	0.75	NA
Gaussian Filtering (3 x 3)		0.9828	0.97	NA

Table 12 (continued)

Noise Attack	Extracted Watermark Image using proposed Algorithm	Normalized Correlation		
		Proposed Algorithm	Wang et al. [30]	Guo et al. [9]
Average Filter (3 x 3)		0.9839	0.96	0.9278
Average Filter (5 x 5)		0.9738	0.83	NA
Sharpening		0.9857	1	0.75
Histogram Equalization		0.9621	0.81	NA
Rotation (0.25°)		0.9735	0.67	NA
Scaling 512-256-512		0.9102	0.91	0.9710
Cropping (25%)		0.9844	0.74	0.4266

6 K bytes. Moreover, the decoding time is 18.817 s for algorithm in [17] whereas this time with proposed algorithm is only 4 s. So, proposed scheme can become substitute of conventional fast watermarking scheme for video standard H.264 with better security.

As the execution time of proposed algorithm varies from one wavelet to other, the time analysis for the different wavelet filters in the presence of different kind of attacks are given in Figs. 12, 13, 14 and 15.

The execution time analysis of proposed algorithm with various wavelets against rotation, median filtering, Gaussian noise and JPEG compression attacks are given in Figs. 12, 13, 14 and 15. For Cameraman cover image, comparison of embedding and extraction time T_1 and the CS measurement generation and recovery time T_2 of the proposed algorithm with different wavelet are shown in Figs. 12 and 13 respectively. The same analysis for Goldhill cover image is given in Figs. 14 and 15. For different types of noise attacks, the algorithm with Haar wavelet takes extraction and embedding time T_1 varying between 0.38 and 0.4 s whereas CS measurement generation and recovery time T_2 is varying between 4.7 and 4.9 s for both the types of cover images. These timings are minimal as compared to other wavelets.

5.6 Comparison of proposed method with existing watermarking techniques

The proposed watermarking scheme not only outperforms over the existing time efficient fast watermarking technique but also more robust than watermarking technique based on reliable SVD [9, 30]. Comparison of proposed algorithm and watermarking technique based on reliable SVD with PSO and without PSO is given in Table 12. The NC values for the algorithm against various attacks like sharpening, JPEG compression, median filtering and Gaussian filtering with different window size are also compared with existing methods.

For JPEG compression attack with quality factor $Q = 10$, Algorithm in [30] gives the NC value as 0.43 whereas the proposed algorithm gives NC value as 0.9828. For most of attacks the proposed algorithm perform better than existing methods except sharpening, scaling and JPEG compression ($Q = 80$) attacks. The best performance of various algorithms against the different attacks is shown by highlighted text in the Table 12.

6 Conclusion

In applications like video streaming, telemedicine and video conferencing, the watermarking algorithms based on optimization techniques are not suitable as their computational complexity is more due to iterative nature. Therefore in this paper, a compressive sensing and principle component based image watermarking algorithm is proposed. This algorithm is computationally efficient as well as robust against various types of noise attacks. Moreover, copyright protection provided by this watermarking algorithm is more due to three layers of security provided by the compressive sensing and principal components techniques. To verify the robustness of algorithm, the geometric, non geometric and compression types of checkmark attacks are applied with different scale factors on embedded watermark image. The algorithm is also tested with two different classes of cover images: one having majority of low frequency components and other having majority of high frequency components.

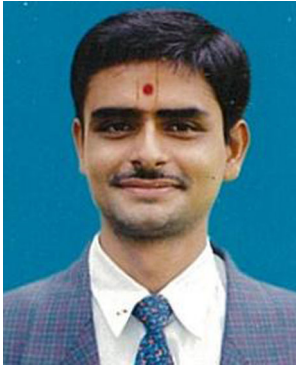
The experimental results show that the NC values are close to 0.9 against most of the attacks. It is also observed that the NC value is above 0.95 for JPEG compression with quality factor $Q = 10$.

For efficient embedding and extraction of watermark by proposed algorithm, the analysis with various types of orthogonal, non-orthogonal, symmetric and non symmetric wavelets is carried out against different noise attack. It is observed that Sym8 and Bior6.8 perform better for non-geometric and JPEG compression attacks whereas the Haar wavelet performs better for geometric type of noise attacks. The comparison of computational time is showing that embedding and extraction time of the proposed algorithm is about 0.4 s which is much less than the watermarking algorithms proposed in literature [9, 11]. The overall execution time of proposed algorithm for payload of 6 K bytes with Haar filter is around 5 s which is less as compared to existing method [17]. Therefore, the proposed algorithm can be included with video standard H.264 as watermarking algorithm. The algorithm requires lesser execution time with Haar wavelet as compared to other wavelets. Moreover, the comparative analysis shows that algorithm outperforms over the various reliable SVD based watermarking algorithms proposed in the literature [9, 30]. In proposed algorithm, the linear measurement matrix of watermark is embedded into HL subband of cover image. The performance analysis of proposed algorithm can be further investigated with different subbands at various levels of wavelet decomposition. Moreover, the DCT is used to generate sparse data set for CS in proposed algorithm; the same can be further examined using wavelet transform as sparse dataset generator for CS which may possibly improve the performance.

References

1. Agarwal H, Atrey PK, Raman B (2015) Image watermarking in real oriented wavelet transform domain. *Multimed Tools Appl* 74:10883–10921
2. Ali M, Ahn C (2014) An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain. *Signal Process*. doi:10.1016/j.sigpro.2013.07.024
3. Baraniuk R (2007) Compressive sensing. In: *IEEE Signal Processing Magazine Lecture Notes*, vol. 24
4. Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel-wise masking. *IEEE Trans Image Process* 10(5):783–791
5. Brannock E, Weeks M, Harrison R (2009) The effect of wavelet families on watermarking. *J Comput* 4(6):554–566
6. Fan T, Lu G, Dou C, Wang D (2013) A digital image watermarking method based on the theory of compressed sensing. *Int J Autom Control Eng* 2(2):56–61
7. Ganic E, Eskicioglu A (2004) Robust DWT-SVD based watermarking: embedding data in all frequencies. In: *ACM 1-58113-854-7/04/0009*, pp 166–174
8. Goyal S, Gupta R, Bansal A (2009) Application of genetic algorithm to optimize robustness and fidelity of watermarked images (a conceptual approach). *Int J Comput Sci Eng* 1(3):239–242
9. Guo J, Prasetyo H (2014) False-positive-free SVD-based image watermarking. *J Vis Commun Image Represent*. doi:10.1016/j.jvcir.2014.03.012
10. Hammouri AI, Alrifai B, Al-Hiary H (2013) An intelligent watermarking approach based particle swarm optimization in discrete wavelet domain. *Int J Comput Sci Issues* 10(2):330–338
11. Jain C, Arora S, Panigrahi P (2008) A reliable SVD based watermarking scheme. arXiv:0808.0309v1 [cs.MM]
12. fLai C, Chan C, Ouyang C, Chiang H (2013) A robust feature-based image watermarking scheme. In: *IEEE Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, pp 581–585
13. Lai C, Tsai C, Lai C, Tsai C (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Trans Instrum Meas* 59(11):3060–3063
14. Liu R, Tan T (2002) An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans Multimed* 4(1):121–128

15. Liu X, Yu J, Yue Y, Wei Y (2014) Double encrypted digital image watermarking algorithm based on compressed sensing. *J Comput Inf Syst* 10(12):5113–5120
16. Lui CS, Sun SW, Chang PC (2005) Robust hash-based image watermarking with resistance to geometric distortions and watermark-estimation attack. In: *Proceedings of SPIE-IS & T Electronic Image SPIE 5681*, pp 147–163
17. Nguyen C, Tay D, Deng G (2006) A fast watermarking system for H.264/AVC video. In: *Asia Specific IEEE Conference on Circuits and Systems*, pp 81–84
18. Orovik I, Stankovic S (2013) Combined compressive sampling and image watermarking. In: *IEEE Symposium, ELMAR*, pp 41–44
19. Pandey P, Kumar S, Singh S (2014) Rightful ownership through image adaptive DWT-SVD watermarking algorithm and perceptual tweaking. *Multimed Tools Appl*. doi:10.1007/s11042-013-1375-2
20. Pereira S, Voloshynovskiy S, Madueno M, Maillat S, Pun T (2001) Second generation benchmarking and application oriented evaluation. In: *Information Hiding Workshop, Lecture Notes in Computer Science*, 2137, pp 340–353
21. Run R, Horng S, Lai J, Kao T, Chen R (2012) An improved SVD-based watermarking technique for copyright protection. *Expert Syst Appl*. doi:10.1016/j.eswa.2011.07.059
22. Rykaczewski R (2007) Comments on “an SVD-based watermarking scheme for protecting rightful ownership”. *IEEE Trans Multimed* 9(2):421–423
23. Song C, Sudirman S, Merabti M (2012) A robust region-adaptive dual image watermarking technique. *J Vis Commun Image Represent*. doi:10.1016/j.jvcir.2012.01.017
24. Surekha P, Sumathi S (2012) Performance comparison of optimization techniques on robust digital-image watermarking, against attacks. *Appl Artif Intell* 26:615–644
25. Thanki R, Borisagar K (2013) A novel robust digital watermarking technique using compressive sensing for biometric data protection. *Int J Electron Commun Comput Eng* 4(4):1133–1139
26. Tropp J, Gilbert A (2007) Signal recovery from random measurements via orthogonal matching pursuit. *IEEE Trans Inf Theory* 53(12):4655–4666
27. Valenzise G, Tagliasacchi M, Tubaro S (2009) A compressive-sensing based watermarking scheme for sparse image tampering identification. In: *IEEE Conference on Image Processing*, pp 1265–1268
28. Veena V, Jyothish Lal G, Vishnu S, Sachin S, Soman K (2012) A robust watermarking method based on compressed sensing and Arnold scrambling. In: *IEEE Conference on Machine Vision and Image processing*, pp 105–108
29. Venkateswara Rao VS, Shekhavart R, Srivastava VK (2012) A reliable digital image watermarking scheme based on SVD and particle swarm optimization. In: *IEEE Student Conference on Engineering and Systems*, pp 1–6
30. Wang Y, Lin W, Yang L (2011) An intelligent watermarking method based on particle swarm optimization. *Expert Syst Appl*. doi:10.1016/j.eswa.2010.12.129
31. Wang Z, Sun X, Zhang D (2007) Novel watermarking scheme based on PSO algorithm. In: Li K (ed) *LSMS 2007, LNCS 4688*. Springer-Verlag Berlin, Heidelberg, pp 307–314
32. Wright J, Yang AY, Ganesh A, Sastry SS, Ma Y (2009) Robust face recognition via sparse representation. *IEEE Trans Pattern Anal* 31(2):210–227
33. Wu J, Wang W, Liang Q, Wu X, Zhang B (2013) Compressive sensing-based data encryption system with application to sense-through-wall UWB noise radar. *Secur Commun Netw* 9:371–379
34. Xiong C, Ward R, Xu J (2008) On the security of singular value based watermarking. In: *Proceeding of IEEE Conference on Image Processing*, pp 437–440
35. Yamac M, Dikici C, Sankur B (2013) Robust watermarking of compressive sensed measurements under impulsive and Gaussian attacks. In: *IEEE Proceeding of 21st European Conference on Signal processing*, pp 1–5
36. Yang Z, Yan W, Xiang Y (2015) On the security of compressed sensing-based signal cryptosystem. *IEEE Trans Emerg Topics Comput* 3(3):363–371
37. Zang X, Li K (2005) Comments on “an SVD-based watermarking scheme for protecting rightful ownership”. *IEEE Trans Multimed* 7(2):593–594
38. Zang Q, Sun Y, Yan Y, Liu H, Shang Q (2013) Research on algorithm of image reversible watermarking based on compressed sensing. *J Inf Comput Sci* 10(3):701–709
39. Zhang M, Zhang Q, Zhou C et al (2011) Robust digital image watermarking in DWT-SVD domain. In: Deng H (ed) *AICI 2011, part II, LNAI 7003*. Springer-Verlag Berlin, Heidelberg, pp 75–84



Falgun N. Thakkar received his M. Tech. in Communication Engineering from G H Patel College of Engineering and Technology, V V Nagar-Anand, Gujarat - India, in 2010 and Pursuing Ph.D. in Electronics and Communication Engineering Department from Motilal Nehru National Institute of Technology, Allahabad. He is Associate Professor in the Department of Electronics and Communication Engineering, G H Patel College of Engineering and Technology, V V Nagar - Anand, Gujarat - India and deputed for Ph.D. under QIP at Motilal Nehru National Institute of Technology. He has authored or co-authored about twelve publications. His main research interest is in Image processing with special focus on Watermarking, Data hiding and image compression.



V. K. Srivastava received his B.E. in Electronics & Telecommunication from GEC Rewa, MP- India, in 1989, M. Tech. in Communication from IIT-BHU, Varanasi - India, in 1991 and Ph.D. in Electrical Engineering from I.I.T. Kanpur- India, in 2001. Presently, he is a Professor in the Department of ECE, MNNIT, Allahabad - India. He has about 25 years of teaching and research experience in the area of signal and image processing. He has chaired many sessions in conferences. He has authored or co-authored about 45 publications. His current research interest includes image compression, post-processing, digital watermarking, image denoising, DSP methods for the identification of protein coding regions, design and analysis of IDMA systems.