Journal of Computer Science

Original Research Paper

Compressive Sensing Theory for Improving the Robustness and the Security of the Discrete Wavelet Transform-Singular Value Decomposition Watermarking Scheme

Rasha Shoitan and Sawsan Morkos Gharghory

Department of Computers and Systems, Electronics Research Institute, Cairo, Egypt

Article history
Received: 12-02-2021
Revised: 06-04-2021
Accepted: 20-04-2021

Corresponding Author:
Sawsan Morkos Gharghory
Department of Computers and Systems, Electronics Research Institute, Cairo, Egypt
Email: Sawsan@eri.sci.eg

Abstract: Digital watermarking has been suggested as a solution to protect copyright and ownership of digital images. The effective watermarking scheme should satisfy imperceptibility, robustness, capacity and security requirements. In this research, the security issue and the lack of reconstruction quality of the watermark logo of the integration of Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and Compressive Sensing (CS) watermark technique are addressed. Wilkinson measurement matrix is proposed to increase the robustness and improve the reconstruction quality of the watermark logo in the DWT and SVD based on the CS watermarking scheme. Additionally, the security issue of the SVD is solved by sending a scrambled compressed logo then extracting U, V matrices from this compressed logo at the decoder. The proposed method not only increases security but also reduces the size of the transmitted watermark logo. The robustness of the proposed algorithm is evaluated in the presence of different attacks like signal processing, compression, geometrical and noise attacks. The simulation results demonstrate that the proposed technique is more robust than the conventional techniques for all attacks, as well as its robust security. Moreover, the quality of the watermarked image is measured and the results show that the imaging performance of the proposed technique is approximately 0.7 to 4 dB better than that of the conventional methods. Consequently, the proposed watermarking scheme proves its ability to achieve the demands of security, imperceptibility and robustness against different attacks.

Keywords: Compressive Sensing, Robustness, Security, Watermark, Wilkinson Matrix

Introduction

Although the internet is considered a beneficial communication tool that recently can make people's lives much more manageable, it also has terrible effects. One of these harmful effects is that the owner's right is threatened by the circulation of illegal and unauthorized digital content. Every day vast amounts of digital information are exposed to different types of attacks via the internet as data theft, spying, data corruption and denial of service attacks. This leads to the risk of violating owner copyright and hampering digital content's authenticity; therefore, the owners of digital content need to provide a form of proof for their owners to preserve their ownership rights. Many researchers introduced various techniques to protect ownership rights by embedding some extra information called watermark into digital content (Potdar *et al*., 2005) and extracting it later for copyright protection and integrity authentication. Strong security of copyright content with sufficient robustness against different attacks is required to design an excellent watermarking scheme. Watermarking schemes are divided according to working domains into spatial or transform domain techniques.

Spatial domain watermarking techniques slightly modify the images' pixels by simple addition or replacement of bits in the selected region according to the watermark. However, these techniques have less robustness against various attacks. Alternatively, the transform domain techniques are proposed in different literature to overcome these spatial domain technique limitations. In transform domain techniques, the

watermark embedding method is applied to the coefficients of the transform domain such as Discrete Cosine Transform (DCT) (Xu *et al*., 2011), Discrete Wavelet Transform (DWT) (Li *et al*., 2008) and Singular Value Decomposition (SVD) (Bahadur and Chandra, 1959; Liu and Tan, 2002; Chang *et al*., 2005) of the image. The advantages of these techniques compared to spatial domain techniques are that they provide more robustness against many types of attacks, especially the SVD technique. SVD is characterized by its good noise immunity of the singular values of an image against any disturbance. Therefore, various research combine between SVD and different transform domain techniques to strengthen the watermarking scheme versus different attacks (Jane and Elbaşi, 2014; Hu and Hsu, 2015; Fazli and Moeini, 2016; Singh and Singh, 2017; Thakkar and Srivastava, 2017; Zhou *et al*., 2018). Although the SVD technique is usually used because of its robustness and stability to various attacks, it has a security issue called the False Positive Problem (FPP) (Makbol *et al*., 2018). It was discovered that the orthogonal matrices U and V keep the geometric properties of an image as they illustrate the Eigenvectors of the corresponding singular values. Therefore, when inverse SVD is applied and any different singular matrix is used with U and V, a correlated output is generated instead of the actual output. This issue is considered a security threat because an attacker may replace his/her own U, V set with the original one during watermark extraction and claims false ownership. This problem is solved in (Gupta and Raval, 2012) by adding a signature based on U and V matrix in the LL band. At the receiver, the extracted signature is compared to the generated signature from the sent U and V to prove the ownership. This solution improves the security problem of the SVD but degrades the quality of the watermarked image.

Compressive Sensing (CS) theory is presented as an alternative way of signal sampling that differs from the standard Shannon-Nyquist theorem in the last ten decades. The compressed sensing paradigm integrates the sensing and compression processes for the sparse signals in a straightforward linear measurement step. Compressive sensing gets randomly projected measurements that containing the content features of the image. The image is reconstructed from the compressed measurements based on the sensing measurement matrix's knowledge (Candès, 2006; Candès and Wakin, 2008). The scrambling sensing method of CS draws the researchers' attention in the security research area. Thus, CS is used in the watermarking schemes to improve the security of the conventional watermarking technique and provide copyright protection.

Different researches have integrated the CS theory and the watermarking scheme in various methods. One of these methods is to apply the CS to the host image by embedding the watermark logo into the host image's measurements (Huang and Chang, 2014; Chi and Feng, 2014). However, this method's disadvantage is that any alteration in the host image can lead to a modification in the measurements. Thus, embedding the watermark directly into the measurements is not robust to frequent attacks. The other method is to apply the CS technique on the watermark logo to represent it by a small number of measurements. Then these measurements are embedded directly into the host image. This method aims to enhance the security of the watermark and provide more payload capacity.

Various researches integrate between the CS, SVD and DWT to get the merits of all of them and overcome the security issue of SVD (Chen *et al*., 2013; Wang *et al*., 2017). However, it was discovered in other researches that this integration suffers from some degradation in the quality of the watermark logo and the watermarked image due to the use of the random measurement matrices in CS theory. These conventional random matrices usually don't provide good reconstruction quality and need high computational times.

In this proposed paper, the integration between CS, DWT and SVD watermarking scheme is addressed to overcome its previously mentioned problem. First, the watermark images are compressed sensing using the Wilkinson matrix instead of the conventional random matrices to improve the reconstructed watermark logo's quality. Then, the compressed sensing watermark logo's singular values are embedded in the HH band of the DWT of the host image. The FPP problem of SVD is solved by sending a compressed watermark as a secret key to the receiver. Therefore, if the attacker replaces his watermark with the original compressed watermark, the compressive sensing reconstruction process is applied to his watermark and a distorted image is produced. Therefore, the CS technique improves the quality of the watermark logo, overcomes the FPP security issue of SVD and reduces the size of the sent watermark logo.

The rest of this paper is prearranged as follows: Section 2 briefly illustrates the CS theory, measurement matrix, OMP and Singular value decomposition method. In section 3, the embedding and the extracting watermark schemes are explained. The evaluation metrics used to evaluate the watermarked and watermark images are introduced in section 4. In section 5, the simulation results are presented and discussed. Finally, section 6 concludes the idea and the results of this study.

Background

Compressive Sensing Theory

Shannon-Nyquist theorem is the most important theorem that sets a limit to the sampling rate, guaranteeing recovery of the signal. This theorem states that the sampling rate of the signal should be at least twice of its bandwidth. Unfortunately, in many important and emerging applications, the resulting Nyquist rate is so high that we end up with far too many samples. CS theory overcomes this Nyquist theorem problem. CS

theory states that if the signal has a sparse representation in a spatial or in another domain; it can be recovered exactly from a far fewer linear, non-adaptive measurements (Candès, 2006; Romberg, 2008). In compressed sensing, the signal to be sampled is generally represented as a vector, say $x \in R^N$ that has at most k ($k << N$) nonzero components. The compressed signal y with the length of M ($M<N$) is gotten through the linear transformation, $y = \Phi x$ where $\Phi \in R^{M \times N}$ (Candès and Wakin, 2008). The compressive sensing goal is to acquire the signal x with no or insignificant loss of information using fewer than N measurements to accurately reconstruct x from y with $M<N$. Therefore, the design of the measurement matrix is an important issue in compressive sensing since data recovery depends on how well the limited measurements provide information about the structure of the signal. To guarantee that the measurement matrix gets the largest amount of information from the signal, it should satisfy certain property which is the mutual coherence property. The less coherent the columns of Φ are, the better the reconstruction works because any two closely related columns will carry the same information about the signal and therefore, they may mislead any reconstruction technique. Therefore in compressive sensing, the measurement matrix should have very low coherence. Many researches introduce measurement matrices that possess these properties one of these matrices is the Random Gaussian matrix. These random matrices have the useful property of being almost maximally incoherent with almost all sparsifying bases. Thus, they are a universal choice for measurement (Candès *et al*., 2006; Qaisar *et al*., 2013). However, these random matrices suffer from very high computational complexity and large storage capacity due to their inherent random structure. Also, these matrices reduce the quality of the reconstructed image from CS.

Reconstructing the original signal x from the compressed signal requires solving an under-determined set of linear equation $y = \Phi x$ where the number of unknowns (N) is much larger than the number of measurements (M). Thus, the estimation of x is considered an ill-posed problem.

A wide variety of approaches exist to recover the sparse signal from a small number of linear measurements. The two major CS recovering approaches are L1-minimization and greedy algorithms Because the greedy algorithms are faster and simpler to implement compared to the L1 (Needell *et al*., 2008), one of the greedy algorithm which is the Orthogonal Matching Pursuit (OMP) will be used in this study for signal reconstruction (Tropp and Gilbert, 2007).

The Orthogonal Matching Pursuit (OMP) main idea is to select columns of the measurement matrix that contribute to greedily generating measurements y. The measurement matrix Φ and the measured vector y is used as inputs for the OMP and an estimate x' of the original signal x is provided as an output. The OMP constructs an approximation by going through an iteration process. During each iteration, one column of Φ is chosen, which is most strongly correlated with the residual vector r. then, the contribution of this column is removed to compute a new residual. The initial condition of the residual vector is chosen equal to the vector that is required to be approximated i.e., $r = y$. The OMP algorithm can be described as follows (Meenakshi, 2015):

Input:

- Signal y and a matrix Φ.
- Stopping criterion, e.g., until a level of accuracy is reached

Output:

- Approximation vector x

Procedure:

1) Start by setting the residual $r_0 = y$, the time $t = 0$ and index set $V_0 = \{\phi\}$
2) Identify the index of the column of the largest correlation $v_t = \arg\max\left|\left\langle r_{t-1}, \Lambda_k \right\rangle\right|$ where Λ_k are the column vectors of Φ
3) Update the augmented matrix V_t with v_t: $V_t = V_{t-1} \cup \{v_t\}$ and the matrix of chosen columns $\Phi'_t = \left[\Phi'_{t-1}\ \Lambda_{v_t}\right]$
4) Compute the least square problem in order to obtain the new estimate of the sparse signal: $x'_t = argmin_x \left\|\Phi'_t x - y\right\|$
5) Update the new residual $r_t = y - \Phi'_t x'_t$
6) Set $t \leftarrow t + 1$
7) Return to step 2 if $t<m$

At the end of the iterations, the non-zero elements of x_t will be at the locations corresponding to the respective columns of the dictionary matrix Φ at the index set V_t and the rest elements will be zeros, making it a sparse vector of size $N \times 1$ (Rabah *et al*., 2014). The OMP will require more iterations to reach the halting criteria if the measurement matrix and the sparsity transform are not incoherent together or the measurement matrix is a dense matrix. This will produce less representative measurement vector y and lead the OMP to select the inappropriate columns during the reconstruction process, resulting in a lack of reconstruction quality.

Singular Value Decomposition

SVD is a linear algebra scheme, which is used to decompose a matrix into three matrices. For a $M \times N$ matrix A, its SVD representation is defined as:

$$A = USV^T \tag{1}$$

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

Where, '*S*' is a diagonal matrix with dimension $M \times N$, the diagonal entries of *S* are known as singular values. These Singular values are organized in a decreasing order automatically as a result of decomposition. These entries are considered as a set of luminance values if *A* is an image. *U*, *V* are orthogonal matrices with dimension $M \times M$ and $N \times N$ respectively. If *A* is an image, the matrix *U* represents the horizontal and *V* represents the vertical detail of this image (Thakkar and Srivastava, 2017). Rotation invariant and translation invariant are the properties of SVD, which make it Robust to many kinds of image processing attacks. Also, SVD is characterized by the immunity of its singular values to noise. A little variation in singular values when a small perturbation is added to an image intensity values does not affect the visual quality of this image. These properties of SVD make it the right candidate for the watermarking application (Rani *et al*., 2015).

The Proposed Watermarking Scheme

In this study, the watermarking scheme based on CS, DWT and SVD techniques is addressed to overcome its previous scheme drawbacks and improve its security and robustness features. First, the proposed scheme provides the system with three different security keys in various stages to guarantee that the scheme is very secure. Second, the security issue of the SVD technique is solved by sending the compressed sensing logo and extracting the *U* and *V* matrices at the decoding side to guarantee that an attacker cannot replace the *U*, *V* of the original watermark logo with his watermark. Moreover, even if the watermark is replaced by the attacker's watermark, the compressive sensing reconstruction process is applied to it and produces a distorted image. Third, the proposed scheme improves the quality of the reconstructed watermark logo and watermarked images by replacing the conventional random matrices in the CS scheme with the Wilkinson matrix.

The Wilkinson matrix, the proposed watermark embedding and the extraction scheme will be explained in detail in the next subsection.

Wilkinson Matrix

The Wilkinson matrix is asymmetric tri-diagonal matrix with 1's on the off-diagonals its structure shown in Fig. 1.

The advantage of this matrix is when re-orthognalize only *M* rows from its rows, different columns with zero value are generated at the end of the matrix as shown in Fig. 2 (Shoitan *et al*., 2018a). This advantage is useful if the DCT is the sparsity transform. The low-frequency components of an image in the DCT domain, which is considered the significant DCT elements, are found on the top left.

Therefore, the compressed vector *y* is a linear multiplication of the most vital coefficients of the DCT and the columns of non-zero values in the Wilkinson matrix, while the columns with zero value are multiplied by the DCT coefficients which contain less information. Thus, the compressed vector *y* is constructed from the most significant information in an image. At the receiver, OMP search for the columns in Φ (Wilkinson matrix), which strongly correlated with the measured vector *y*, then removes its contribution from *y*.

$\frac{n-1}{2}$	1	0	0	0	0	0	0	0
1	$\frac{n-2}{2}$	1	0	0	0	0	0	0
0	1	$\frac{n-3}{2}$	1	0	0	0	0	0
0	0	⋱	⋱	⋱	⋱	⋱	⋱	0
⋮	⋱	⋱	⋱	⋱	⋱	⋱	⋱	⋮
0	0	0	⋱	⋱	⋱	⋱	⋱	0
0	0	0	0	0	1	$\frac{n-3}{2}$	1	0
0	0	0	0	0	0	1	$\frac{n-2}{2}$	1
0	0	0	0	0	0	0	1	$\frac{n-1}{2}$

Fig. 1: Wilkinson matrix structure

3.5	1	0	0	0	0	0	0
1	2.5	1	0	0	0	0	0
0	1	1.5	1	0	0	0	0
0	0	1	0.5	1	0	0	0
0	0	0	1	0.5	1	0	0
0	0	0	0	1	1.5	1	0
0	0	0	0	0	1	2.5	1
0	0	0	0	0	0	1	3.5

(a)

-0.78	0.58	-0.21	-0.05	0	0	0	0
-0.57	0.53	0.57	0.25	0	0	0	0
-0.23	0.54	-0.44	-0.68	0	0	0	0

(b)

Fig. 2: (a) 8×8 Wilkinson matrix (b) the re-orthgnlization of 3 rows from Wilkinson matrix in (a)

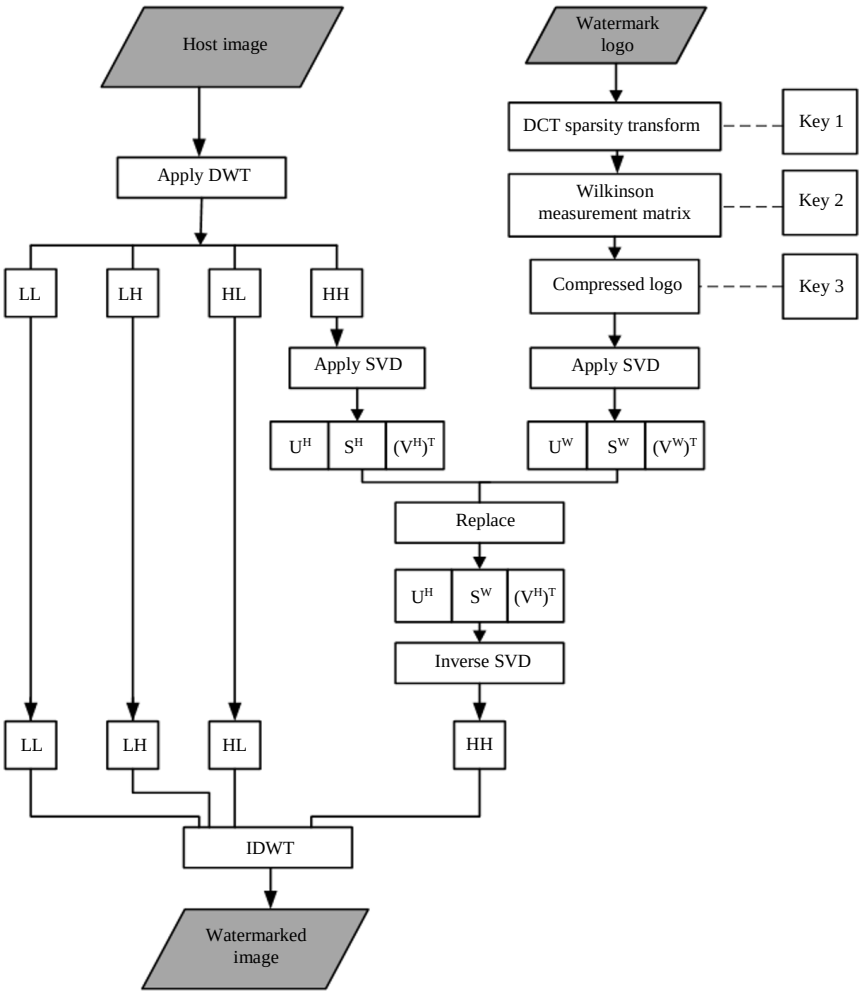

Fig. 3: The proposed embedding watermarking technique

Then, search for the second highly correlated column from the residual and repeat this step until the DCT elements of *x* are recreated according to the OMP algorithm's steps. Thus, when the OMP search for the Wilkinson matrix columns most correlated with *y*, it will find all the columns with non-zero coefficients. However, if the vector y is constructed from a linear multiplication of most of the columns of the Gaussian measurement matrix Φ and most of the DCT coefficients, this misdirects the OMP to find the proper columns from the Gaussian matrix (Shoitan *et al*., 2018b).

The Proposed Watermark Embedding Scheme

Figure 3 presents the structure of the proposed watermark embedding scheme. At the transmitter, the watermark is embedded using two main processes. The first process is applying CS to the sparse watermark logo in the DCT domain. Then the Wilkinson measurement matrix is applied to the produced sparse watermark logo and then these measurements are sent by the owner as keys. The second process is applying DWT to the host image. Because the HH band contains the finer details and contributes insignificantly to the image energy, it is selected to replace their singular values with the compressed watermark's singular values. The watermark logo cannot be reconstructed at the receiver without inversing the produced sparse coefficients using IDCT. Thus the measurement matrix and the sparsity transform are considered as secret keys at the receiver to restore the Watermark logo from the host image. The algorithm steps for watermark embedding are given below:

1. Apply the discrete wavelet transform on the host image using the Haar Wavelet basis function. Four subbands are obtained which are LL, LH, HL and HH
2. Apply the singular value decomposition method on the HH subband
3. Get the sparse watermark logo by applying DCT on the watermark logo:

$$x_W = DCT\left(watermark\log o\right) \tag{2}$$

4. Apply the Wilkinson measurement matrix on the sparse watermark logo to get the CS measurements (compressed logo):

$$y_W = \Phi x_W \tag{3}$$

5. Apply the singular value decomposition method on the compressed logo:

$$U_W S_W V_W = SVD\left(y_W\right) \tag{4}$$

6. Substitute the singular values of the HH band with the singular values of the compressed watermark logo
7. Apply inverse SVD to obtain the modified HH band:

$$HH' = U_{HH} * S_w * V_{HH}^T \tag{5}$$

8. Apply inverse the discrete wavelet transform IDWT on LL, LH, HL, HH' subbands to get the watermarked image

The Proposed Watermark Extraction Scheme

Figure 4 shows the block diagram for the proposed extraction procedure. In the proposed watermark extraction scheme, the Wilkinson measurement matrix, the compressed logo and the DCT sparsity transform are considered secret keys that should be given as an input for the extraction algorithm to extract the watermark logo the watermarked image. So if someone wants to extract the watermark, all the keys must be obtained, which increases the proposed system's security. The algorithms steps of the proposed watermark extraction process are given below:

1. Apply the DWT on the watermarked image to decompose it into 4 sub-bands: LL, HL, LH and HH using Haar Wavelet basis function
2. Apply the singular value method on the HH:

$$U_{HH'} S_{HH'} V_{HH'} = SVD\left(HH'\right) \tag{6}$$

3. Apply the singular value method on the compressed logo:

$$U_W S_W V_W = SVD\left(y_W\right) \tag{7}$$

4. Substitute the singular values of the HH band with the singular values of the compressed watermark logo
5. Apply inverse SVD to obtain the modified compressed sensing logo:

$$y'_W = U_W * S_{HH'} * V_W^T \tag{8}$$

6. Use the OMP method to restore all the DCT coefficients of the watermark logo from its CS measurements y'_W
7. Reconstruct the watermark logo by applying Inverse Discrete Cosine Transform (IDCT) on the restored low-frequency and high-frequency coefficients

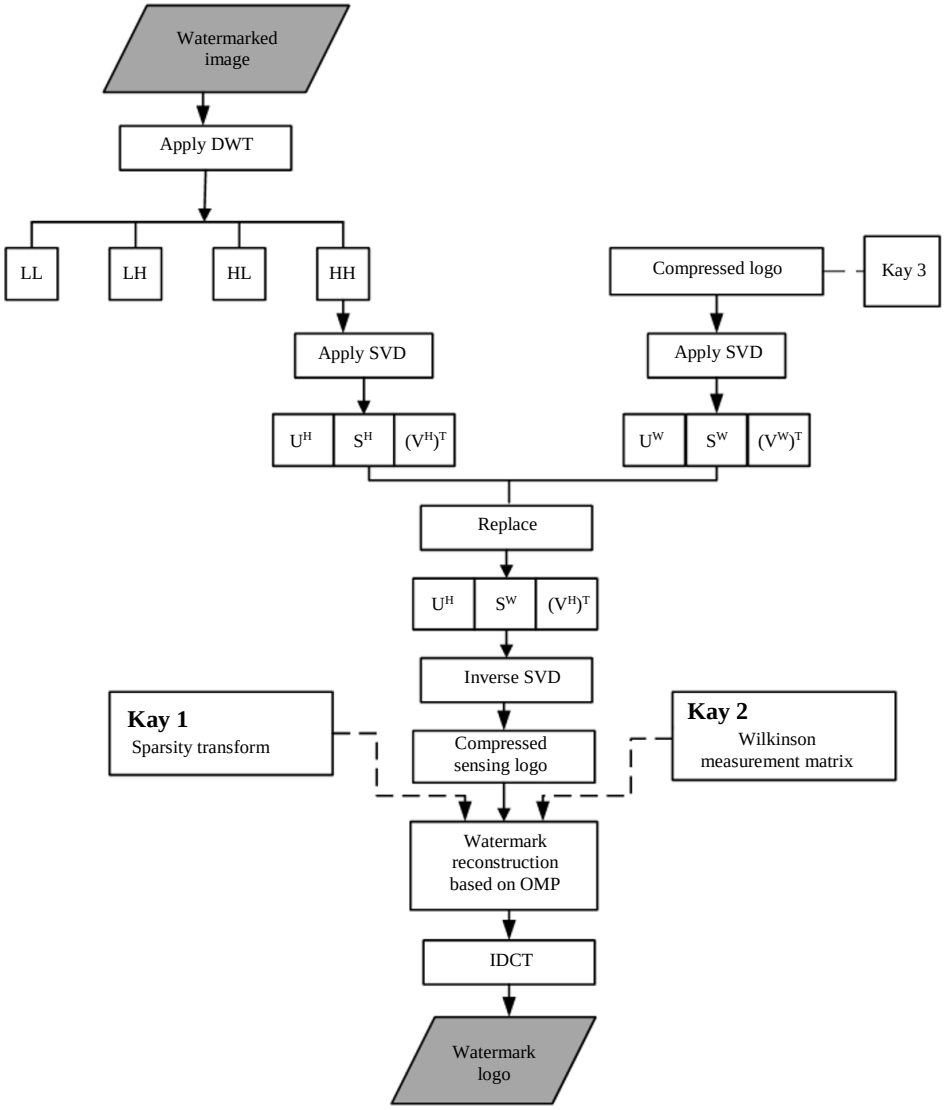

Fig. 4: The proposed extracting watermarking scheme

Evaluation Metrics

In this study, the perceptual quality and the robustness of the proposed watermarking scheme are evaluated using the following parameter.

Peak Signal to Noise Ratio (PSNR)

PSNR metric is used to validate the perceptual similarity between host image and watermarked image. The PSNR represents the ratio between the maximum power of the image and the power of distorting noise that affects the quality of its representation. While the maximum power is expressed as MAX^2 and MAX is the maximum pixel intensity. All images here are expressed using 8-bit intensity values per pixel; thus, the maximum pixel power MAX^2 is 255^2. The mathematical representation of PSNR is given as follows:

$$PSNR = 10\log_{10}\left(MAX^2 / MSE\right) \quad (9)$$

The PSNR approach infinity as MSE approaches zero; this shows that a higher PSNR value provides a high-quality image (Mrak, 2004).

Correlation Coefficient (CC)

The correlation coefficient metric is used to measure the robustness of the proposed watermark scheme against various attacks. The correlation coefficient measures the closeness or similarity between the original and the extracted watermark logo. The CC values vary between -1 to +1. The two images are very similar when the CC closes to +1.

However, CC value close to -1 indicates that the two images are highly dissimilar. The formula to compute

the correlation between the original watermark logo and the extracted watermark logo, both of size $N \times M$ pixels is given by:

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(A_{i,j}-\bar{A}\right)\left(B_{i,j}-\bar{B}\right)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(A_{i,j}-\bar{A}\right)^2\sum_{i=1}^{M}\sum_{j=1}^{N}\left(B_{i,j}-\bar{B}\right)^2}} \quad (10)$$

Where, $\bar{A}$, $\bar{B}$ are the means of the original watermark logo and the extracted watermark logo respectively, both of $A_{i,j}$, $B_{i,j}$ are the pixel values at position (i, j) of the original watermark logo and the extracted watermark logo, respectively.

Experimental Results

In this section, the proposed watermarking scheme's performance is numerically evaluated and compared to the Conventional DWT+SVD and the DWT+SVD using the signature technique (Gupta and Raval, 2012). Furthermore, the impact of the Wilkinson matrix on the performance of the proposed method is compared to the impact of the Gaussian matrix by comparing the proposed algorithm to DWT+SVD+CS based on Gaussian matrix algorithm.

In this experiment, the measurement rate in the proposed method and the CS+SVD+DWT based on Gaussian matrix is adopted at M/N = 0.5. The proposed method's block size is empirically chosen as 64×64, as mentioned (Shoitan *et al*., 2018b). The sparsity transform in the CS+DWT+SVD based on the Gaussian matrix is the DCT and OMP is the reconstruction algorithm.

Two different sets of host images are employed for performance evaluation. These test images are the Barbara and the Lena images of 512×512 pixels shown in Fig. 5. Lena is a smooth image in which most of its content is low-frequency components, while Barbara is a detailed image in which most of its content are high-frequency components. Copyrights logo of size 512×512 pixels is used as a watermark logo.

The performance of the proposed and the conventional watermarking techniques are evaluated by applying various standard watermarking attacks. Geometric attacks such as shear, rotation and cropping; Signal processing attacks as mean filter, median filter and Gaussian low pass filter. Noise attacks such as Gaussian noise, Salt and Pepper noise, JPEG compression and histogram equalization attacks. PSNR measures watermarked image quality while CC measures the reconstructed watermark logo quality. To evaluate the perceptual quality of the proposed technique's watermarked image relative to the other techniques, the PSNR is calculated and presented in Table 1.

From the results given in this table, it can be realized that the quality of the watermarked Lena image increased by approximately 4d B using the proposed technique over the conventional DWT+SVD with signature technique. This result reflects that the signature used to solve the security issue of SVD in the conventional DWT+SVD degrades the quality of the watermarked image.

The proposed technique enhances the quality of Lena images over the rest of the conventional methods by approximately 0.1 to 0.5 dB. For Barbara image, the proposed technique is slightly better than the conventional techniques by approximately 0.04 to 0.7 dB.

Table 1: The quality assessment of the watermarked image in terms of PSNR

	PSNR /dB	
Techniques	Barbara	Lena
DWT+SVD	33.92	43.54
DWT+SVD with signature (Gupta and Raval, 2012)	33.29	39.78
DWT+SVD+CS (Gaussian)	33.73	43.16
DWT+SVD+CS (Wilkinson)	33.96	43.67

(a) (b) (c)

Fig. 5: Cover images (a) the Barbara image, (b) the Lena image (c) Copyright logo

For evaluating the FPP security issue of the proposed technique, the watermark extraction program is run many times by inserting wrong inputs.

First, if the attacker adds a different compressed logo to the proposed technique, a distorted watermark logo is obtained, as shown in Fig. 6a. Second, if the attacker inserts the whole logo instead of the compressed logo, a distorted watermark logo is obtained, as shown in Fig. 6b. On the contrary, if the attacker inserts his logo instead of the required logo to the conventional DWT+SVD, the attacker logo is extracted instead of the owner logo. This result confirms that the program is very secure compared to the DWT+SVD technique.

To evaluate the robustness of the proposed method versus different attacks, the CC between the original and extracted watermark is measured and tabulated in Table 2 to 4. Table 2 summarizes the proposed technique's CC results and the conventional techniques in signal processing and compression attacks. It can be noticed from Table 2 that the proposed technique is more robust to signal processing and compression attacks compared to the conventional techniques, especially if the logo is embedded in the Barbara image.

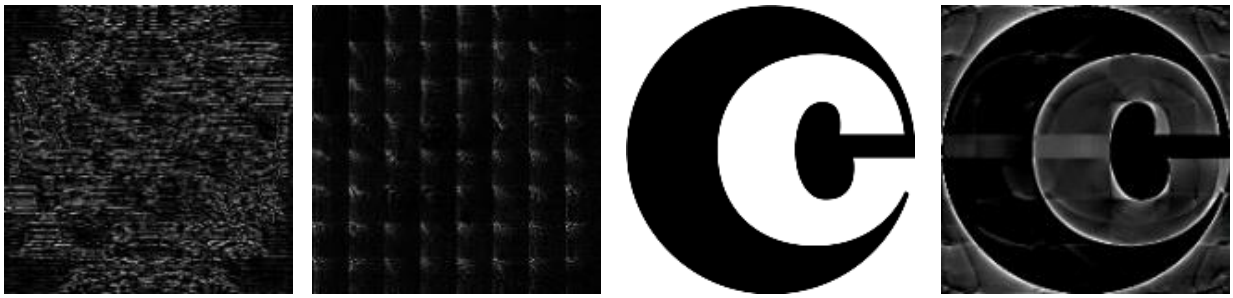

Fig. 6: Security evaluation (a) inserting a different measured vector y for the proposed technique, (b) inserting the whole logo (c) attacker logo (d) inserting attacker logo to the conventional DWT+SVD

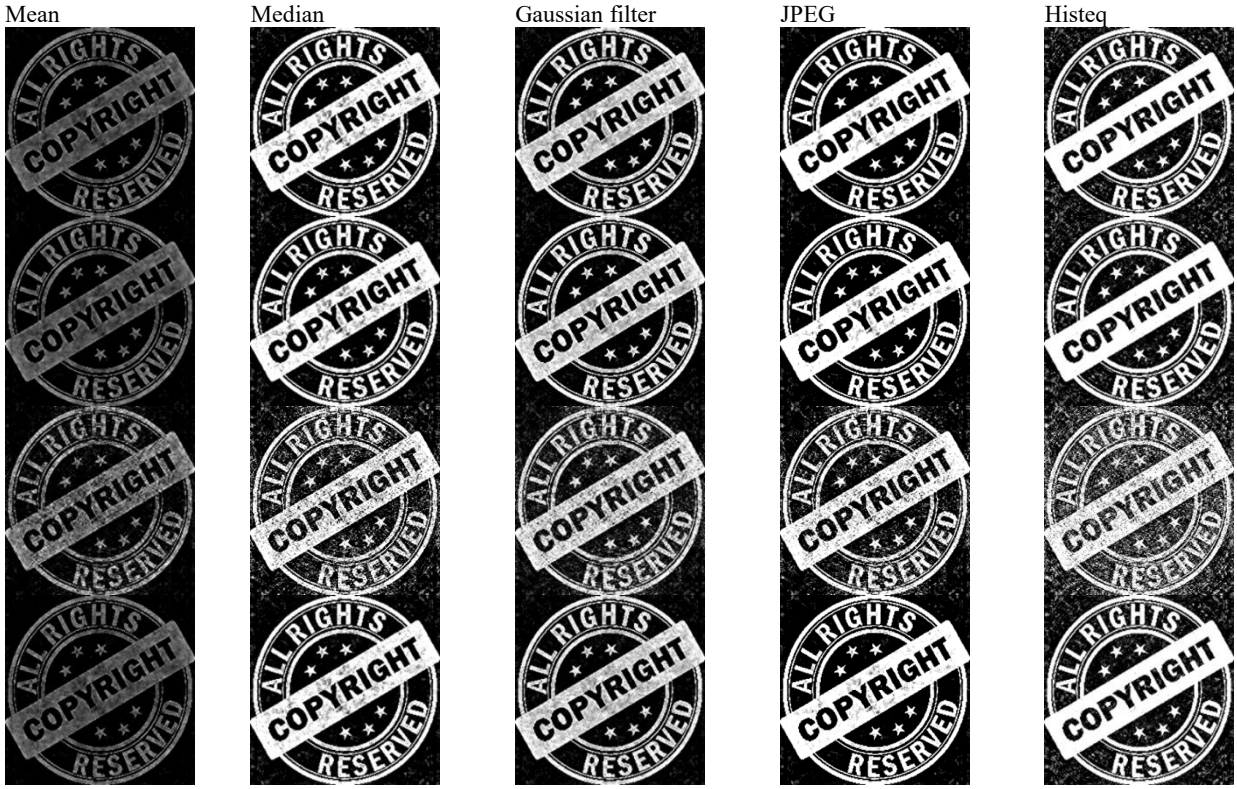

Fig. 7: Extracted watermark logo after signal processing and compression attacks for different technique. Row1: DWT+SVD technique, Row2: DWT+SVD with signature technique, Row3: CS+DWT+SVD based on Gaussian matrix technique and Row4: Proposed CS+DWT+SVD technique

Table 2: The signal processing and compression attack analysis of the proposed Technique versus the conventional techniques in terms of CC

		Signal processing and compression attacks									
		Barbara					Lena				
Techniques		Mean	Median	Gaussian	Jpeg	Histeq	Mean	Median	Gaussian	Jpeg	Histeq
DWT+SVD	CC	0.921	0.871	0.933	0.904	0.884	0.901	0.868	0.912	0.896	0.867
DWT+SVD with signature		0.921	0.871	0.933	0.904	0.885	0.901	0.867	0.912	0.896	0.870
DWT+SVD+CS (Gaussian) (Gupta and Raval, 2012)		0.817	0.737	0.818	0.798	0.727	0.806	0.738	0.775	0.779	0.690
DWT+SVD+CS (Wilkinson)		0.930	0.889	0.942	0.918	0.900	0.909	0.885	0.923	0.910	0.885

Table 3: The Noise attack analysis of the proposed Technique versus the conventional techniques in terms of CC

		Noise attack							
		Barbara				Lena			
Techniques		Salt and pepper	Salt and pepper 15%	Salt and pepper 15%+Adp-filter	Gaussian noise	Salt and pepper	Salt and pepper 15%	Salt and pepper 15%+Adp-filter	Gaussian noise
DWT+SVD	CC	0.760	0.738	0.847	0.739	0.757	0.737	0.852	0.739
DWT+SVD with signature (Gupta and Raval, 2012)		0.755	0.738	0.849	0.737	0.752	0.737	0.842	0.738
DWT+SVD+CS (Gaussian)		0.604	0.579	0.712	0.580	0.602	0.578	0.692	0.578
DWT+SVD+CS (Wilkinson)		0.785	0.764	0.864	0.767	0.784	0.763	0.853	0.764

Table 4: The geometric attack analysis of the proposed Technique versus the conventional techniques in terms of CC

		Geometric attack							
		Barbara				Lena			
Techniques		Rotate 45	Rotate 90	Shear	Crop	Rotate 45	Rotate 90	Shear	Crop
DWT+SVD	CC	0.861	0.958	0.906	0.949	0.757	0.959	0.852	0.852
DWT+SVD with signature		0.860	0.958	0.906	0.949	0.757	0.959	0.852	0.836
DWT+SVD+CS (Gaussian)		0.717	0.806	0.784	0.859	0.604	0.810	0.709	0.701
DWT+SVD+CS (Wilkinson)		0.879	0.961	0.921	0.957	0.782	0.962	0.871	0.856

The CC results of the proposed technique and the conventional techniques against noise attacks are given in Table 3. The results in this table reflect that the proposed method improves the robustness in noise attacks compared to the conventional techniques, especially the DWT+SVD+CS technique based on the Gaussian matrix. Also, concerning the geometric attacks, the CC is measured and given in Table 4. It can be observed that the performance of the proposed method is more robust than conventional techniques against the geometric attack.

Therefore, it can be concluded from the tables' results that the proposed DWT+SVD+CS based on the Wilkinson matrix technique outperforms the other techniques in robustness. However, it can be noticed that the proposed technique has a strong ability to resist signal processing, compression and geometric attack better than the noise attack.

To compare visually between the extracted watermark logo obtained from the proposed technique and the conventional techniques Figs. 7 and 8 present the extracted watermark logo from those techniques.

Figure 7 shows the extracted watermark logo after applying signal processing and compression attack. It can be perceived that the extracted watermark logo from DWT+SVD and DWT+SVD with signature and the proposed technique is clear except the logo extracted after the mean filter attack, the images suffer from some darkness. The extracted watermark logo from CS+DWT+SVD based on the Gaussian matrix suffers from the darkness for mean attack and suffers from distortion for JPEG and histogram equalization attacks.

Figure 8 shows the extracted watermark logo for noise attacks and geometric attacks after applying these attacks for all the mentioned techniques. It can be noticed from row 1 and row 2 that the extracted watermark logo from CS+DWT+SVD based on the Gaussian matrix suffers from a high distortion for all the noise attacks. However, the DWT+SVD, DWT+SVD with signature and the proposed techniques suffer from a little distortion.

For geometric attack, the extracted watermark logo from CS+DWT+SVD based on the Gaussian matrix suffers from high distortion and darkness for the geometric attack except for rotate 90 the distortion is smaller than the other geometric attacks as shown in row 3,4 and 5 in Fig. 8. On the contrary, the extracted watermark logo from the proposed technique and the DWT+SVD and DWT+SVD with signature techniques suffer from a bit of distortion compared to DWT+SVD+CS based on Gaussian matrix for rotate 45 and crop attacks. This visual analysis is matched with the numerical results in the tables.

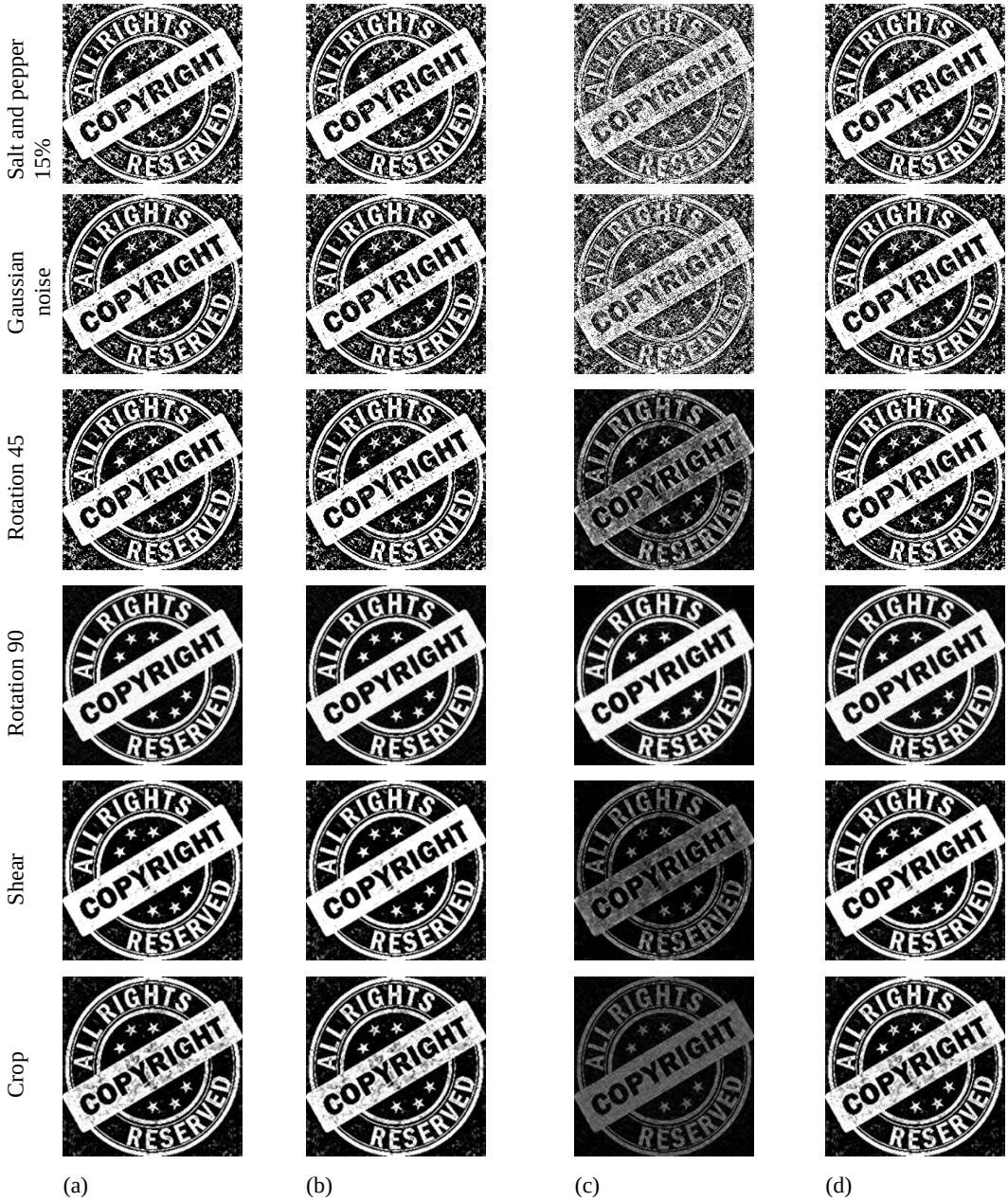

Fig. 8: Extracted watermark logo after noise and geometric attacks for different techniques (a) DWT+SVD technique (b) DWT+SVD with signature technique (c) CS+DWT+SVD based on Gaussian matrix technique (d) proposed CS+DWT+SVD technique

Conclusion

In this research, the idea of scramble compressed sensed watermark logo based on Wilkinson matrix is proposed. The objective of the proposed work is to overcome the lack of reconstruction quality of the watermark logo, increase the robustness and improve the traditional DWT+SVD+CS scheme's security. Signal processing, compression, geometric and noise attacks are applied to the traditional and the proposed technique to evaluate their robustness. PSNR and CC are used as metrics to evaluate the watermarked image and watermark logo's quality, respectively. First, the PSNR results illustrate that the proposed technique improves the watermarked image quality compared to all the conventional techniques, especially for a smooth image. Second, the CC results demonstrated that the proposed techniques resist all the attacks better than conventional techniques, especially for Signal processing, compression and geometric attacks and these results are confirmed through visual analysis. Third, the security is tested by using an unauthorized watermark logo for the extraction program. The

proposed technique did not extract the watermark logo; however, DWT+SVD extract the attacker logo.

Moreover, sending the watermark logo in a compressed form increases the security and is considered an advantage for limited resource applications that need to save power and reduce the required bandwidth to transmit the whole watermark logo. However, the proposed technique has a limitation on the property of the selected watermark. It should be sparse on time or frequency domains to apply the Compressive sensing to it and improve the performance.

Applying the proposed method to the color images using different color systems will be addressed in future research using different measurement matrix and reconstruction algorithms in compressive sensing theory.

Acknowledgment

The authors would like to thank all our colleagues and the researchers in the department who give us useful comments about the work, also we are grateful to the encourage and support of our institute with the required tools and software.

Author's Contributions

Rasha Shoitan: Contributed to the Algorithm design, the Algorithm implementation, experiments and the paper writing.

Sawsan Morkos Gharghory: Supervised the problem definition, the design method, the experiments and the paper writing.

Ethics

The Authors confirm that the research paper is original, the experimental results are not published before and no ethical issues are involved.

References

Bahadur, K., & Chandra, V. (1959). Decomposition of urea by urease. Enzymologia, 21, 1-12.

Candès, E. J. (2006, August). Compressive sampling. In Proceedings of the international congress of mathematicians (Vol. 3, pp. 1433-1452). https://doi.org/10.4171/022-3/69

Candès, E. J., & Wakin, M. B. (2008). An introduction to compressive sampling. IEEE signal processing magazine, 25(2), 21-30. https://doi.org/10.1109/MSP.2007.914731

Candès, E. J., Romberg, J. K., & Tao, T. (2006). Stable signal recovery from incomplete and inaccurate measurements. Communications on Pure and Applied Mathematics: A Journal Issued by the Courant Institute of Mathematical Sciences, 59(8), 1207-1223. https://doi.org/10.1002/cpa.20124

Chang, C. C., Tsai, P., & Lin, C. C. (2005). SVD-based digital image watermarking scheme. Pattern Recognition Letters, 26(10), 1577-1586. https://doi.org/10.1016/j.patrec.2005.01.004

Chen, G., Chen, Q., Zhang, D., & Chen, Y. (2013). A watermarking scheme based on compressive sensing and Bregman iteration. International Journal of Computers and Applications, 35(4), 173-180. https://www.tandfonline.com/doi/abs/10.2316/Journal.202.2013.4.202-3844

Chi, X., & Feng, G. (2014, October). A robust digital watermarking algorithm based on SVD of compressive sampling measurements. In 2014 7th International Congress on Image and Signal Processing (pp. 318-322). IEEE. https://doi.org/10.1109/CISP.2014.7003799

Fazli, S., & Moeini, M. (2016). A robust image watermarking method based on DWT, DCT and SVD using a new technique for correction of main geometric attacks. Optik, 127(2), 964-972. https://doi.org/10.1016/j.ijleo.2015.09.205

Gupta, A. K., & Raval, M. S. (2012). A robust and secure watermarking scheme based on singular values replacement. Sadhana, 37(4), 425-440. https://doi.org/10.1007/s12046-012-0089-x

Hu, H. T., & Hsu, L. Y. (2015). Exploring DWT–SVD–DCT feature parameters for robust multiple watermarking against JPEG and JPEG2000 compression. Computers & Electrical Engineering, 41, 52-63. https://doi.org/10.1016/j.compeleceng.2014.08.001

Huang, H. C., & Chang, F. C. (2014). Robust image watermarking based on compressed sensing techniques. Journal of Information Hiding and Multimedia Signal Processing, 5(2), 275-285. http://www.jihmsp.org/~jihmsp/2014/vol5/JIH-MSP-2014-02-014.pdf

Jane, O., & Elbaşi, E. (2014). Hybrid non-blind watermarking based on DWT and SVD. Journal of applied research and technology, 12(4), 750-761. https://doi.org/10.1016/S1665-6423(14)70091-4

Li, N., Zheng, X., Zhao, Y., Wu, H., & Li, S. (2008, August). Robust algorithm of digital image watermarking based on discrete wavelet transform. In 2008 International Symposium on Electronic Commerce and Security (pp. 942-945). IEEE. https://doi.org/10.1109/ISECS.2008.140

Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. IEEE transactions on multimedia, 4(1), 121-128. https://doi.org/10.1109/6046.985560

Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2018). Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. Multimedia Tools and Applications, 77(20), 26845-26879. https://doi.org/10.1007/s11042-018-5891-y

Meenakshi, S. B. (2015). A survey of compressive sensing based greedy pursuit reconstruction algorithms. International Journal of Image, Graphics and Signal Processing, 7(10), 1-10. https://doi.org/10.5815/ijigsp.2015.10.01

Mrak, S. G. M. G. (2004). Reliability of objective picture quality measures. Journal of Electrical Engineering, 55(1-2), 3-10. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.105.3785&rep=rep1&type=pdf

Needell, D., Tropp, J., & Vershynin, R. (2008, October). Greedy signal recovery review. In 2008 42nd Asilomar conference on signals, systems and computers (pp. 1048-1050). IEEE. https://doi.org/10.1109/ACSSC.2008.5074572

Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. (pp. 709-716). IEEE. https://doi.org/10.1109/INDIN.2005.1560462

Qaisar, S., Bilal, R. M., Iqbal, W., Naureen, M., & Lee, S. (2013). Compressive sensing: From theory to applications, a survey. Journal of Communications and networks, 15(5), 443-456. https://doi.org/10.1109/JCN.2013.000083

Rabah, H., Amira, A., Mohanty, B. K., Almaadeed, S., & Meher, P. K. (2014). FPGA implementation of orthogonal matching pursuit for compressive sensing reconstruction. IEEE Transactions on very large scale integration (VLSI) Systems, 23(10), 2209-2220. https://doi.org/10.1109/TVLSI.2014.2358716

Rani, A., Bhullar, A. K., Dangwal, D., & Kumar, S. (2015). A zero-watermarking scheme using discrete wavelet transform. Procedia Computer Science, 70, 603-609. https://doi.org/10.1016/j.procs.2015.10.046

Romberg, J. (2008). Imaging via compressive sampling. IEEE Signal Processing Magazine, 25(2), 14-20. https://doi.org/10.1109/MSP.2007.914729

Shoitan, R., Nossair, Z., Ibrahim, I. I., & Tobal, A. (2018a). Improving the reconstruction efficiency of sparsity adaptive matching pursuit based on the Wilkinson matrix. Frontiers of Information Technology & Electronic Engineering, 19(4), 503-512. https://doi.org/10.1631/FITEE.1601588

Shoitan, R., Tobal, A., Nossair, Z., & Ibrahim, I. I. (2018b, April). Performance Improvement of Orthogonal Matching Pursuit Based on Wilkinson Matrix for Block Compressive Sensing. In 2018 1st International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-7). IEEE. https://doi.org/10.1109/CAIS.2018.8442028

Singh, D., & Singh, S. K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimedia Tools and Applications, 76(11), 13001-13024. https://doi.org/10.1007/s11042-016-3706-6

Thakkar, F. N., & Srivastava, V. K. (2017). A fast watermarking algorithm with enhanced security using compressive sensing and principle components and its performance analysis against a set of standard attacks. Multimedia Tools and Applications, 76(14), 15191-15219. https://doi.org/10.1007/s11042-016-3744-0

Tropp, J. A., & Gilbert, A. C. (2007). Signal recovery from random measurements via orthogonal matching pursuit. IEEE Transactions on information theory, 53(12), 4655-4666. https://doi.org/10.1109/TIT.2007.909108

Wang, N., Li, Z., Cheng, X., & Chen, Y. (2017, October). Dual watermarking algorithm based on singular value decomposition and compressive sensing. In 2017 IEEE 17th International Conference on Communication Technology (ICCT) (pp. 1763-1767). IEEE. https://doi.org/10.1109/ICCT.2017.8359932

Xu, Z. J., Wang, Z. Z., & Lu, Q. (2011). Research on image watermarking algorithm based on DCT. Procedia Environmental Sciences, 10, 1129-1135. https://doi.org/10.1016/j.proenv.2011.09.180

Zhou, X., Zhang, H., & Wang, C. (2018). A robust image watermarking technique based on DWT, APDCBT and SVD. Symmetry, 10(3), 77. https://doi.org/10.3390/sym10030077