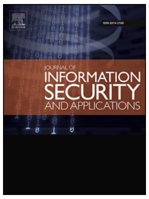
Journal of Information Security and Applications 44 (2019) 144–156

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa



Hybrid secure and robust image watermarking scheme based on SVD and sharp frequency localized contourlet transform

E. Najafi[a,*], K. Loukhaoukha[b,c]

[a] Department of Mathematics, Faculty of Science, Urmia University, Urmia 51818-57561, Iran
[b] Development Research Center, Algiers, Algeria
[c] Department of Electrical and Computer Engineering, Laval University, Québec, Canada

ARTICLE INFO

Article history:

Keywords:
Contourlet transform
Singular values
Image processing
Image watermarking
Ambiguity attacks

ABSTRACT

In this paper, using singular value decomposition (SVD) and sharp frequency localized contourlet transform (SFLCT) a secure and robust image watermarking procedure is introduced. The SVD and SFLCT are applied on both watermark and original images and using the properties of the SVD and utilizing the advantages of the SFLCT, noticeable results of the watermarking requirements are obtained. Since most of the SVD based watermarking schemes are not resistant against ambiguity attacks and suffer from the false positive problem, this objection is resolved without adding extra steps to the watermarking algorithm and the suggested scheme is secure and resistant against ambiguity attacks. The simulation of the scheme is implemented and its robustness against various types of attacks is experimented. In comparison with some of the recent schemes this procedure shows high imperceptibility, capacity and robustness and these features make the scheme a suitable choice for the image processing applications.

1. Introduction

Nowadays, multimedia productions and their distributions are performed in digital form. One of the most important features of the digital data is their unlimited copying without any loss of quality. This advantage is not good for multimedia owners. Digital watermarking is developed to serve them to protect their products against unauthorized usages. The digital watermarking has applications like copy and copyright protections, ownership identification, authentication, secret communication and medical applications [1–3,5]. The information related to the ownership is watermark and is embedded in the original data (cover work) without loss of quality of the data and resistant (robust) under some digital operations.

All digital watermarking procedures include two apart processes: the embedding process of the watermark and its detection process. The embedding process is done in the transmitter side and the detection process is implemented in the receiver part.

The important requirements of a watermarking scheme are robustness, capacity, imperceptibility and security. Robustness is the ability of the scheme in protecting the watermark under several attacks and is application-dependent [6,18,41]. This feature is measured by normalized correlation (NC) quantity which has an absolute value between 0 and 1. The second requirement is capacity and indicates the amount of all information which is embedded in the selected cover work [20]. Embedding the watermark changes the visual properties of the cover work. This reduction is imperceptibility feature of the scheme and is measured by peak signal-to-noise ratio (PSNR). A scheme is more imperceptible if this loss is low and then PSNR is high. For an image, generally the minimum acceptable value for the PSNR is 38 dB [21]. The security refers to ability of the watermarking scheme to resist intentional tampering [19].

Digital watermarking is classified into two categories: spatial domain techniques like least significant bits (LSB) [4] and transform domain techniques in which the most used transforms are discrete cosine transform (DCT) [7,8], discrete Fourier transform (DFT) [9], and discrete wavelet transform (DWT) [11–16]. Digital watermarking has been implemented widely with DWT which has good properties like multiresolution representation, superior human visual system modeling and time frequency localization. But in 2D, wavelets lack the directional property which is important in efficient computational image representation. This problem is solved using contourlet transform (CT) introduced by Do and Vetterli [22]. The contourlet is a non-separable 2D transform and a combination of the Laplacian pyramid [23] and the directional filter banks (DFB) [42].

* Corresponding author.
E-mail addresses: e.najafi@urmia.ac.ir (E. Najafi), khaled.loukhaoukha.1@ulaval.ca (K. Loukhaoukha).

https://doi.org/10.1016/j.jisa.2018.12.002
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

CT captures the edges of the images in many directions and resolutions efficiently, but is not ideal in the frequency domain. Some waste components of frequency reduce the efficiency of contourlets in representing smooth contours of images. In [24] the authors represent sharp frequency localized contourlet transform (SFLCT) in which the non-localization problem is considerably decreased. In this study, the proposed watermarking scheme utilizes the useful properties of the SFLCT to enhance the watermarking requirements.

In most of the image processing applications researchers are considered the combination of two or more transforms to achieve the watermarking procedure goals [10,12–14,17,25,36]. Because of efficient properties, singular value decomposition (SVD) is used as a second transform in these hybrid watermarking systems. In this transform, image A is decomposed as

$$A = U \Sigma V^T,$$

where U and V are orthogonal matrices and Σ is a diagonal matrix. The diagonal entries of Σ are called singular values of A. These singular values are insensitive to small perturbations and the visual quality of the image changes very slightly under small variations of the singular values. Because of this special feature, SVD has been used in watermarking and the imperceptibility and robustness of SVD-based watermarking algorithms have been improved. However, considering SVD-based watermarking algorithms shows that these algorithms suffer from security requirement and are not resistant against ambiguity attacks introduced by Craver et al. [26]. In the lack of security, both the owner and attacker are able to extract their watermarks from the watermarked image, then neither can prove the ownership. This is the false positive problem which is a serious objection for the SVD-based watermarking techniques.

In this study a secure, robust and imperceptible image watermarking based on sharp frequency localized contourlet transform and SVD (SFLCT-SVD) is investigated and proposed. These two transforms have useful properties and we show that combining them increase the quality of the watermarking scheme. We solve the false positive problem of the SVD based schemes and resisting against ambiguity attacks by increasing the dependency of the embedding and detection processes on the watermark and it is possible due to variant downsampling rate d of the SFLCT. This preference also allows us to increase the watermark image size and choose it as same size as the original image. On the other hand, using SFLCT the useful properties of the SVD based algorithms (high PSNR and robustness) are protected. In the other words, these two transforms resolve the fault of each other and the advantages of each of them are preserved in the watermarking scheme. The host and the watermark images are both decomposed using SFLCT. Then the SVD transform are applied to some subbands of the host and watermark images.

The rest of the paper is organized as follows: In Section 2 the methodology and related work are stated and a brief review of the transforms used in the scheme are given. In Section 3 the proposed watermarking scheme (i.e., the embedding and detection processes) is explained in details. Section 4 describes the requirements of a watermarking procedure and Section 5 includes the experimental implementations and obtained results of the suggested procedure. In Section 6 the introduced scheme in this paper is compared to some recent schemes and finally in Section 7 the conclusions of the paper are stated.

2. Methodology and related work

When we consider the SVD-based image watermarking schemes, we see that the reason of the false positive problem is concerned with low dependency of schemes on the watermark in both embedding and detection processes. Indeed, by reviewing these algorithms, the most of them act as follows:

$$\Sigma + \alpha w = U_w \Sigma_w V_w^T.$$

In this equation Σ is the singular values of a frequency subband of original image, w is the watermark or a subband of its transform and α is the strength factor. The singular values Σ are modified by Σ_w in the host image and the orthogonal matrices U_w and V_w are used as secret keys in the detection process. These matrices include lots of important information of an image in comparison with the singular values which contain minor data of image like luminance. Then insufficient information of the watermark is embedded in the host image. This weakness is intensified by small strength factor α and the false positive problem takes place such that applying pirate matrices U_p and V_p as secret keys, will extract pirate watermark w_p independent of the extracted singular values, then the scheme is leaved unprotected against ambiguity attacks [28,29]. This shows that the singular values of an image solely are not sufficient in some applications like ownership right proof, transaction tracking and data authentication. Algorithms in [10,12,13,25,37] used this exposed and insecure scheme.

In recent years authors aim to introduce and solve this problem and several solutions are proposed. In [30] the authors comment on a watermarking scheme that use SVD and is fundamentally flawed in that the extracted watermark is not the embedded watermark. Again in [31] the authors show that a SVD-based scheme has some defects ans it cannot be used in secure multimodal biometric systems. In [32] the authors gather all the issues belong to the false positive problem with SVD-based schemes.

To solve the security shortcoming in [34] the authors suggested encrypting the watermark in the embedding process. Signature-based solutions are also proposed in [14,35]. In [35] the authors construct a signature for excepting the orthogonal matrices U and V and perform this authentication system before extraction step. In [14] the authors generate a digital signature using the orthogonal matrices U and V, a special key and a SHA-1 algorithm and then embed it into the watermarked image.

It seems that extracting a signature from a watermarked image is not enough in applications like the proof of ownership. An attacker can extract a pseudo-signature from the watermarked image and then by using the false positive problem of the SVD transform frustrates the proof of ownership.

Our proposed SFLCT-SVD scheme shows high robustness against many types of geometrical and non-geometrical attacks. The PSNR value related to the imperceptibility property is enhanced and moreover, as explained before, the false positive problem is solved without performing extra implementations like authentication processes or signatures recognition and also it is shown that our watermarking scheme is resistant against ambiguity attacks. The suggested procedure possesses all requirements of the watermarking schemes involving imperceptibility, robustness, capacity and security with high level in comparison with the preceding schemes [12,14,36] and these features make the scheme a good choice for the proof of ownership, data authentication and copyright protection applications.

2.1. The sharp frequency localized contourlet transform

The sharp frequency localized contourlet transform introduced by Lu et al. [24] is a new construction of the contourlet transform which solves the non-localization problem of the original contourlet transform. The original one is a combination of the Laplacian pyramid [23] and directional filter banks (DFB) [42] and as a directional multiresolution image representation, can efficiently capture and represent smooth object edges of the natural images.

In the practice, the filters which are used in the original transform are non-ideal where lead the non-localization problem in the

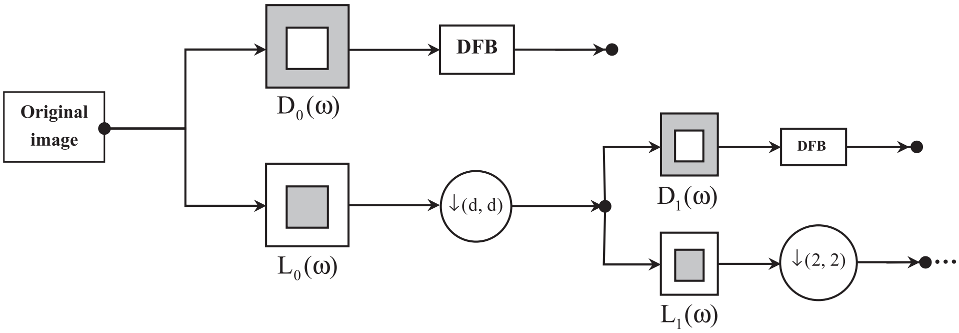


Fig. 1. The block diagram of 2 levels image decomposition of SFLCT. The synthesis part is exactly symmetric.

frequency domain. In these filters, there are components of frequencies at locations far away from the desired support. These aliasing components have noticeable effect on the edge representation in the spatial domain and cause their representation to be irregular, then decreasing the efficiency of the contourlets in displaying smooth boundaries in natural images [24].

In the new construction the problem has been solved by introducing a new multiscale decomposition defined in the frequency domain instead of using the Laplacian pyramid, and the DFB is still used for directional decomposition (See Fig. 1).

As an important difference from the Laplacian pyramid, the new multiscale pyramid can employ a different set of lowpass and highpass filters for the first level and all other levels. This is a crucial step in reducing the frequency-domain aliasing of the DFB [24]. In this implementation first lowpass filters $L_i(\omega), i = 0, 1$ are specified such that the aliasing components are canceled. To reach this aim, the passband and stopband frequencies are properly limited such that the resulting contourlet filter is localized in frequency domain. Then from the simplified perfect reconstruction condition $|L_i(\omega)|^2 + |D_i(\omega)|^2 = 1$, the highpass filters $D_i(\omega)$ can be obtained. This new contourlet construction is implemented for each three choices of downsampling rate $d = 1, \frac{3}{2}, 2$.

Compared to the old version, the new construction produces basis images with much better localization in the frequency domain and regularity in the spatial domain. Fig. 2 shows the differences between the new and the old versions of the contourlet transform. Our watermarking scheme benefits from these useful properties of the SFLCT along with the different choices of d.

In spite of the preferences, in the new contourlet transform more filters than the original contourlet transform are used and still both the up-sampling and down-sampling operations are employed meaning that it is not shift-invariant. Applying lowpass and highpass filters and the lack of shift-invariant property impose some limitations on our watermarking scheme. The extraction of the watermark is not perfect and when extracting the watermark some subbands other than those the watermark is embedded are varied in the watermarked image.

2.2. Singular value decomposition (SVD)

In recent years the SVD has become a computationally viable tool for solving a wide variety of problems arising in many practical applications. The crux of using the SVD in many applications is in the fact that the most of the computations need to be done under the presence of impurities (noises) in the data and the SVD is very effective for these computations [43]. In signal and speech processing the SVD can be regarded as a filter that produces an estimate of a signal from noisy data. In the area of digital signal processing, the SVD is effective and widely used such as in noise reduction, image restoration, power spectrum estimation and data compression [44,46,47].

Let image A is as a real $N \times N$ matrix with rank $r \leq N$. Then there exist unitary $N \times N$ matrices U and V such that

$$A = U\Sigma V^T,$$

where $\Sigma = diag(\sigma_1, \sigma_2, \ldots, \sigma_N)$ is a diagonal matrix and the diagonal entries $\sigma_i, i = 1, \ldots, N$ are called singular values of the matrix A. The singular values are in nonincreasing order $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r = \cdots = \sigma_N = 0$ and many of these singular values have a small value in comparison with the σ_1. For the large matrices the computation of the SVD must be done using data analysis methods. Of the most effective methods are the algorithms based on parallel computing such as sparse principle component analysis [40].

We have the following properties of the SVD of an image A:

- The singular values represent the algebraic properties of A like luminance. To show, let we change these values as $\Sigma_\varepsilon = \varepsilon\Sigma$, then

  $$A_\varepsilon = U\varepsilon\Sigma V^T = \varepsilon A.$$

  Now, if $0 < \varepsilon < 1$, A will be darkened and if $\varepsilon > 1$, then A will be brightened.
- For an arbitrary matrix the singular values always exist. These values are insensitive to small perturbations and are well-conditioned. Indeed, for $\varepsilon > 0$ let $\Sigma_\varepsilon = \Sigma + \varepsilon I$, then

  $$A_\varepsilon = U\Sigma_\varepsilon V^T = A + \varepsilon UV^T.$$

  The arrays of the matrix εUV^T are small and can be ignored in comparison with the arrays of A. Then adding a small value ε to the singular values does not change A significantly.
- Since a lot of data of an image belong to the orthogonal matrices U and V, then image A is sensitive to their small variations. In this case, if we let $U_\varepsilon = U + \varepsilon\mathbf{1}$ with $\mathbf{1}$ a matrix with 1 arrays, we have

  $$A_\varepsilon = U_\varepsilon\Sigma V^T = A + \varepsilon\mathbf{1}\Sigma V^T.$$

  The matrix $\varepsilon\mathbf{1}\Sigma V^T$ has big arrays, then A_ε is very different than A.

3. The proposed SFLCT-SVD scheme

In this section the suggested SFLCT-SVD watermarking scheme is described in details. The scheme has two important parts: the embedding and the detection processes. In the embedding process the watermark image is embedded in the host image and the result is the watermarked image. The watermarked image may be attacked by image processing or geometrical manipulations during the transfer operation and in the receiver part the attacked watermarked image is considered by detection process to extract the watermark. The two embedding and extracting procedures are shown in Figs. 3 and 4 and Algorithms 1 and 2 represent the steps, respectively.

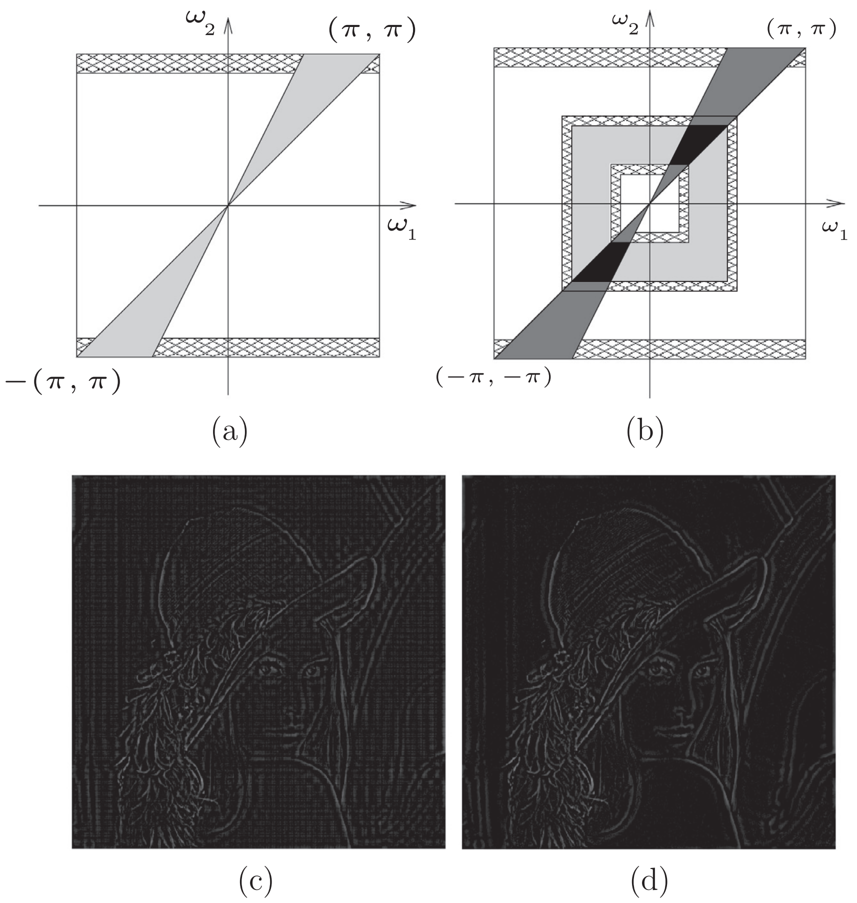


Fig. 2. The differences between the original and the new contourlet transforms: (a) Frequency domain aliasing problem in the original contourlet transform. (b) Illustration of how aliasing components are canceled in the new construction. (c) Frequency localization in the spatial domain in the original contourlet transform of Lena image. (d) The improvement in the frequency localization in the spatial domain.

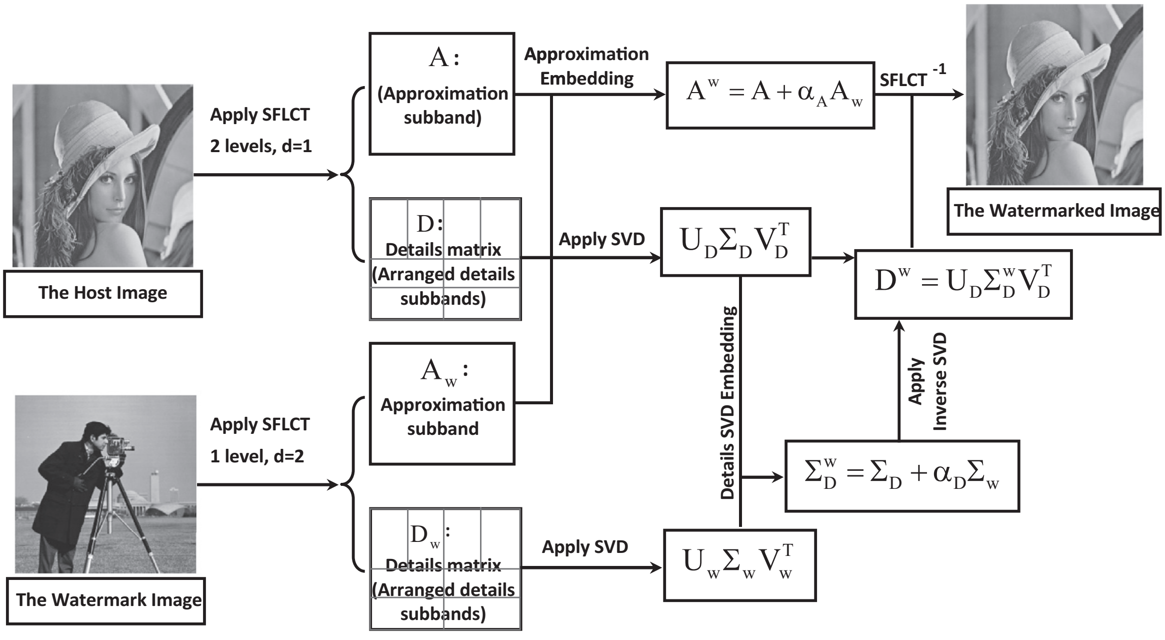


Fig. 3. The watermark embedding scheme.

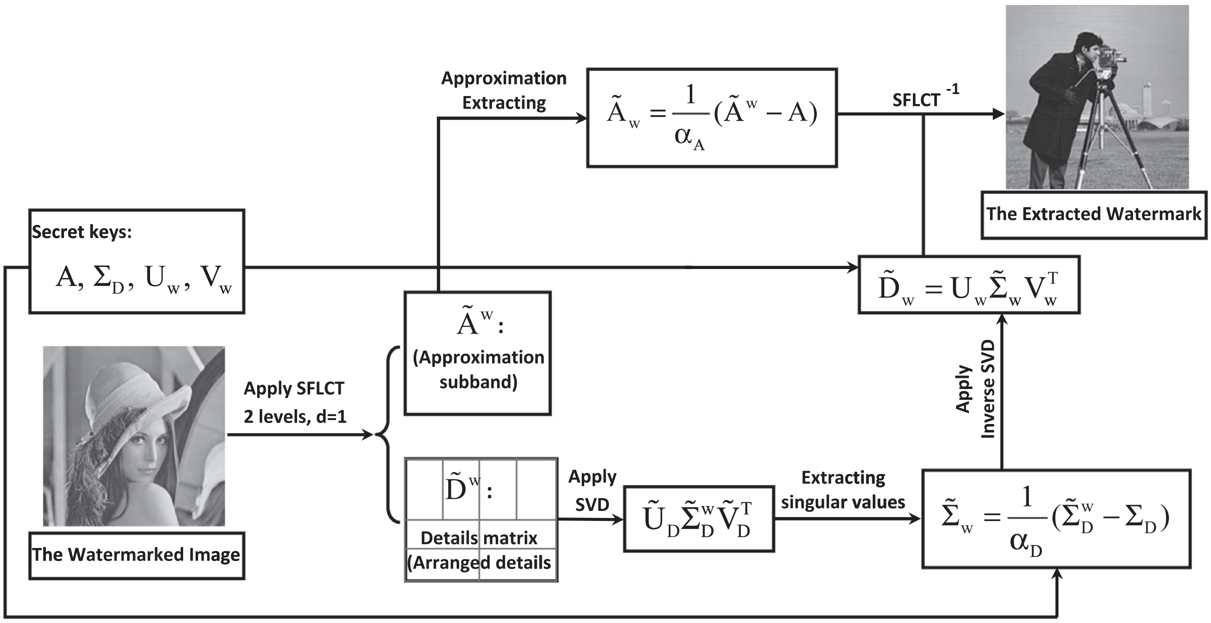

Approximation Extracting
$\tilde{A}_w = \frac{1}{\alpha_A}(\tilde{A}^w - A)$
SFLCT $^{-1}$
The Extracted Watermark
Secret keys:
A, Σ_D, U_w, V_w
$\tilde{D}_w = U_w \tilde{\Sigma}_w V_w^T$
$\tilde{A}^w$: (Approximation subband)
Apply SFLCT 2 levels, d=1
Apply Inverse SVD
The Watermarked Image
$\tilde{D}^w$:
Details matrix (Arranged details
Apply SVD
$\tilde{U}_D \tilde{\Sigma}_D^w \tilde{V}_D^T$
Extracting singular values
$\tilde{\Sigma}_w = \frac{1}{\alpha_D}(\tilde{\Sigma}_D^w - \Sigma_D)$

Fig. 4. The watermark extracting scheme.

Table 1
PSNR and noise attacks mean NC in selection of optimal values for α_A and α_D.

α_A \ α_D	0.002	0.004	0.006	0.008	0.010	0.012	0.014	0.016	0.018	0.020
0.002	59.06 0.1364	58.49 0.1428	57.69 0.1531	56.77 0.1777	55.81 0.1935	54.87 0.2065	53.97 0.2122	53.13 0.2184	52.33 0.2254	51.59 0.2332
0.004	53.19 0.8121	53.04 0.8276	52.80 0.8425	52.47 0.8545	52.09 0.8652	51.67 0.8730	51.22 0.8799	50.75 0.8843	50.27 0.8893	49.79 0.8916
0.006	49.70 0.8721	49.63 0.8834	49.52 0.8944	49.36 0.9044	49.17 0.9131	48.95 0.9201	48.70 0.9248	48.43 0.9290	48.15 0.9317	47.85 0.9312
0.008	47.21 0.8929	47.17 0.9002	47.11 0.9071	47.02 0.9135	46.91 0.9182	46.77 0.9222	46.62 0.9251	46.45 0.9273	46.27 0.9295	46.07 0.9284
0.010	45.28 0.9373	45.25 0.9414	45.21 0.9448	45.15 0.9477	45.08 0.9495	44.99 0.9506	44.89 0.9510	44.78 0.9505	44.65 0.9498	44.52 0.9480
0.012	43.70 0.9558	43.68 0.9596	43.65 0.9626	43.61 0.9652	43.56 0.9672	43.50 0.9686	43.43 0.9693	43.34 0.9695	43.25 0.9691	43.15 0.9679
0.014	42.36 0.9584	42.35 0.9617	42.33 0.9634	42.30 0.9646	42.26 0.9653	42.21 0.9650	42.16 0.9644	42.10 0.9631	42.03 0.9613	41.95 0.9589
0.016	41.20 0.9702	41.19 0.9720	41.18 0.9736	41.15 0.9748	41.12 0.9757	41.09 0.9761	41.05 0.9762	41.00 0.9760	40.95 0.9757	40.89 0.9744
0.018	40.18 0.9757	40.17 0.9775	40.16 0.9788	40.14 0.9808	40.12 0.9818	40.09 0.9815	40.06 0.9800	40.02 0.9818	39.98 0.9816	39.93 0.9803
0.020	39.26 0.9780	39.26 0.9792	39.25 0.9801	39.23 0.9807	39.21 0.9811	39.19 0.9812	39.16 0.9809	39.13 0.9805	39.10 0.9800	39.06 0.9787

3.1. The embedding process of the watermark

In the embedding process the SFLCT is applied to the both host and watermark images. To achieve the maximum size of the watermark we employ different choices of the downsampling rate d. To this end, in each SFLCT decomposition the parameter d is selected such that the size of the similar subbands of the two decompositions are matched. The host image is decomposed in two levels with downsampling rate $d = 1$ and the watermark image is decomposed in one level with $d = 2$. In the last level of the two decompositions, we unite the details subbands to form a unit details matrix in each decomposition. Then the SVD transform is applied only to the details matrices in both decompositions of the host and the watermark images. This application of SVD increases the robustness feature of the scheme in comparison with the embedding of the details matrix directly to the host image without using SVD.

Two strength factors α_A for approximation subband and α_D for details matrix are used to embed the watermark SFLCT-SVD decomposition components in the host image ones. The values of the two strength factors α_A and α_D affect on the imperceptibility and robustness of the scheme. If we decrease the factors, the imperceptibility is increased but on the other hand, the robustness will be decreased and vice versa (Tables 1 and 2). Then suitable values must be selected to achieve nearly optimal imperceptibility and robustness. To reach this aim, we first compute the PSNR and mean NC under noise attacks for $0.002 \leq \alpha_A \leq 0.02$ and $0.002 \leq \alpha_D \leq 0.02$ with step size 0.002. We choose noise addition

Table 2
PSNR and noise attacks mean NC in selection of nearly optimal values for α_A and α_D.

α_A \ α_D	0.006	0.007	0.008	0.009	0.010	0.011	0.012
0.010	45.21 0.9448	45.19 0.9464	45.15 0.9477	45.12 0.9487	45.08 0.9495	45.04 0.9501	44.99 0.9505
0.0105	44.80 0.9515	44.77 0.9530	44.74 0.9539	44.71 0.9549	44.68 0.9558	44.64 0.9565	44.60 0.9570
0.011	44.40 0.9565	44.37 0.9580	44.35 0.9593	44.32 0.9603	44.29 0.9612	44.25 0.9620	44.22 0.9626
0.0115	44.02 0.9606	44.00 0.9620	43.97 0.9634	43.95 0.9644	43.92 0.9654	43.88 0.9663	43.85 0.9670
0.012	43.65 0.9627	43.63 0.9640	43.61 0.9652	43.59 0.9663	43.56 0.9673	43.53 0.9680	43.50 0.9686

for computing NC, because based on the experimental results, the weakest robustness for our scheme are achieved for these attacks. The PSNR and NC values are calculated for five images with five different watermarks and the mean of the results are observed in Table 1. According to the data, the highlighted values are the best choices, because high PSNR and NC values take place simultaneously. Then, we select smaller step size 0.001 for highlighted small intervals $0.010 \le \alpha_A \le 0.012$ and $0.006 \le \alpha_D \le 0.012$ and compute the PSNR and NC again as are shown in Table 2. As we see the values $\alpha_A = 0.011$ and $\alpha_D = 0.009$ are nearly optimal choices according to the high robustness and acceptable imperceptibility. Recently, some optimization methods for strength factors such as cuckoo search in [48] and firefly algorithm in [49] are presented. Applying such approaches clearly will give same optimal values for our strength factors according to the obtained data.

The steps of the embedding algorithm are as follows:

- Decompose the host image x using SFLCT in two levels with downsampling rate $d = 1$ and obtain the approximation subband A and the details matrix D of the second level.
- In the same manner, apply the SFLCT in one level with $d = 2$ to decompose the watermark image w into approximation subband A_w and details matrix D_w.
  In these two steps we select the decomposition levels and downsampling rate d in such a way the maximum size of the watermark (same size as host image) can be used.
- Change the approximation subband A by directly embedding the approximation subband A_w of watermark with the strength factor α_A:
  $$A^w = A + \alpha_A A_w.$$
  This step will preserve the security property of the watermarking scheme.
- Apply the SVD transform on the details matrices D and D_w:
  $$SVD(D) = U_D \Sigma_D V_D^T, \qquad SVD(D_w) = U_w \Sigma_w V_w^T.$$
- Alter the singular values of the details matrix of the host image Σ_D by embedding the watermark ones using the strength factor α_D as follows:
  $$\Sigma_D^w = \Sigma_D + \alpha_D \Sigma_w.$$
  In these two steps, applying SVD will increase the robustness of the scheme in comparison with the case that SVD is not used (Table 10).
- Employ the inverse SVD on the watermarked singular values Σ_D^w to derive the watermarked details matrix:
  $$D^w = U_D \Sigma_D^w V_D^T.$$
- Finally, the watermarked image is obtained by applying the inverse SFLCT (recomposition) on the watermarked approximation subband A^w and details matrix D^w:
  $$x^w = SFLCT^{-1}(A^w, D^w).$$

Algorithm 1: The watermark embedding process.

```
$(A, D)$=SFLCT($x$) in two levels with $d = 1$;
$(A_w, D_w)$=SFLCT($w$) in one level with $d = 2$;
$A^w := A + \alpha_A A_w$;
$(U_D, \Sigma_D, V_D) = svd(D)$;
$(U_w, \Sigma_w, V_w) = svd(D_w)$;
$\Sigma_D^w = \Sigma_D + \alpha_D \Sigma_w$;
$D^w = U_D \Sigma_D^w V_D^T$;
$x^w$ :=SFLCT$^{-1}(A^w, D^w)$;
```

3.2. The watermark extraction procedure

After embedding the watermark, the watermarked image may be reshaped or changed to $\tilde{x}^w$ by some filtering or conversion attacks when transmitting to the receiver part. Many of these attacks that may alter the contents of the watermarked image, are considered in this work. The recipient side must perform the extraction process to detect the watermark. Due to the security property of the scheme, the false positive problem does not occur and if the embedded watermark exists, the detection process only reveals it. If the embedded watermark is different from the considered watermark, then in the detection process no watermark will be detected. The steps of the extraction process are listed below:

- Decompose the distorted watermarked image $\tilde{x}^w$ in two levels by SFLCT with downsampling rate $d = 1$ and in the second level derive the approximation subband $\tilde{A}^w$ and arrange the details subbands to form the details matrix $\tilde{D}^w$.
- Compute the approximation subband of the watermark using the strength factor α_A as follows:
  $$\tilde{A}_w = \frac{1}{\alpha_A}(\tilde{A}^w - A).$$
  In this step the main component of the watermark is extracted.
- Perform the SVD transform on the details matrix $\tilde{D}^w$:
  $$SVD(\tilde{D}^w) = \tilde{U}_D \tilde{\Sigma}_D^w \tilde{V}_D^T.$$
- Compute the singular values of the details matrix of the watermark using strength factor α_D and the secret key Σ_D:
  $$\tilde{\Sigma}_w = \frac{1}{\alpha_D}(\tilde{\Sigma}_D^w - \Sigma_D).$$
- Implement the inverse SVD transform to obtain the details matrix:
  $$\tilde{D}_w = U_w \tilde{\Sigma}_w V_w^T.$$

Table 3
Imperceptibility comparison of the proposed scheme with Makbol et al. [14], Ansari et al. [36] and Lagzian et al. [12] by PSNR values (dB) in watermarking the Lena image.

The proposed scheme	IWD-SVD [14]	DWT-SVD-ABC [36]	RDWT-SVD [12]
44.4589	43.6769	38.3904	38.52

- Apply one level inverse SFLCT with $d = 2$ on the obtained $\tilde{A}_w$ and $\tilde{D}_w$ to extract the attacked watermark $\tilde{w}$:

$$\tilde{w} = SFLCT^{-1}(\tilde{A}_w, \tilde{D}_w).$$

Algorithm 2: The watermark extraction process.

```
$(\tilde{A}^w, \tilde{D}^w)$=SFLCT($\tilde{x}^w$) in two levels with $d = 1$;
$\tilde{A}_w := \frac{1}{\alpha_A}(\tilde{A}^w - A)$;
$(\tilde{U}_w, \tilde{\Sigma}_D^w, \tilde{V}_w) = svd(\tilde{D}_w)$;
$\tilde{\Sigma}_w = \frac{1}{\alpha_D}(\tilde{\Sigma}_D^w - \Sigma_D)$;
$\tilde{D}_w = U_w \tilde{\Sigma}_w V_w^T.$;
$D^w = U_D \Sigma_D^w V_D^T$;
$\tilde{w}$ =SFLCT$^{-1}(\tilde{A}_w, \tilde{D}_w)$;
```

To consider the computational complexity of the proposed scheme, since in the implementation of the procedure, we use two transforms SFLCT and SVD and their inverses, then the computational complexity of the scheme is sum of their computations. The computational complexity of the SFLCT is $O(N)$ [22] and for the SVD is $O(N^3)$ [45] which $N \times N$ is the size of the host image x. Then the computational complexity of the scheme is $O(N^3)$.

4. Requirements of a watermarking system

In this section the requirements which are needed for any watermarking algorithm are considered. The most important criteria are capacity, security, imperceptibility and robustness under different attacks. The offered scheme is compared to some available schemes with respect to these principles.

Capacity is the amount of the data which is embedded in the image. Security and robustness principles are neighboring concepts, which are hardly perceived as different. The intentionality behind the attack is not enough to make a clear cut between these two concepts. For example, image compression is clearly an attack related to robustness, but it might happen intentionally, i.e., with the purpose of removing the watermark, or not [50]. Then our security discussion is limited to the ambiguity attacks and considering the lack of the SVD based watermarking algorithms, the false positive problem. The imperceptibility of the scheme is related to the sensibility of the embedded watermark to the human eye. A high imperceptibility implies high invisibility of the watermark in the watermarked image. This requirement is measured by peak signal-to-noise ratio (PSNR) which calculates the effect of the embedded watermark on the host image. If x is the host image and x^w is the watermarked image, then the PSNR of the watermarking scheme are computed as follows:

$$PSNR = 20\log_{10}\left(\frac{Max(x(i,j))}{\sqrt{MSE}}\right),$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}\Big(x(i,j) - x^w(i,j)\Big)^2,$$

In this relation M and N are the dimensions of the original image and MSE is the mean square error between x and x^w. If the PSNR is high, this shows that the watermark is more invisible and the host image is less affected by the embedding process.

Other criterions which are used for perceptual quality of watermarked images are weighted PSNR (WPSNR) and structural similarity (SSIM) measurements [38,39]. WPSNR uses a texture masking function named noise visibility function (NVF) with a Gaussian model which evaluates existing textures in any area of image:

$$WPSNR = 20\log_{10}\left(\frac{Max(x(i,j))}{\sqrt{WMSE}}\right),$$

$$WMSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} NVF(i,j)\Big(x(i,j) - x^w(i,j)\Big)^2,$$

$$NVF(i,j) = \frac{1}{1 + \theta\sigma_x^2(i,j)}$$

The function σ_x denotes the local variance of image with a 3 × 3 window and θ is a tuning parameter [38]. The SSIM criteria applies luminance, contrast and structure comparison functions and is defined as follow:

$$SSIM(x, x^w) = \frac{(2\mu_x\mu_{x^w} + C_1)(2\sigma_{xx^w} + C_2)}{(\mu_x^2 + \mu_{x^w}^2 + C_1)(\sigma_x^2 + \sigma_{x^w}^2 + C_2)}$$

where μ_x is the mean intensity of image x and C_1 and C_2 are constants dependent on the dynamic range of the pixel values [39].

The next essential is robustness. The robustness is the remain in force of the watermark when the watermarked image is attacked by opponent to remove it. The robustness of a watermarking algorithm is estimated by the normalized correlation (NC) which is defined as

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(w(i,j) - \mu_w)(\tilde{w}(i,j) - \mu_{\tilde{w}})}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(w(i,j) - \mu_w)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(\tilde{w}(i,j) - \mu_{\tilde{w}})^2}}.$$

where $M \times N$ is the size of the watermark and w and $\tilde{w}$ are the embedded and the extracted watermarks, respectively.

5. Experimental implementation and results

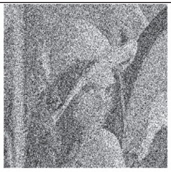
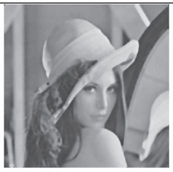
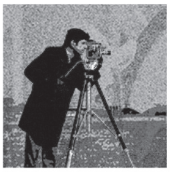
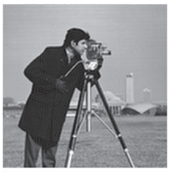
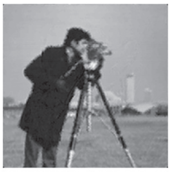
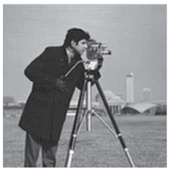
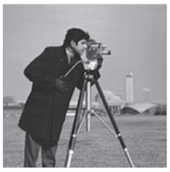
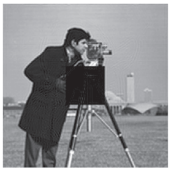
The simulation of the suggested scheme has been performed in MATLAB. We have implemented our scheme on about twenty test images and the results for the known test images Lena of size 512 × 512 and Cameraman of size 512 × 512 have been reported as host and watermark images, respectively, due to comparisons with the other methods.

5.1. The imperceptibility and capacity tests of the proposed scheme

The proposed SFLCT-SVD scheme has been implemented on the Lena image and the computed imperceptibility is stated by PSNR value. This PSNR value is derived with respect to the best NC values of the robustness under all types of attacks according to the selected optimal values of the strength factors α_A and α_D. The calculated value is 44.4589 dB which is compared to the best results of the recent works Makbol et al. [14], Ansari et al. [36] and Lagzian et al. [12] in Table 3. In all of the schemes the selected host and watermark images are Lena and Cameraman, respectively. Table 3 shows the superiority of the proposed SFLCT-SVD scheme when comparing to the previous schemes in the imperceptibility requirement of the watermarking algorithm. Also for the WPSNR and mean SSIM we have computed the values 45.8523 dB and 0.9996 respectively.

About the capacity of the scheme, the property of choosing different downsampling rates d for the SFLCT enables the scheme to have a high capacity between the similar procedures. Fig. 5 shows

Table 4
The NC values of the extracted watermark under different attacks for Lena watermarked image.

Attack	Gaussian noise $V = 0.3$	Sharpening $S = 40$	Median filtering 9×9
Watermarked image			
Extracted watermark			
NC	0.9215	0.9928	0.9693
Attack	Rotation 35°	Shearing $(0.5, 0.5)$	Center cropping 120×120
Watermarked image			
Extracted watermark			
NC	0.9904	0.9906	0.9208

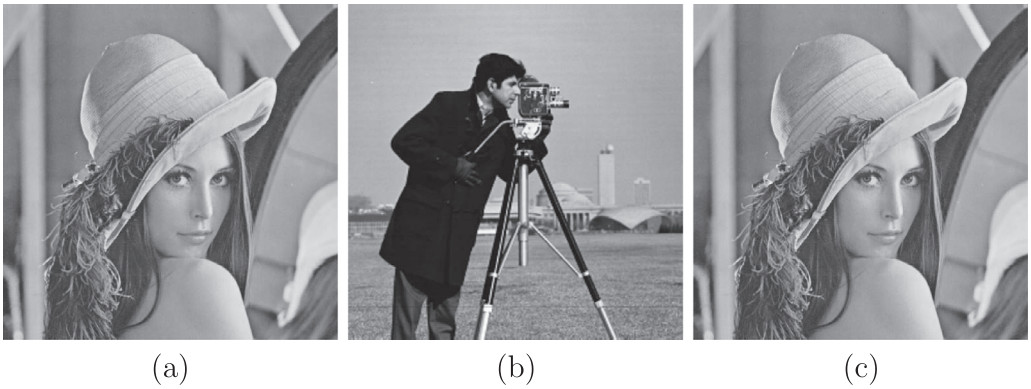


Fig. 5. (a) The Lena host image (512 × 512), (b) The Cameraman watermark image (512 × 512), (c) The Lena watermarked image (512 × 512), WPSNR=45.8523 *dB*, MSSIM=0.9996.

Table 5
The NC results of the noise attacks with different variances and densities.

Density or variance	Salt & pepper noise	Gaussian noise	Speckle noise
0.001	0.9640	0.9567	0.9631
0.005	0.9633	0.9564	0.9721
0.01	0.9622	0.9562	0.9788
0.05	0.9563	0.9504	0.9799
0.1	0.9508	0.9414	0.9711
0.5	0.8675	0.9100	0.8848

the Lena watermarked image and the efficiency of the proposed scheme in embedding the invisible watermark with a high PSNR value.

Table 6
The NC values of the filtering attacks with different block sizes.

Block size	Gaussian filter	Median filter	Wiener filter
3 × 3	0.9932	0.9910	0.9627
5 × 5	0.9932	0.9855	0.9614
7 × 7	0.9932	0.9779	0.9587

5.2. Examination of the robustness requirement

When the host image is watermarked and made public, the adversary tries to remove the watermark using many kinds of attacks. These attacks are in two categories: The image processing attacks and the geometrical attacks.

Table 7
The NC results of wavelet and JPEG compressions and sharpening attacks.

Attack	NC	Attack	NC	Attack	NC
Wavelet comp. $R = 10$	0.9933	JPEG comp. $Q = 90$	0.9933	Sharpening 0.2	0.9933
Wavelet comp. $R = 20$	0.9932	JPEG comp. $Q = 80$	0.9933	Sharpening 0.5	0.9932
Wavelet comp. $R = 40$	0.9928	JPEG comp. $Q = 70$	0.9933	Sharpening 0.8	0.9932
Wavelet comp. $R = 60$	0.9925	JPEG comp. $Q = 50$	0.9932	Sharpening 1.2	0.9932
Wavelet comp. $R = 70$	0.9923	JPEG comp. $Q = 40$	0.9932	Sharpening 1.8	0.9932
Wavelet comp. $R = 80$	0.9920	JPEG comp. $Q = 30$	0.9931	Sharpening 3	0.9931
Wavelet comp. $R = 90$	0.9918	JPEG comp. $Q = 20$	0.9930	Sharpening 5	0.9930
Wavelet comp. $R = 100$	0.9916	JPEG comp. $Q = 10$	0.9926	Sharpening 10	0.9929

Table 8
The NC results of scaling and rotation attacks.

Attack	NC	Attack	NC
Scaling (0.5, 0.5)	0.9879	Rotation 2°	0.9906
Scaling (0.5, 2)	0.9906	Rotation 45°	0.9906
Scaling (0.25, 4)	0.9866	Rotation 70°	0.9906
Scaling (0.125, 8)	0.9751	Rotation 110°	0.9905
Scaling (2, 2)	0.9920	Rotation −2°	0.9934
Scaling (2, 0.5)	0.9893	Rotation −50°	0.9902
Scaling (4, 0.25)	0.9818	Rotation −80°	0.9904
Scaling (8, 0.125)	0.9627	Rotation −110°	0.9904

Noise addition (salt and pepper, Gaussian, speckle), filtering (median, wiener, Gaussian), JPEG compression and sharpening are of image processing attacks which are examined on the scheme. The geometrical attacks including scaling, rotation, cutting, shearing and translation are selected and the robustness of the scheme are considered (Table 4).

Noise addition for images may take place in many operations such as during their acquisitions by sensors or their transmissions. Results of noise addition attacks are listed in Table 5. The results show good resistance of the scheme against these attacks.

The second considered attacks are filtering attacks. The NC values of the extracted watermark with different sizes of the filtering blocks are listed in Table 6 where confirm the resistance of the procedure against these types of attacks with high values of the NC criteria.

Wavelet and JPEG compressions and also sharpening attacks are considered as image processing attacks. In the attack classification, these attacks are included in the checkmark benchmarking attacks. Another attack is sharpening. The sharpness is the contrast between different colors. The NC values of the detected watermark with different compression rates of wavelet and different qualities of JPEG compressions and strengths of the sharpening effect are shown in Table 7 where verify good robustness of the proposed SFLCT-SVD scheme under these three attacks.

The second category of the attacks are geometrical attacks. In the Scaling attack alters the bit values of the image which can weaken the embedded watermark. This attack is considered in Table 8 and the watermarked image is tested under various scaling attacks.

Rotation attack is rotating the watermarked image to a special angle and then rotating back to the original one. The watermarked image is considered under various rotation angles and the computed NC values in Table 8 shows how the scheme is robust under this attack.

Cutting attack also is applied to the watermarked image with different parameters in order to show the resistance of the procedure and the results of the NC values are observed in Table 9 proving the robustness of the scheme against this kind of attack. Finally shearing and translation attacks are used on the watermarked image of SFLCT-SVD scheme. Table 9 shows the NC values of the attacks under different parameters, confirming the robustness of the scheme.

5.3. Security investigation of the scheme

For the security investigation, we examine our scheme against two classes of attacks. First one is copy attack, a checkmark bench-

Table 9
The NC values of cutting, shearing and translation attacks.

Attack	NC	Attack	NC	Attack	NC
Cutting 10 rows	0.9267	Shearing (0.2,0.2)	0.9920	Translation (10,10)	0.9266
Cutting 10 columns	0.9446	Shearing (0.2,0.5)	0.9914	Translation (10,20)	0.8906
Cutting 20 rows	0.8613	Shearing (0.5,0.2)	0.9908	Translation (20,20)	0.8686
Cutting 20 columns	0.8973	Shearing (0.5,0.5)	0.9906	Translation (20,35)	0.8249
Cutting 30 rows	0.8015	Shearing (1, 0.5)	0.9819	Translation (35,40)	0.7891
Cutting 30 columns	0.8542	Shearing (3, 3)	0.9850	Translation (40,40)	0.7823
Cutting 40 columns	0.8138	Shearing (5, 5)	0.9831	Translation (50,50)	0.7468

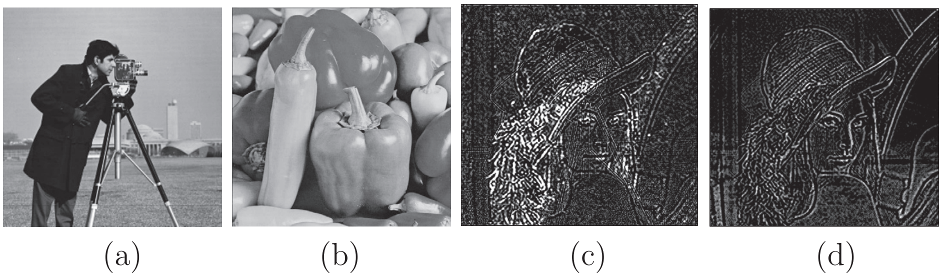


Fig. 6. Robustness against copy attack: (a) Watermark, (b) Unwatermarked image (c) Extracted watermark with median filtering (d) Extracted watermark with wiener filtering.

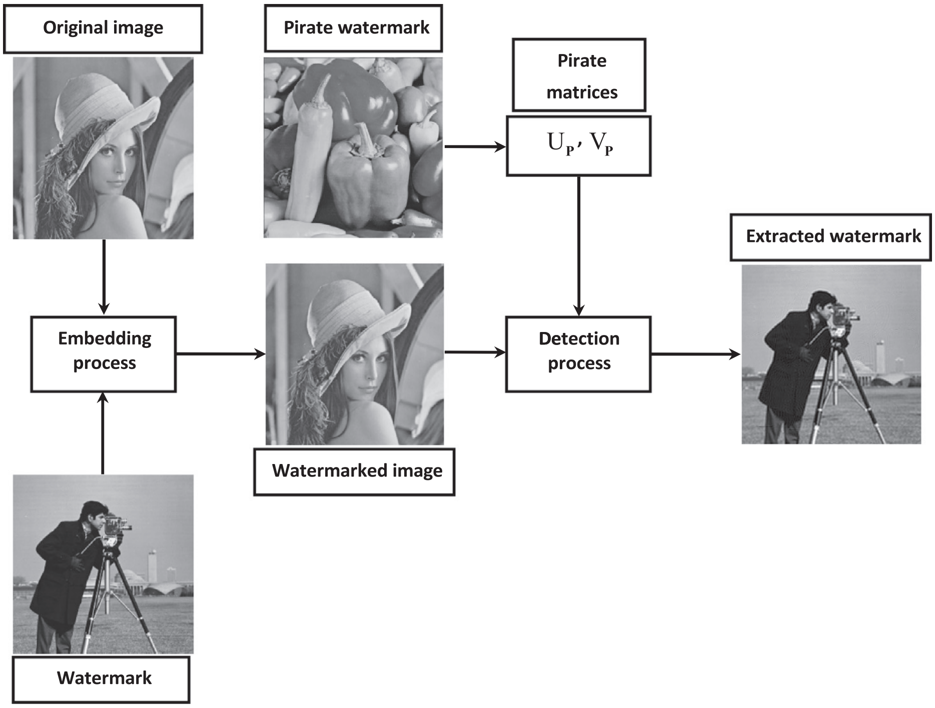


Fig. 7. Block diagram of the first ambiguity attack.

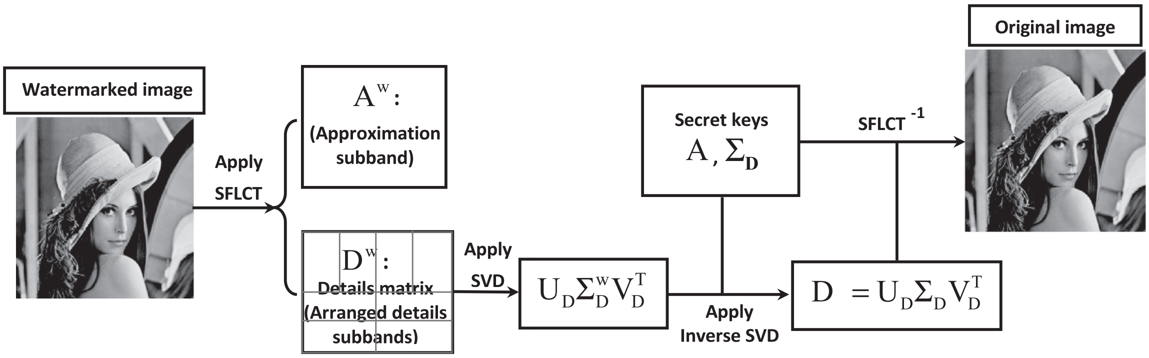


Fig. 8. Undo embedding process.

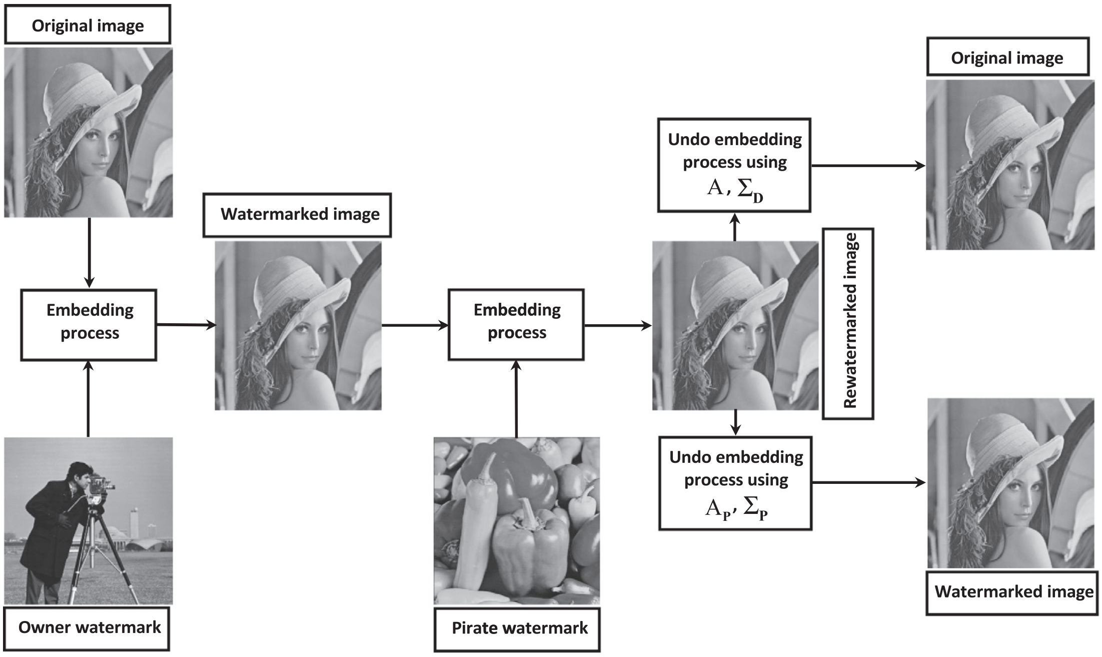


Fig. 9. Block diagram of the second ambiguity attack.

Table 10
The NC comparison of the SFLCT-SVD scheme with the previous schemes.

Type of attack	SFLCT-SVD	SFLCT	Makbol et al. [14]	Lagzian et al. [12]	
	scheme	scheme		LL	HL
Salt & pepper noise $D = 0.001$	0.9640	0.9486	**0.9950**	0.9860	0.6038
Gaussian noise $M = 0, V = 0.005$	0.9564	0.9487	**0.9610**	0.6774	0.6376
Gaussian noise $M = 0, V = 0.3$	**0.9206**	0.8416	0.6190	–	–
Speckle noise $V = 0.4$	**0.8999**	0.8012	0.8200	0.3281	0.6838
Median filtering 3×3	**0.9910**	0.9867	0.9890	0.7218	-0.7912
JPEG compression $Q = 30$	0.9931	0.9169	**0.9980**	-	-
JPEG compression $Q = 40$	0.9932	0.9169	**0.9990**	0.9724	-0.4009
Sharpening $S = 80$	**0.9928**	0.9893	0.9470	–	–
Scaling 0.5	**0.9879**	0.9637	0.9840	–	–
Scaling 2	**0.9920**	0.9638	0.9840	–	–
Rotation $d = 20^\circ$	**0.9905**	0.9640	0.9773	–	–
Rotation $d = 50^\circ$	**0.9904**	0.9642	0.9750	0.5617	−0.8282
Cutting 20	0.8973	0.8527	**0.9840**	−0.8881	0.0087
Histogram equalization	**0.9932**	0.9396	0.9850	0.5670	0.8815

mark attack which is related to the security property. The copy attack is copying a watermark from the watermarked image to a host image [27]. Another one is ambiguity attack. The most important issue with the security property of SVD-based algorithms is its resistance against ambiguity attacks and the false positive problem. In the proposed SFLCT-SVD scheme this problem is solved by directly embedding the approximate subband of the watermark, then increasing the dependency of the watermark to the extracted data without adding extra steps to the watermarking algorithm like authentication mechanism in signature-based solutions or applying operations on the orthogonal matrices U and V for the authentication. Two kinds of ambiguity attacks have been considered in recent works, e.g., [26,33]. In the following, we apply these attacks on the watermarked image by the SFLCT-SVD technique and we show that the scheme is resistant against these kinds of attacks.

5.3.1. *Copy attack*

A copy attacks takes place when an adversary tries to copy watermark from a watermarked image to another. To this aim, the adversary applies a watermark removal attack to a legitimately watermarked image x^w and tries to derive a reasonable approximation of the original image, $\tilde{x}$. For this step, nonlinear noise reduction filters such as wiener or median filters are applied. The next step is estimation of the added watermark pattern by the subtraction $\tilde{w} = x^w - \tilde{x}$ and adding it to the unwatermarked image c to obtain a watermarked version c^w:

$$c^w = c + \tilde{w}.$$

Now, we apply the detection process on the c^w to extract the watermark. The extracted watermarks are shown in Fig. 6 when wiener and median filters are used as noise reduction filters. The results show that our scheme is robust against this scheme.

5.3.2. *First ambiguity attack*

In the first kind of attack, the owner of the image x adds own watermark w according to the embedding process to derive the watermarked image x^w. An attacker constructs pirate matrices U_p and V_p from a pirate watermark w_p and use them in the detection process to extract the faked watermark and create ambiguity about the legitimate owner of the original image. But our scheme is resistant against this attack and in spite of applying pirate matrices U_p and V_p the extracted watermark is w which is shown in Fig. 7. The NC value between w and $\tilde{w}$ is 0.9858. In this test we assumed that the other secret keys (A, Σ_D, α_A and α_D) are known and only the effects of pirate matrices U_p and V_p are considered.

5.3.3. *Second ambiguity attack*

In the second kind of attack, after watermarking the original image x by the owner and creating x^w, the attacker embed the pirate watermark w_p on the watermarked image x^w and makes rewatermarked image x_p^w. Then in the detection process tries to extract the pirate watermark w_p by the faked matrices U_p^w and V_p^w.

In this case, first we define Undo embedding process in which we can derive the original image from the watermarked image using secret keys Σ_D and A. This process is shown in Fig. 8.

Now, as is observed in Fig. 9, if we employ the undo embedding process on the rewatermarked image x_p^w using secret keys Σ_D and A, we derive the original image x with NC value 1, while applying this process with pirate secret keys Σ_p and A_p will give the watermarked image x^w with NC value 1.

6. Comparative analysis of the proposed scheme

In this section the comparison of the SFLCT-SVD procedure with the schemes of Makbol et al. [14], Ansari et al. [36] and Lagzian et al. [12] is considered. In all of the schemes the Lena and Cameraman images are selected as host and watermark images, respectively. The comparison examination is based on the four requirements of the watermarking schemes security, robustness, imperceptibility and capacity. About the security, in our proposed scheme the false positive problem is solved without doing extra work like authentication mechanism in signature-based solutions as in [14] or calculating principle components in [36]. The other method in [12] suffers from the false positive problem as is discussed in [51].

In the robustness requirement, all of the algorithms are investigated under different types of attacks and the results are compared in Tables 10 and 11. Since in the methods presented in [12,14] the watermarking schemes are performed in one of the four subbands

Table 11
The NC comparison of the SFLCT-SVD scheme with Ansari et al. [36].

Type of attack	SFLCT-SVD scheme	Ansari et al. [36]
Gamma correction 0.8	**0.9932**	0.5499
Gaussian noise $M = 0, V = 0.001$	**0.9567**	0.8286
speckle noise $M = 0, V = 0.001$	**0.9631**	0.9516
Wiener filtering 3×3	**0.9627**	0.9355
Median filtering 3×3	**0.9910**	0.8828
Gaussian filtering 3×3	**0.9932**	0.9739
JPEG compression $Q = 50$	**0.9932**	0.9293
Sharpening $S = 0.8$	**0.9932**	0.8991
Scaling 0.5	**0.9879**	0.9548
Scaling 2	**0.9920**	0.9837

Table 12
Security, capacity, imperceptibility and robustness comparison of the proposed scheme with Makbol et al. [14], Ansari et al. [36] and Lagzian et al. [12].

Basis of comparison	Makbol et al. [14]	Ansari et al. [36]	Lagzian et al. [12]	Proposed scheme
Type of transforms	IWD + SVD	DWT + SVD + ABC	RDWT + SVD	SFLCT + SVD
Transforms on watermark	No	DWT + SVD	SVD	SFLCT + SVD
extra steps for security	Yes, Secure	Yes, Secure	No, Insecure	No, Secure
Scheme robustness	⋆⋆⋆	⋆⋆	⋆	⋆⋆⋆⋆
Host image size	512 × 512	512 × 512	512 × 512	512 × 512
Watermark image size	256 × 256	128 × 128	512 × 512	512 × 512
Scheme capacity	⋆⋆	⋆	⋆⋆⋆⋆	⋆⋆⋆⋆
Scheme imperceptibility	⋆⋆⋆	⋆	⋆⋆	⋆⋆⋆⋆

HH, LH, HL and LL, then for each of these schemes the best result of the four subbands is selected to be compared. Accordingly, the LL subband of [14] and HL subbands of [12] are chosen. The negative values mean that the watermark is detected as a negative image and the sign - means that the result is not reported under that attack. In both Tables 8 and 9, high scores are bolded for clarity. From the results the overall superiority of the proposed SFLCT-SVD scheme is observed. Also about the imperceptibility property, our proposed scheme has a high PSNR value with respect to the schemes [12,14,36] as considered in Table 3. Table 12 adds up all comparative results of the schemes according to the similarities, differences and some of the strong points of each scheme. In this table, taking into account all of the properties, the proposed SFLCT-SVD scheme surpasses the other schemes with respect to the high security, capacity, imperceptibility and robustness.

7. Conclusion

In this paper, a combination of the sharp frequency localized contourlet transform (SFLCT) and SVD is used to construct a secure watermarking algorithm. The useful properties of these two transforms lead to enhancing the quality of the proposed watermarking scheme in terms of the watermarking requirements. The different downsampling rates of SFLCT caused to achieve high capacity of the watermarking procedure and using SVD to the details subbands increased the imperceptibility and moreover, the robustness of the scheme is improved against all considered geometrical and image processing attacks. On the other hand, resistance against ambiguity attacks and the false positive problem of the SVD-based schemes are promoted by increasing the dependency of the embedding and detection processes on the watermark and without adding extra implementations like signature-based algorithms. In comparison with the recent techniques, the SFLCT-SVD scheme showed high capacity, imperceptibility and security and its high resistance makes the scheme a good choice for the watermarking area applications such as proof of ownership, data authentication and copyright protection applications. Considering to utilize the proposed scheme on color images due to their layers and modification of applying the SVD on subbands such that optimizes the scheme and the scheme is still remained secure, are of future works that should be considered.

References

[1] Surekha B, et al. Digital image watermarking tools: state-of-the-art Information technology and intelligent transportation systems: proceedings of the second international conference on information technology and intelligent transportation systems, Xi'an, China, vol. 296; 2017.

[2] Singh AK, et al. Medical image watermarking: techniques and applications, book series on multimedia systems and applications. USA: Springer; 2017.

[3] Singh A, Dave M, Mohan A. Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl 2015;75. doi:10.1007/s11042-015-2754-7.

[4] Parah SA, et al. Realization of a new robust and secure watermarking technique using DC coefficient modification in pixel domain and chaotic encryption. J Glob Inf Manag (JGIM) 2017;25(4):80–102.

[5] Dey N, et al. Watermarking in biomedical signal processing. In: Intelligent techniques in signal processing for multimedia security. Cham: Springer; 2017. p. 345–69.

[6] Ben AY, et al. Robust watermarking of polygonal meshes based on vertex norms variance distortion. J Glob Inf Manag (JGIM) 2017;25(4):46–60.

[7] Singh S, Singh R, Singh AK, Siddiqui TJ. SVD-DCT Based medical image watermarking in NSCT domain. In: Quantum computing: an environment for intelligent large scale real application. studies in big data, vol. 33. Springer; 2018. p. 467–88.

[8] Zear A, Singh AK, Kumar P. A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. Multimed Tools Appl 2018;77(4):4863–82.

[9] Premaratne P, Ko C. A novel watermark embedding and detection scheme for images in DFT domain. In: Proceedings of the seventh international conference on image processing and its applications; 1999. p. 780–3.

[10] Poonam, Arora SM. A DWT-SVD based robust digital watermarking for digital images. Procedia Comput Sci 2018;132:1441–8.

[11] Najafi E. A robust embedding and blind extraction of image watermarking based on discrete wavelet transform. Math Sci 2017;11(4):307–18.

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

[13] Makbol NM, Khoo BE. Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. AEU, Int J Electron Commun 2013;67(2):102–12.

[14] Makbol NM, Khoo BE. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. Digit Signal Process 2014;33:134–47.

[15] Kumar C., Singh AK, Kumar P. Improved wavelet-based image watermarking through SPIHT. In: Multimedia tools and applications. Springer; p. 1–14. doi:10.1007/s11042-018-6177-0.

[16] Pandey R, Singh AK, Kumar B, Mohan A. Iris based secure NROI multiple eye image watermarking for teleophthalmology. Multimed Tools Appl 2016;75(22):14381–97.

[17] Chakraborty S, et al. Comparative approach between singular value decomposition and randomized singular value decomposition-based watermarking. In: Intelligent techniques in signal processing for multimedia security. Cham: Springer; 2017. p. 133–49.

[18] Koz A. Digital watermarking based on human visual system, Master's thesis. Dept. of Electrical and Electronics Engineering, Orta Dogu Teknik University; 2002.

[19] Cox I, Miller M, Bloom J, Fridrich J, Kalker T. Digital watermarking and steganography, 2nd ed.. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc.; 2007.

[20] Lin ET, et al. Video and image watermark synchronization Center for education and research in information assurance and security; 2005.

[21] Lee YP, Lee JC, Chen WK, Chang KC, Su IJ, Chang CP. High-payload image hiding with quality recovery using tri-way pixel-value differencing. Inf Sci 2012;191:214–25.

[22] Do MN, Vetterli M. The contourlet transform: an efficient directional multiresolution image representation. IEEE Trans Image Process 2005;14(12):2091–106.

[23] Jahne B. Digital image processing. Berlin Heidelberg: Springer Science & Business Media; 2013.

[24] Lu Y, Do MN. A new contourlet transform with sharp frequency localization. In: Proceedings of the 2006 IEEE international conference on image processing, IEEE. Atlanta, USA; 2006. p. 1629–32.

[25] Abdallah HA, et al. Homomorphic image watermarking with a singular value decomposition algorithm. Inf Process Manag 2014;50(6):909–23.

[26] Craver S, Memon N, Yeo BL, Yeung MM. Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications. IEEE J Sel. Areas Commun 1998;16(4):573–86. May.

[27] Kutter M, Voloshynovskiy S, Herrigel A. The watermark copy attack. In: Security and watermarking of multimedia contents II, Proc. SPIE-3971; 2000. p. 371–80.

[28] Ling HC, Phan RCW, Heng SH. On the security of a hybrid watermarking algorithm based on singular value decomposition and radon transform, AE. Int J Electron Commun 2011;65(11):958–60.

[29] Zhang XP, Li K. Comments on "an SVD-based watermarking scheme for protecting rightful ownership". IEEE Trans Multimed 2005;7(3):593–4.

[30] Loukhaoukha K, Refaey A, Zebbiche K. Comments on homomorphic image watermarking with a singular value decomposition algorithm. Inf Process Manag 2016;52(4):644–5.

[31] Loukhaoukha K, Refaey A, Zebbiche K. Comments on “a robust color image watermarking with singular value decomposition method”. In: Advances in engineering software, vol. 93; 2016. p. 44–6.

[32] Makbol NM, Khoo BE, Rassem TH. Security analyses of false positive problem for the SVD-based hybrid digital image watermarking techniques in the wavelet transform domain. Multimed Tools Appl 2018;77(20):26845–79.

[33] Loukhaoukha K, Refaey A, Zebbiche K, Nabti M. On the security of robust image watermarking algorithm based on discrete wavelet transform, discrete cosine transform and singular value decomposition. Appl Math Inf Sci 2015;9(3):1159–66.

[34] Gokhale U, Joshi Y. A semi fragile watermarking algorithm based on SVD-IWT for image authentication. Int J Adv Res Comput Commun Eng 2012;1(4).

[35] Gupta A, Raval M. A robust and secure watermarking scheme based on singular values replacement. Sadhana 2012;37:425–40.

[36] Ansari IA, Pant M. Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern Recognit Lett. doi:10.1016/j.patrec.2016.12.010.

[37] Ernawan F, Kabir MN. A block-based RDWT-SVD image watermarking method using human visual system characteristics. Vis Comput 2018. doi:10.1007/s00371-018-1567-x.

[38] Voloshynovskiy S., et al. A stochastic approach to content adaptive digital image watermarking. Proceedings of the international workshop on information hiding1999;211–236.

[39] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 2004;13(4):600–12.

[40] Liu W, Zhang H, Tao D, Wang Y, Lu K. Large-scale paralleled sparse principal component analysis. Multimed Tools Appl. 10.1007/s11042-014-2004-4.

[41] Tao H, Chongmin L, Zain JM, Abdalla AN. Robust image watermarking theories and techniques: a review. J Appl Res Technol 2014;12(1):122–38.

[42] Do MN, Vetterli M. Pyramidal directional filter banks and curvelets. In: Proceedings of the 2001 International Conference on Image Processing (Cat. No.01CH37205), Thessaloniki, vol. 3; 2001. p. 158–61.

[43] Datta BN. Numerical linear algebra and applications. Philadelphia: SIAM; 2010.

[44] Ford W. Numerical linear algebra with applications: using MATLAB. Elsevier Science; 2014.

[45] Demmel JW. Applied numerical linear algebra. SIAM: Society for Industrial and Applied Mathematics; 1997.

[46] Pratt WK. Introduction to digital image processing. New York: CRC Press; 2013.

[47] Netravali AN, Haskell BG. Digital pictures: representation, compression and standards, second edition. New York: Springer Science; 1995.

[48] Dey N, Samanta S, Yang XS, Das A, Chaudhuri SS. Optimisation of scaling factors in electrocardiogram signal watermarking using cuckoo search. Int J Bio Inspired Comput 2013;5(5):315–26.

[49] Dey N, Samanta S, Chakraborty S, Das A, Chaudhuri SS, Suri JS. Firefly algorithm for optimization of scaling factors during embedding of manifold medical information: an application in ophthalmology imaging. J Med Imag Health Inform 2014;4(3):384–94.

[50] Cayre F, Fontaine C, Furon T. Watermarking security: theory and practice. IEEE Trans Signal Process 2005;53(10).

[51] Ling HC, Phan RCW, Heng SH. On the security of a robust watermarking scheme based on RDWT-SVD. In: Kim T., et al., editor. Future generation information technology. FGIT 2011. Lecture Notes in Computer Science; vol. 7105. Berlin, Heidelberg: Springer;

Esmaeil Najafi received his Ph.D. degree in Applied Mathematics - Numerical Analysis from Iran University of Science and Technology, Tehran, Iran in 2012, M.Sc. degree in Applied Mathematics from Iran University of Science and Technology, Tehran, Iran in 2008 and B.Sc. degree in Applied Mathematics from Payame Noor University, Tabriz, Iran in 2006. He is currently an assistant professor in Faculty of Science, Department of Mathematics at Urmia University, Urmia, Iran. His research interest is in the area of image processing and image watermarking.

Khaled Loukhaoukha received Doctorate (Ph.D.) degree in electrical engineering from Laval University, Quebec, Canada in 2010, the Electronics Engineer degree and Master’s degree in electrical engineering from Saad Dahlab University, Blida, Algeria in 1999 and 2002, respectively. He has pursuing his Ph.D. degree research project in digital watermarking and image encryption field at the Department of Electrical and Computer Engineering of Laval University. He has pursuing his master’s degree research project in speech coding field at the Division of Architecture and Multimedia Systems of the Center for Development of Advanced Technologies (CDTA), Algiers. He is the author or co-author of more than 20 journal and conference papers. His research interests include information security, digital watermarking, cryptography, image processing, information theory, telecommunication and optimization methods.