A New Robust Digital Image Watermarking Algorithm Based on LWT-SVD and Fractal Images

Kayvan Ghaderi  
Department of Computer Engineering, University of Kurdistan, Sanandaj, Iran  
keyvan.ghaderi@uok.ac.ir

Fardin Akhlaghian Tab*  
Department of Computer Engineering, University of Kurdistan, Sanandaj, Iran  
f.akhlaghian@uok.ac.ir

Parham Moradi  
Department of Computer Engineering, University of Kurdistan, Sanandaj, Iran  
p.moradi@uok.ac.ir

Received: 30/Jun/2014 Revised: 04/Sep/2014 Accepted: 07/Oct/2014

Abstract
This paper presents a robust copyright protection scheme based on Lifting Wavelet Transform (LWT) and Singular Value Decomposition (SVD). We have used fractal decoding to make a very compact representation of watermark image. The fractal code is presented by a binary image. In the embedding phase of watermarking scheme, at first, we perform decomposing of the host image with 2D-LWT transform, then SVD is applied to sub-bands of the transformed image, and then the watermark, “binary image,” is embedded by modifying the singular values. In the watermark extraction phase, after the reverse steps are applied, the embedded binary image and consequently the fractal code are extracted from the watermarked image. The original watermark image is rendered by running the code. To verify the validity of the proposed watermarking scheme, several experiments are carried out and the results are compared with the results of the other algorithms. In order to evaluate the quality of image, we use parameter peak value signal-to-noise ratio (PSNR). To measure the robustness of the proposed algorithm, the NC coefficient is evaluated. The experimental results indicate that, in addition to high transparency, the proposed scheme is strong enough to resist various signal processing operations, such as average filter, median filter, Jpeg compression, contrast adjustment, cropping, histogram equalization, rotation, etc.

Keywords: Image Watermarking; Lifting Wavelet Transforms; Singular Value Decomposition; Fractal Image.

1. Introduction

During the last decade, the availability of information in digital form has increased rapidly. The success of the Internet and cost-effective recording and storage devices have made it possible to easily create, replicate, transmit, and distribute digital content. However, the information security, authentication of data and protection of intellectual property rights have also become an important issue. In such a scenario, a mechanism for copyright protection of multimedia data is essential. Digital watermarking is a process that embeds ownership protection data, named watermark, into the host data. The embedded data could be a signature image, an audio or textual data. This process is highly necessary to protect digital data against unauthorized use [1, 2].

Basically, a set of requirements is evaluated for a watermarking scheme to be effective. These requirements can be categorized as follows: (1) imperceptibility, (2) robustness, (3) capacity [3].

According to operation domain, digital watermarking can be divided into two categories: spatial domain and transform domain. Early image watermarking schemes operated directly in spatial domain, which was mostly associated with poor robustness properties [4]. In contrast, watermarking in the transform domain such as discrete cosine transform (DCT), wavelet transforms (WT) and singular value decomposition (SVD) provide more advantages, and better performances will be obtained compared to those of spatial ones in most of recent research [5-8].

The watermark-extraction techniques can also be classified into non-blind, semi-blind, and blind categories. Non-blind methods need the original signal, which limits their usage since the original media are difficult to obtain sometimes. In semi-blind methods some features of the original signal are needed to be known a priori. Finally, in blind methods, there is no need for the original signal or the watermark in the watermark extraction phase [9-11].

The main motivation of this work is to provide a robust digital image watermarking.

To achieve higher imperceptibility and robustness in the watermarking algorithm, the main idea of this work is based on compact representation of watermark image using fractal encoding. In this way, watermark image is selected from the set of fractal images. In the watermark embedding stage, instead of storing the raw data of the
original watermark image, we embed a binary image which shows the constructor code of the fractal image. In the extraction phase, the binary image is extracted from the host image. Consequently, from this retrieved binary image, the constructor fractal code is also simply extracted. Perhaps the impression is created that when we choose the watermark from the set of fractal images, a limitation is imposed on this algorithm. However, considering the philosophy and application of watermarking algorithms, it is clear that regardless of the watermark image type, the algorithm can achieve its goals such as copyright protection or proving of ownership. Therefore it can be said that selection of fractal images as watermark is not a fundamental limitation and, in favor of its significant improvement, can be entirely disregarded.

In the embedding and extraction phases of the proposed algorithms, LWT and SVD transforms are used. The host image is decomposed by K-level LWT transform, and then the binary image is inserted in the singular values of the $K_0$ level of the decomposed host image. In the extraction phase, after reverse steps of the embedding stage, the inserted values (binary image) can be caught up from the watermarked image. The fractal code is normally a text, typed with a keyboard with regular fonts. This text file is then turned to a binary image for watermarking application. Therefore the embedded code can be obtained from the extracted watermark image easily by a user, or automatically by a simple OCR system. Although both methods are acceptable, however considering the focus of this paper on watermarking algorithm, we extract the fractal code by a user. Rendering the fractal code will produce the final watermark image.

The proposed algorithm achieves higher robustness and improved fidelity, which is one of the important challenges of the watermarking schemes. Since the singular values of the original image are required for extracting the watermark, the introduced algorithm is semi-blind.

The proposed watermarking algorithm is tested against different attacks such as average filter, rotation, cropping, Jpeg compression, etc. The experimental results indicate more robustness against different attacks compared to other algorithms, while significant improvement in PSNR value is also achieved.

The rest of the paper is structured as follows. In Section 2, LWT and SVD transforms are briefly described. The proposed algorithm is discussed in Section 3. The experimental results to demonstrate the performance of this scheme are described in Section 4 and finally the conclusion is drawn in Section 5.

2. Preliminaries of LWT and SVD Transforms

In this section, LWT and SVD transforms are briefly described.

2-1- Lifting wavelet transform

Let $I(m,n)$ be a 2D signal. Without loss of generality, we assume that this signal is first performed with 1D wavelet transform on the vertical direction and then on the horizontal direction. With the basic principle of lifting structure given in [12], each 1D wavelet transform can be factored into one or multiple lifting stages. A typical lifting stage consists of three steps: split, predict and update.

In the first step, all samples are split into two parts: the even poly-phase samples and the odd poly-phase samples,

$$\begin{align*}
    I_{e}(m,n) &= I(2m,2n) \\
    I_{o}(m,n) &= I(2m,2n+1)
\end{align*}$$

(1)

In the predict step, the odd poly-phase samples are predicted from the neighboring even poly-phase samples. In the conventional lifting, the predictions always come from the vertical neighboring even poly-phase samples.

LWT which is the second generation fast wavelet transform is a substitute method for DWT to transform images into the transform domain for real time applications. In lifting wavelet transformation, up sampling and down sampling are replaced simply by split and merge in each of the levels. Split and merge process in LWT reduces computational complexity to 50%. Information loss is less as compared to DWT algorithm, because in LWT based algorithm up sampling and down sampling have not been used. The odd poly-phase and even poly-phase components of the signal are filtered in a specific parallel process by using the corresponding wavelet filter coefficients, producing the better result compared to up sampling and down sampling which is required in the traditional DWT approach. In comparison with general wavelets, reconstruction of images by lifting wavelet is a good idea because it increases smoothness and reduces aliasing effects [13]. Employing LWT reduces information loss, increases intactness of embedded watermark in the image and helps to increase the robustness of watermark. Lifting wavelet transform also provides several advantages [14, 15] such as less memory requirements, reduced distortion and aliasing effects, good reconstruction, less computation and computational complexities. In this decomposition, filter coefficients are converted into lifting coefficients (predict $s(z)$, update $t(z)$ and scaling $k$) using Euclidian algorithm, and the original image is split into (odd and even) sets of samples. Further lifting coefficients are applied to the sampled original image to get approximate and detailed sub bands (Fig. 1).
Let $A$ be a general real (complex) matrix of order $m \times n$. The singular value decomposition is the following factorization:

$$TAU = SV^T$$

where $U$ and $V$ are orthogonal (unitary) and $S$ are the singular values of the matrix $A$ with $r = \min (m, n)$ and satisfying:

$$\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r$$

Use of SVD in digital image processing has some advantages which are listed as follows:

1. The size of the matrices from SVD transformation should not necessarily square and can be a rectangle.
2. Singular values in a digital image are less affected if general image processing is performed. It means that for a small perturbation added to an image, its SVs do not change fast.
3. Singular values contain intrinsic algebraic image properties, where singular values correspond to the brightness of the image and singular vectors reflect geometry characteristics of the image. [16-18].

SVD can effectively reveal essential properties of image matrices, so it has been used in a variety of image processing applications such as noise estimation and digital watermarking [19-21].

### 3. Proposed Watermarking Scheme

This section is divided into three parts as follows: (1) watermark generating, (2) embedding stage and (3) extraction stage.

#### 3-1- Watermark generation using fractal images

At first, considering properties of fractal images, the mathematical equation and then the related fractal based code for producing the selected watermark image is determined. Thus, instead of using the original watermark image, a small binary image which shows the fractal code of the watermark image is used in the watermarking scheme. This stage is shown in TABLE 1. Next, the binary image is called as the substitute watermark image. As can be seen in the aforementioned table, the code section is divided to two parts: Constant and Main. The Constant part is used in the rendered original watermark stage as a key extraction. Also, the Main part is used after converting to a binary image, as the substitute for the original watermark.

In this way, since the volume of inserted information in the host image is much less than the original watermark, and also due to function of the fractal code in producing the original watermark image, watermarking criteria such as transparency and robustness are very well satisfied.

#### 3-2- Embedding stage

The watermark embedding procedure has been represented in Fig. 2, followed by a detailed explanation:

1. Perform $k^1$-level 2D-LWT on the host image to provide multi-resolution sub bands: $LL_k$, $LH_k$, $HL_k$, and $HH_k$.
2. Apply SVD transform to sub bands: $LH_1$, $LH_2$, ..., $LH_k$, and $HH_k$ to get $U$, $V$ and $S$ matrices at each sub band.

$$I = U_i \times S_i \times V_i^T \quad i = 1, 2, \ldots, k$$

3. Modify the singular values of the host image in $LH_i$ and $HL_i$ sub-bands according to those of the watermark.

$$S_{\text{modified}} = S + (\alpha \times \text{watermark})$$

Where $\alpha$ represents the scaling factor.

4. Perform inverse SVD with updated $S$ matrix.
5. Apply $K$-level 2D-ILWT to obtain watermarked image.

---

1 In the proposed algorithm, selection of the number of 2D-DWT level depends on parameters such as size of the host and watermark images, number of sub bands, etc.
Table 1. Watermark construction process.

<table>
<thead>
<tr>
<th>Code</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>z=log(2)*0.0185; a=0; b=0; c=15000; curx=zeros(1,c); cury=zeros(1,c); xn=0; yn=0;</td>
<td>Constant As a reconstruction key</td>
</tr>
<tr>
<td>For k=1:c a=mod(a+2<em>pi</em>z,2<em>pi); b=mod(b,2</em>pi)+a; [x,y]=pol2cart(b,1); xn=x+xn; yn=y+yn; curx(k)=xn; cury(k)=yn; end</td>
<td>Original watermark Size=1024×1024</td>
</tr>
<tr>
<td>Converted code to image as a substitute watermark Size=128×128</td>
<td></td>
</tr>
</tbody>
</table>

3-3- Extraction stage

Our aim in watermark extraction is to obtain embedded substitute watermark. To reconstruct the original watermark image, in the first step, this fractal code and reconstruction key are combined together, so this new code is run. The extraction procedure is explained as follows.

1. Perform K-level 2D-ILWT on the watermarked image to provide multi-resolution sub bands: LL_k, LH_k, HL_k and HH_k.
2. Apply SVD transform to sub bands LH_k, HL_k, ..., LH_k and HL_k to get U, V and S matrices.
3. Extract watermark from S matrices by the following equation:

\[ \text{watermark} = (D' - S) / \alpha \]

4. Experimental Results

In simulation, we use the images "Lena" and "Pepper" whose size is 512 × 512 pixels as the original image and the embedded binary image, which shows the fractal code, with size 128 × 128 Pixels as the substitute watermark image. In Fig. 3 these images are shown. Considering the size of images, the number of decomposition levels (named k) in these experiments is set to 4.

In order to evaluate the transparency of watermarked image, we use the criterion peak value signal-to-noise ratio (PSNR). PSNR is used as an efficient measure of visual fidelity between the host image and the watermarked image. The PSNR in decibels is given by the following equation:

\[ \text{PSNR} = 10\log_{10}\left(\frac{225^2}{MSE}\right) \] (9)

where

\[ \text{MSE} = \frac{1}{N_1 \times N_2} \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} \left( I(i,j) - I'(i,j) \right)^2 \] (10)

Where N_1×N_2 is the size of image, I and I' are the pixel gray values of the host image and the watermarked image respectively. Since the higher value of PSNR presents better transparency, it is desired.

The similarity (evaluate the robustness) between W (the original watermark) and W* (the extracted watermark) can be measured by means of normalized correlation. The normalized correlation is defined as:

\[ \text{Correlation} = \frac{\sum_{i=1}^{N_1} \sum_{j=1}^{N_2} [I(i,j) - \bar{I}] [I'(i,j) - \bar{I}]}{\sqrt{\sum_{i=1}^{N_1} \sum_{j=1}^{N_2} [I(i,j) - \bar{I}]^2 \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} [I'(i,j) - \bar{I}]^2}} \]
where \( \bar{W} = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} W_{ij} \) and 
\( \bar{W}^* = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} W_{ij}^* \)

![Image](image1.png)

### Fig. 3. (a) Original image and (b) Substitute watermark image.

Fig. 4 shows the watermarked image and the extracted binary watermark image without any attacks. The PSNR between embedded watermark image and original image is 71.382 db. The value of \( \alpha \) in this paper for trade-off between transparency and robustness is set to 0.07. Fig. 5 shows a relation between \( \alpha \) and transparency in terms of the PSNR value. In this table the abbreviation W.F means Fractal watermark.

In order to evaluate the robustness of watermarking algorithm, the watermarked image is attacked by several types of attacks and then correlation coefficients between original watermark \( w \) and detected watermark \( w' \) is calculated (TABLE 2). In Figures 6 to 14, the sub images (a, b) show the attacked watermarked image with several attacks in common image processing. Similarly, in sub images (c, d) the extracted substitute watermark images, when the watermarked images are attacked with the image manipulation, are shown.

**Table 2. Correlation coefficients**

<table>
<thead>
<tr>
<th>Attack</th>
<th>Correlation Coefficients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host image: Pepper</td>
<td>0.9802</td>
</tr>
<tr>
<td>Host image: Lena</td>
<td>0.9982</td>
</tr>
<tr>
<td>No</td>
<td>0.9996</td>
</tr>
<tr>
<td>Average Filter 9×9</td>
<td>0.9802</td>
</tr>
<tr>
<td>Median Filter 9×9</td>
<td>0.9770</td>
</tr>
<tr>
<td>Histogram Equalization</td>
<td>0.9614</td>
</tr>
<tr>
<td>Gaussian Noise 50%</td>
<td>0.9632</td>
</tr>
<tr>
<td>Contrast Adjustment</td>
<td>0.9831</td>
</tr>
<tr>
<td>Cropping 50%</td>
<td>0.9810</td>
</tr>
<tr>
<td>Jpeg Compression with QF=20</td>
<td>0.8726</td>
</tr>
<tr>
<td>Resizing (100% → 25%)</td>
<td>0.9616</td>
</tr>
<tr>
<td>Rotation 90°</td>
<td>0.9840</td>
</tr>
</tbody>
</table>

![Image](image2.png)

**Fig. 4. (a) Watermarked image, (b) The extracted substitute watermark image and (c) Rendered original watermark.**

**Fig. 5. Relationship between \( \alpha \) and PSNR.**
Fig. 6. (a), (b) Attacked watermarked images by Average filter 9x9; (c), (d) Extracted watermark images.

Fig. 7. (a), (b) Attacked watermarked images by Median filter 9x9; (c), (d) Extracted watermark images.

Fig. 8. Attacked watermarked images by Histogram equalization; (c), (d) Extracted watermark images.

Fig. 9. (a), (b) Attacked watermarked images by Gaussian noise 50%; (c), (d) Extracted watermark images.
Fig. 10. (a), (b) Attacked watermarked images by Contrast Adjustment; (c), (d) Extracted watermark images.

Fig. 11. (a), (b) Attacked watermarked images by Cropping; (c), (d) Extracted watermark images.

Fig. 12. (a), (b) Attacked watermarked images by Jpeg Compression with QF=20; (c), (d) Extracted watermark images.

Fig. 13. (a), (b) Attacked watermarked images by Resizing (100% to 25%); (c), (d) Extracted watermark images.
4.1 - Comparison

In this subsection, the results of performing the proposed and the other four watermarking algorithms are compared. The host image is Lena and the Robustness and transparency are the criteria for comparison.

Table 3 shows the result of the comparison between the correlation coefficient of the proposed method and four other recently published papers1 ([22]-[25]).

For the sake of comparison these algorithms are implemented in the same conditions. In this table the last row shows the average amount of correlation coefficients for the applied attacks.

Table 4 shows the result of the PSNR comparison between the mentioned methods. There is no difference between these methods from the image quality aspect. Scaling factor for this comparison is 0.1. The results indicate both higher PSNR values and more robustness for the proposed algorithm than the other compared algorithms. This is in spite of the limitation of the images which can be produced by the fractal images.

In table 5, the blindness of the proposed algorithm with references no. [22-25], has been compared. In this table the non-watermarked parameters/data needed to reconstruct the watermark image moreover the extracted information from the host image has been briefly explained. As the table shows, except the work of Yang et al. [25], the blindness property of proposed algorithm is better or analogous to the other compared works in the table.

Table 3. Correlation coefficients comparison.

<table>
<thead>
<tr>
<th>Attack</th>
<th>Proposed</th>
<th>[22]</th>
<th>[23]</th>
<th>[25]</th>
<th>[24]</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>0.9998</td>
<td>0.9980</td>
<td>0.9995</td>
<td>0.9990</td>
<td>0.9724</td>
</tr>
<tr>
<td>Average Filter</td>
<td>0.9802</td>
<td>0.9010</td>
<td>0.8990</td>
<td>0.9060</td>
<td>0.8100</td>
</tr>
<tr>
<td>Un-sharpening</td>
<td>0.9600</td>
<td>0.9610</td>
<td>0.9100</td>
<td>0.8560</td>
<td>0.9100</td>
</tr>
<tr>
<td>Histogram Equalization</td>
<td>0.9684</td>
<td>0.9862</td>
<td>0.9000</td>
<td>0.9635</td>
<td>0.9890</td>
</tr>
<tr>
<td>Gaussian Noise</td>
<td>0.9399</td>
<td>0.9575</td>
<td>0.8560</td>
<td>0.9460</td>
<td>0.6800</td>
</tr>
<tr>
<td>Contrast Adjustment</td>
<td>0.9754</td>
<td>0.9900</td>
<td>0.9450</td>
<td>0.9000</td>
<td>0.7800</td>
</tr>
<tr>
<td>Gama Correction</td>
<td>0.9693</td>
<td>0.9296</td>
<td>0.9301</td>
<td>0.9554</td>
<td>0.9100</td>
</tr>
<tr>
<td>Jpeg Compression</td>
<td>0.9567</td>
<td>0.9658</td>
<td>0.9010</td>
<td>0.9541</td>
<td>0.9700</td>
</tr>
<tr>
<td>with QF=75</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resizing</td>
<td>0.9839</td>
<td>0.9700</td>
<td>0.9600</td>
<td>0.8628</td>
<td>0.8500</td>
</tr>
<tr>
<td>Average</td>
<td>0.9716</td>
<td>0.9621</td>
<td>0.9223</td>
<td>0.9269</td>
<td>0.8736</td>
</tr>
</tbody>
</table>

Table 4. PSNR for several watermarking schemes on Lena host image.

<table>
<thead>
<tr>
<th>Method</th>
<th>PSNR with α=0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yang et al.[25]</td>
<td>40.1891 db</td>
</tr>
<tr>
<td>L&amp;T [22]</td>
<td>46.02 db</td>
</tr>
<tr>
<td>Tk&amp;L [23]</td>
<td>24 db</td>
</tr>
<tr>
<td>Proposed Method</td>
<td>70.515 db</td>
</tr>
</tbody>
</table>

Table 5. Comparing the blindness of different schemes

<table>
<thead>
<tr>
<th>Watermarking Algorithm</th>
<th>Data used in Extraction Watermark Step</th>
<th>Non-Blind, Semi-Blind or Blind</th>
</tr>
</thead>
<tbody>
<tr>
<td>[22]</td>
<td>S matrix after applying SVD transforms to host image.</td>
<td>Semi-Blind or Blind</td>
</tr>
<tr>
<td>[23]</td>
<td>Using SVR Training</td>
<td>Not Fully Blind (Similar to Semi-Blind)</td>
</tr>
<tr>
<td>[24]</td>
<td>Used host image (B, Sub-bands in embedding stage) and watermark image</td>
<td>Non-Blind</td>
</tr>
<tr>
<td>[25]</td>
<td>Neither needs the original host image nor any other side information.</td>
<td>Blind</td>
</tr>
<tr>
<td>Proposed</td>
<td>S matrix after applying SVD transforms to host image.</td>
<td>Semi-Blind</td>
</tr>
</tbody>
</table>

5. Conclusion

In this paper, a hybrid image watermarking technique based on LWT and SVD has been presented, where the watermark is embedded on the singular values of the cover image’s LWT sub-bands (LH and HL). In this work, original watermark is fractal image that converts to its constructor codes. In this way, instead of the original watermark for embedding, we used fractal coding that is much smaller than original watermark. Our algorithm is robust against various attacks including average filter, median filter, contrast adjustment, Jpeg compression, rotation, scaling, resizing and cropping. Experimental results of the proposed technique have shown both the significant improvement in imperceptibility and the robustness under attacks.

---

1 Although there are many published watermarking algorithms in the literature, regarding the robustness and transparency criteria, these two algorithms are better than or at the same level with other algorithms. Therefore comparison with these two algorithms is reasonable and enough to show the priority of the proposed algorithm.
References


Kayvan Ghaderi received his M.Sc. in artificial intelligence from the Faculty of Computer Engineering, University of Kurdistan, Sanandaj, Iran in 2013. His current research areas of interest include digital watermarking, data hiding, image enhancement, multimedia communications and fuzzy systems.

Fardin Akhlaghian Tab was born in Sanandaj, Iran in 1965. He received his bachelor's degree in Electronic Engineering from Isfahan University of Technology in 1989 and his M.Sc. Degree in Telecommunications and Signal Processing from Tehran University of Tarbiat Modarres in 1992. From 1993 until 2000 he was a scientific member of Computer Engineering Department at University of Kurdistan, Sanandaj, Iran. From 2001 until 2006 he studied for his Ph.D. degree at University of Wollongong, Australia and then after receiving the Ph.D. degree in 2005, he again joined the Department of Computer Engineering and Information Technology at University of Kurdistan. His major research interests are pattern recognition, image processing and computer vision.

Parham Moradi received his Ph.D. degree in Computer Science from Amirkabir University of Technology in March 2011. Moreover, he received M.Sc. and B.Sc. degrees in Software Engineering and Computer Science from Amirkabir University of Technology, Tehran, Iran, in 1998 and 2005 respectively. He conducted a part of his Ph.D. research work in the Laboratory of Nonlinear Systems, EPFL (Ecole Polytechnique Federale de Lausanne), Lausanne, Switzerland, form September 2009 to March 2010. Currently he is working as an Assistant Professor in the Department of Computer Engineering and Information Technology, University of Kurdistan, Sanandaj, Iran. His current research areas include Reinforcement Learning, Graph Clustering, Social Network Analysis, Data Mining and Recommender Systems.