A new robust reference watermarking scheme based on DWT-SVD

Gaurav Bhatnagar *, Balasubramanian Raman 1

Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee – 247667, India

ARTICLE INFO

Article history:
Received 27 March 2008
Received in revised form 9 September 2008
Accepted 28 September 2008
Available online 18 November 2008

Keywords:
Reference watermarking
Wavelet transform
Directive contrast
Singular value decomposition
Ambiguity

ABSTRACT

This paper presents a new semi-blind reference watermarking scheme based on discrete wavelet transform (DWT) and singular value decomposition (SVD) for copyright protection and authenticity. We are using a gray scale logo image as watermark instead of randomly generated Gaussian noise type watermark. For watermark embedding, the original image is transformed into wavelet domain and a reference sub-image is formed using directive contrast and wavelet coefficients. We embed watermark into reference image by modifying the singular values of reference image using the singular values of the watermark. A reliable watermark extraction scheme is developed for the extraction of watermark from distorted image. Experimental evaluation demonstrates that the proposed scheme is able to withstand a variety of attacks. We show that the proposed scheme also stands with the ambiguity attack also.

© 2008 Elsevier B.V. All rights reserved.

1. Introduction

Illegal copying, modifying, tampering and copyright protection have become very important issues with the rapid use of internet. Hence, there is a strong need of developing the techniques to face all these problems. Digital watermarking [1] emerged as a solution for protecting the multimedia data. Digital Watermarking is the process of hiding or embedding an imperceptible signal (data) into the given signal (data). This imperceptible signal (data) is called watermark or metadata and the given signal (data) is called cover work. The watermark should be embedded into the cover work, so that it should be robust enough to survive not only the most common signal distortions, but also distortions caused by malicious attacks. This cover work can be an image, audio or a video file. A watermarking algorithm consists of two algorithms, an embedding and an extraction (or detection) algorithm.

Watermarking techniques can be broadly classified into two categories: Spatial and Transform domain methods. Spatial domain methods [2,3] are less complex and not robust against various attacks as no transform is used in them. Transform domain methods [4–6] are robust as compared to spatial domain methods. This is due to the fact that when image is inverse transformed, watermark is distributed irregularly over the image, making the attacker difficult to read or modify. Due to the fact of localization in both spatial and frequency domain, wavelet transform is the most preferable transform among all other transforms.

Barni et al. [7] proposed a wavelet domain based method which exploits the characteristics of human visual system (HVS). Based on the texture and the luminance content of all image sub-bands, a mask is accomplished pixel by pixel. Dawei et al. [8] proposed a new type of technique in which the authors used the wavelet transform applied locally, based on the chaotic logistic map. This technique shows very good robustness to geometric attacks but it is sensitive to common attacks like filtering and sharpening.

Kundur et al. [4] proposed the use of gray scale logos as watermark. They addressed a multiresolution fusion based watermarking method for embedding gray scale logos into wavelet transformed images. The logo undergoes 1-level decomposition for watermarking. Each sub-band of the host image is divided into block of size equal to the size of sub-band of the logo. Four sub-bands of the logo corresponding to different orientations are added to the blocks of the same orientation.

For fusion, the watermark is scaled by a salience factor computed on a block by block basis.

Reddy et al. [9] proposed a method in which the authors used a gray scale logo as watermark. To embed watermark, HVS characteristics were used to select the significant coefficients and watermark is added to these selected coefficients. Further, they used the model of Barni et al. [7] to calculate the weight factors for wavelet coefficients of the host image. They extracted watermark from the distorted image by taking into consideration the distortion caused by the attacks.

In the recent years, singular value decomposition (SVD) is used as a new transform for watermarking. The SVD based watermarking algorithm is introduced by Liu et al. [10]. In this algorithm, the authors found the singular values of the host image and then modified them by adding the watermark. SVD transform was again applied on the resultant matrix for finding the modified singular values. These singular values were combined with the known component to get the watermarked image. For watermark extraction inverse process is used.

Ganic et al. [11] proposed the watermarking scheme in which
the authors found the wavelet transform of the host image and then applied SVD transform on all detail, approximation part and watermark image. In order to find the modified singular values they sum up the singular values of watermark and sub parts of the image.

Li et al. [12] proposed a hybrid DWT-SVD domain watermarking scheme considering human visual system properties. After decomposing the host image into four sub-bands, they applied SVD to each sub-band and embedded singular values of the watermark into the sub-bands. The embedding strength is determined by a human visual model. Chang et al. [13] used D and U components for embedding the watermark. Chandra et al. [14] described a method by embedding singular values of the watermark to the singular values of entire image. First, singular values of the host and watermark images are computed, then the singular values of the watermark image are magnified and added to those of the host image.

In this paper, a new reference watermarking technique is presented. First, we transform the host image into wavelet domain and then a sub-band at the coarsest level is selected. Suppose \( l \) be the coarsest level then either approximation or any detail or all sub-bands are selected. First 1-level DWT is applied on the selected sub-band. Then we find out the directive contrast for each detail. Based on this directive contrast, we put all wavelet coefficients (in all detail sub-bands) to zero which have directive contrast less than a given threshold. Threshold is different for each detail sub-bands and inverse 1-level DWT is performed to get the reference image. Watermark is embedded in the reference image by modifying its singular values. An efficient watermarking extraction algorithm is introduced to find the watermark estimate.

This paper is organized as follows: In Section 2, an introduction for existing reference watermarking schemes are given. In Sections 3 and 4, we introduce singular value decomposition and directive contrast. Our proposed watermarking embedding scheme and the extraction scheme are described in detail in Section 5. Section 6 discusses the results obtained using the proposed watermarking scheme and finally in Section 7, the concluding remarks are given.

2. Existing reference watermarking schemes

There are two reference watermarking schemes in literature. Joo et al. [15] introduced robust reference watermarking scheme in which they have embedded watermarking into low frequency (Fig. 1). For this purpose, host image is decomposed by the means of DWT. Suppose the coarsest level of decomposition is \( n \), then \( LL_n \) is selected and again 1-level DWT is applied on it. Hence the sequence of sub-bands \( LL_{n+1}, LH_{n+1}, HL_{n+1}, HH_{n+1} \) are obtained. Then the reference image \( LL_n' \) is formed by taking inverse wavelet transform after initializing high frequency sub-bands to zero.

The watermark used by the authors is a binary watermark sequence, \( w(i) \in \{-1, +1\} \). The \( LL_n \) values are replaced with \( LL_n' \pm K \times w(i) \) where \( K \) is a factor to control the embedding intensity. To maintain the visual quality of the image, watermark is embedded into the locations where the difference between \( LL_n \) and \( LL_n' \) is smaller. The embedding process is repeated because the changes in \( LL_n \) values also cause some changes in leading \( LL_n' \) values. The main draw back of this scheme is that, as the embedding process is repeated, the PSNR is decreased but the reliability is increased. The embedding algorithm is given below:

```plaintext
for i=1:wm_length
    if (w(i)==1)
        if (LL_n(idx(i))<LL_n'(idx(i))+K)
            LL_n(idx(i))=LL_n'(idx(i))+K
        end
    else if (w(i)==-1)
        if (LL_n(idx(i))<LL_n'(idx(i))-K)
            LL_n(idx(i))=LL_n'(idx(i))-K
        end
    end
end
```

Fig. 1. Block diagram of Joo reference watermarking scheme.
Original image is required to extract the watermark. First, same wavelet decomposition is applied on both the original and watermarked images. Then, the next step is to find the embedding locations since $LL_n$ and $LL'_n$ are known. Finally, based on comparison between $LL_n$ and $LL'_n$, watermark bits have been extracted.

Another reference watermarking scheme is given by Liu et al. [16] in which the authors have modified Joo’s scheme. First, original image is transformed into frequency domain by taking 1-level wavelet decomposition. Then, all high frequency sub-bands are initialized to zero and inverse wavelet transform is performed to construct the reference image. It is assumed that $X$, $X'$ and $X_w$ denote the original, reference and watermark images respectively. The difference between original and reference image is computed and the location $idx(i,j)$ is obtained such that $s|\sigma f^i(i,j)-\sigma f'(i,j)|<t$, where $s, t \in \mathbb{Z}^+$. Based on $idx$ watermark is embedded as depicted in Fig. 2.

Fig. 2. Block diagram of Liu et al.’s reference watermarking scheme.

Fig. 3. Proposed reference watermarking scheme.
The value of $x_w(idx)$ is defined by

$$x_w(idx(i,j)) = \begin{cases} 
    x'(idx(i,j)) + \alpha & \text{if } w(k) = 1 \& s < x'(idx(i,j)) - x(idx(i,j)) < t \\
    x'(idx(i,j)) - \alpha & \text{if } w(k) = 1 \& s > x'(idx(i,j)) - x(idx(i,j)) < t
\end{cases}$$

(1)

where $\alpha = \text{round}[(s + t)/2]$. To extract the watermark, first watermarked image is transformed by 1-level DWT. The high frequencies are set to zero and the inverse wavelet transform is performed to obtain its reference image (denoted by $X'_w$) and watermark bits are extracted as

$$w'(k) = \begin{cases} 
    1 & \text{if } x_w(idx(i,j)) \geq X'_w(idx(i,j)) \\
    -1 & \text{if } x_w(idx(i,j)) < X'_w(idx(i,j))
\end{cases}$$

(2)

3. Singular value decomposition

Every real (or complex) $m \times n$ matrix $A$ can be decomposed into two orthogonal (or Unitary) matrices $U$ and $V$ and a diagonal matrix $S$. 

Fig. 4. a) Original Test Images b) Watermarked Test Images.
The entries in this diagonal matrix are called the singular values of the matrix $A$. This decomposition is called Singular Value Decomposition of $A$ and can be expressed as

$$ A = USV' $$

where $r$ is the rank of the matrix $A$ and hence $r = \min(m, n)$. The first $r$ columns of $V$ are the right singular vectors and the first $r$ columns of $U$ are the left singular vectors. These singular values $(\sigma_i)$ are such that it satisfies, $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r$. Further, we rearrange this decomposition as

$$ A = \sum_{i=1}^{r} \sigma_i U_i V_i' $$

Use of SVD in digital image processing has some advantages. First, the size of the matrices from SVD transformation is not fixed. It can be a square or a rectangle. Secondly, singular values in a digital image are less affected if general image processing is performed because bigger singular values not only preserve most energy of an image but also resist against attacks. Generally, the matrix $S$ has many small singular values. Finally, singular values possess intrinsic algebraic image properties. It is important to note that each singular value specifies the luminance of an image layer while the corresponding pair of singular vectors specifies the geometry of the image layer.

### 4. Directive contrast

According to Human Visual System (HVS), the local luminance contrast of the images is defined as [17]:

$$ C = \frac{L - L_B}{L_B} = \frac{L_H}{L_B} $$

where $L$ and $L_B$ represent the local luminance and the luminance of the local background. Generally, $L_B$ is regarded as local low frequency and hence $L - L_B = L_H$ is treated as local high frequency. Hence, local luminance contrast is used to denote the differences of objects in an image. On the above discussion, a sequence of Directive Contrast is defined as: [18]

- **Horizontal Contrast**
  $$ C_H = \frac{L_H}{L_H} $$

- **Vertical Contrast**
  $$ C_V = \frac{H_L}{H_L} $$

- **Diagonal Contrast**
  $$ C_D = \frac{H_H}{H_H} $$

where $L_L$, $H_L$, $L_H$, and $H_H$ are approximate (low frequency), horizontal, vertical and diagonal (high frequency) sub-bands at resolution level $i$ such that $1 \leq i \leq n$. Due to orthogonality of DWT, mixing in the frequency domain during decomposition and reconstruction of image is eliminated. Based on this fact, directive contrast gives more accurate results than the traditional local luminance contrast definition. Directive contrast depicts the high frequency information of an image and the relative intensity of high frequency to the background.

Another benefit of directive contrast is that the detail parts of the signal can be restored precisely by reversing the construction of the directive contrast:

- **Horizontal Contrast**
  $$ LH_i = C_H^i \times LL_i $$

- **Vertical Contrast**
  $$ HL_i = C_V^i \times LL_i $$

- **Diagonal Contrast**
  $$ HH_i = C_D^i \times LL_i $$

### 5. Proposed watermarking technique

In this section, we discuss some motivating factors in design of our approach to watermarking. The proposed method embeds watermark by decomposing the host image by the means of Discrete Wavelet Transform. The watermark used for embedding is a gray scale image.

First, the reference image is formed and is used for watermark embedding. Also, we save this reference image for the extraction process. Therefore, watermarking is applied on both reference and watermark images and the singular values of reference image is modified with the help of singular values of watermark image. Inverse wavelet transform is performed to reconstruct the watermarked image. The block diagram of proposed watermarking technique is shown in Fig. 3. Original image is not required for the extraction. Reference image is used for the watermark extraction. Hence, the extraction scheme is considered as semi-blind and hence the proposed watermarking technique is formulated as follows:

#### 5.1. Watermark embedding process

Let $f(i, j)$ represents the host image of size $M \times N$ and $W(i, j)$ represents the watermark of size $M_1 \times N_1$. To embed gray scale logo, the following technique is formulated:

1. Perform $n$-level discrete wavelet decomposition of the host image which is denoted by $f_{\theta}^p$, where $\theta \in \{H, V, D\}$ and $1 \leq p \leq n$. If we select all sub-bands then four reference images will be obtained. For our convenience and without loss of generality, we select only one sub-band. Let us denote the selected sub-band by $f_{\theta}^{select}$ and the information about selected sub-band is saved in $K$, where $K \in \{A, H, V, D\}$. If the value of $K$ is $A$ then the selected sub-band to form the reference image is $f_{\theta}^A$. This $K$ is used in extraction process.

2. Select any or all $f_{\theta}^{select}$ to make reference image, where $\theta \in \{A, H, V, D\}$.

### Table 1

<table>
<thead>
<tr>
<th>Images</th>
<th>Lena</th>
<th>Pepper</th>
<th>Mandril</th>
<th>Lake</th>
<th>Bridge</th>
<th>Pirate</th>
<th>L.Room</th>
<th>Tree</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>43.65</td>
<td>44.12</td>
<td>40.93</td>
<td>41.60</td>
<td>42.44</td>
<td>44.53</td>
<td>44.01</td>
<td>41.49</td>
<td></td>
</tr>
</tbody>
</table>

### Table 2

<table>
<thead>
<tr>
<th>Images</th>
<th>Lena</th>
<th>Pepper</th>
<th>Mandril</th>
<th>Bridge</th>
<th>Pirate</th>
<th>L.Room</th>
<th>Tree</th>
<th>$\rho$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.9996</td>
<td>0.9996</td>
<td>0.9995</td>
<td>0.9996</td>
<td>0.9996</td>
<td>0.9994</td>
<td>0.9991</td>
<td></td>
</tr>
</tbody>
</table>
Table 3
Correlation coefficient of all extracted logos after attacks.

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Pepper</th>
<th>Pirate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Filtering (13 × 13)</td>
<td>0.3696</td>
<td>0.6209</td>
</tr>
<tr>
<td>Median Filtering (13 × 13)</td>
<td>0.3233</td>
<td>0.5636</td>
</tr>
<tr>
<td>Additive Gaussian Noise (75%)</td>
<td>0.2843</td>
<td>0.5604</td>
</tr>
<tr>
<td>JPEG Compression (80:1)</td>
<td>0.9922</td>
<td>0.9829</td>
</tr>
<tr>
<td>Cropping ((1/4)th area remaining)</td>
<td>0.3840</td>
<td>0.6297</td>
</tr>
<tr>
<td>Rotation (50°)</td>
<td>0.3309</td>
<td>0.6297</td>
</tr>
<tr>
<td>Resizing (512)</td>
<td>0.2492</td>
<td>0.5604</td>
</tr>
<tr>
<td>JPEG Compression (80:1)</td>
<td>0.9922</td>
<td>0.9829</td>
</tr>
<tr>
<td>Additive Gaussian Noise (75%)</td>
<td>0.3696</td>
<td>0.6209</td>
</tr>
</tbody>
</table>

Table 3 continues...

(3) Perform 1-level discrete wavelet decomposition on the selected sub-band, which is denoted by $f_{n+1}^{ref}$, where $\theta \in \{A, H, V, D\}$.

(4) Find the Directive Contrast for all high frequency sub-bands (as defined in Section 4), which is denoted by $C_{fn}^{max}$, where $\theta \in \{H, V, D\}$.

(5) Initialize high frequency component to zero whose directive contrast are less than the threshold. The threshold directive contrast is given by:

$$T_{\theta} = \text{Sort}(p \cdot S_{\theta})$$

where $\text{Sort}(\circ)$ are the sorted directive contrast, $S_{\theta}$ is the size of the sub-band and $p$ is the percentage of the wavelet coefficients which we want to retain. Those wavelet coefficients in each orientation which have directive contrast more than the threshold value $T_{\theta}$ are considered as significant coefficients and are retained.

(6) Perform 1-level inverse discrete wavelet decomposition to get the watermarked image.

(7) Perform SVD transform on both reference and watermarked image,

$$f_n^{ref} = U_n S_n (V_n^{ref})^T$$

$$W = U_W S_W V_W^T$$

(8) Modify the singular values of reference image with the singular values of the watermark as

$$\sigma_{fn}^{ref} = \sigma_{fn}^{ref} + \alpha \sigma_W$$

where $\alpha$ is the watermark strength.

(9) Obtain modified reference image as,

$$\left(f_n^{ref}\right)^n = U_n^{ref} \left(S_n^{ref}\right)^n (V_n^{ref})^T.$$  

(10) After embedding the watermark, replace $f_n^{ref}$ by $(f_n^{ref})^n$.

(11) Perform n-level inverse discrete wavelet decomposition to get the watermarked image.

5.2. Watermark extraction process

The objective of this semi blind watermark extraction is to obtain the estimate of the original watermark. For watermark extraction from watermarked image, original image is not required. Hence this extraction is called semi-blind. The extraction process is formulated as follows:

(1) Perform n-level discrete wavelet decomposition on the watermarked image, which is denoted by $f_w^n$, where $\theta \in \{A, H, V, D\}$ and $1 \leq n \leq N$.

(2) Based on $K$, which we saved in embedding process, select the watermarked reference image, denoted by $f_{wn}^{ref} = f_w^n$.

(3) Perform SVD transform on both original reference and watermarked reference image,

$$f_n^{ref} = U_n S_n (V_n^{ref})^T$$

$$f_{wn}^{ref} = U_{wn} S_{wn} (V_{wn}^{ref})^T.$$  

(4) Extract the singular values of watermark image as:

$$\sigma_{W}^{ext} = \frac{\alpha \sigma_{fn}^{ext} - \sigma_{fn}^{ref}}{\alpha}.$$  

(5) Obtain the estimate of watermark image as,

$$W^{ext} = U_W S_{W}^{ext} V_W.$$

6. Results and discussions

6.1. Experimental setup

In order to explore the performance of the proposed watermarking algorithm, MATLAB platform is used and a number of experiments are performed on different images of size 512 × 512, namely Lena, Pepper, Mandrill, Lake, Bridge, Pirate, Living Room and Tree (shown in Fig. 4(a)). Four different gray scale logos of size 64 × 64, namely IT, IIT, Circles and IEEE are used as watermarked images (shown in Fig. 5).

![Fig. 7. (a) Watermarked Pepper Image after 13 × 13 average filtering b) Extracted Watermark c) Watermarked Pirate Image after 13 × 13 average filtering d) Extracted Watermark.](image-url)
Logo IT is embedded into Lena and Pepper images, IIT is embedded into Lake and Mandrill images, Circles is embedded into Bridge and Pirate images and finally IEEE logo is embedded into Living Room and Tree images. The watermarked image quality is measured using PSNR (Peak Signal to Noise Ratio). Fig. 4(b) shows the resultant watermarked image and the corresponding PSNR values are given in Table 1. No perceptual degradation is observed between the original and watermarked image according to HVS (Fig. 4).

Fig. 6(a,b,c,d,e,f,g,h) shows the extracted watermark logos from Lena, Pepper, Mandrill, Lake, Bridge, Pirate, Living-room and Tree images respectively and the corresponding correlation coefficients are given in Table 2. For watermark embedding, strength factor $\alpha$ is set to 0.035. For wavelet decomposition of original image, Daubechies filter coefficients and 3-level of decomposition are used. In order to find the threshold value, we retain 50% of wavelet coefficients as significant coefficients and without loss of generality, we selected $D_{sub}$-band for forming the reference image in the simulation.

To verify the presence of watermark, different measures can be used to show the similarity between the original and the extracted singular values. In the proposed algorithm, correlation coefficient is defined as

$$\rho(w, \bar{w}) = \frac{\sum_{i=1}^{r} w(i) \bar{w}(i)}{\sqrt{\sum_{i=1}^{r} w^2(i)}}$$

where $w$ is the singular values of the original watermark, $\bar{w}$ is the extracted singular values and $r = \max(M_1, N_1)$. $p$ is the number that lies between $[-1, 1]$. If the value of $p$ is equal to 1 then the extracted singular values are just equal to the original one, if it is $-1$ then the difference is negative for the largest singular values. In this case, the constructed watermark looks like a negative thin film.

6.2. Results

In order to demonstrate, the robustness of the proposed watermarking algorithm, the watermarked image is attacked by a variety of attacks namely Average and Mean Filtering, Gaussian noise addition, JPEG Compression, Cropping, Resize, Rotation, Histogram Equalization, Wrapping, Pixilation, Sharpen, Motion Blur and Contrast Adjustment. After these attacks on the watermarked image, the extracted logo is compared with the original one. For further analysis, Peppers and Pirate images are used, since these images are having higher PSNR values among all test images (the results for other images can be seen in our web site [20, 21].

6.2.1. Filtering

The most common manipulation in digital image is filtering. The extracted watermarks, after applying $13 \times 13$ averaging and median filtering, are shown in the Figs. 7 and 8. It can be observed that after applying these filters, images are very much degraded and lot of data is lost but the extracted logo watermark is still recognizable.

6.2.2. Addition of noise

Addition of noise is another method to estimate the robustness of the watermark. Generally, addition of noise is responsible for the degradation and distortion of the image. The watermark information is also degraded by noise addition and results in difficulty in watermark extraction. Robustness against additive noise is estimated by degrading the watermark image by randomly adding 75% Gaussian noise.
noise. The extracted logos are shown in Fig. 9(b,d) and it can be observed that extracted logo is a noisy image, but recognizable.

### 6.2.3. JPEG compression

The another most common manipulation in digital image is image compression. To check the robustness against Image Compression, the watermarked image is tested with JPEG compression attacks. The extracted watermark logo from 80:1 compressed images are shown in Fig. 10.

### 6.2.4. Cropping and resizing

Image cropping is very frequently used in real life. Cropping is the process of selecting and removing a portion of an image to create focus or strengthen its composition. Cropping an image is done by either hiding or deleting rows or columns. This is a lossy operation. For this attack, 50% of the watermarked image is cropped and then watermark is extracted (Fig. 11). To fit the image into the desired size, enlargement or reduction is commonly performed and resulted in information loss of the image including embedded watermark. For this attack, first the size of the watermarked image is reduced to 128×128 and again brought to its original size 512×512. Extracted watermark logo is shown in Fig. 12.

### 6.2.5. Rotation and pixilation

From the literature, we know that the wavelet transform is not rotational invariant. Proposed method can extract watermark for sufficiently large rotations. We extracted watermark from 50° rotated watermarked image. **Pixilation** is the process of displaying a digitized image where the individual pixels are apparent to the viewer. These

---

**Fig. 10.** a) Watermarked Pepper Image after JPEG Compression(80:1) b) Extracted Watermark c) Watermarked Pirate Image after JPEG Compression(80:1) d) Extracted Watermark.

**Fig. 11.** a) Watermarked Pepper Image after cropping b) Extracted Watermark c) Watermarked Pirate Image after cropping d) Extracted Watermark.

**Fig. 12.** a) Watermarked Pepper Image after Resizing b) Extracted Watermark c) Watermarked Pirate Image after Resizing d) Extracted Watermark.
kind of situations occur in real life when a low-resolution image designed for an ordinary computer display is projected on a large screen. Results are shown in Figs. 13 and 14 respectively.

6.2.6. Wrapping

Wrapping is the process of giving 3D effect to an object by distorting the image and stretching it to fit the selected curve. Robustness against wrapping is estimated by giving the 3D effect to watermark image around a spherical shape. Results are shown in Fig. 15.

6.2.7. General image processing attacks

We also tested our proposed watermarking method for histogram equalization, Motion Blur, Sharpen and Contrast Adjustment. Figs. 16 and 17 show the results for Histogram Equalization and Motion Blur respectively. For sharpening attack, the sharpness of the watermarked host image is increased by a factor of 100. Fig. 18 shows that the information is almost lost but we are still able to extract the watermark. For Contrast Adjustment, the contrast of the watermarked host image is increased by 50% (Fig. 19). Our proposed method is somewhat resilient against Histogram Equalization, Sharpen and Contrast Adjustment as observed by the obtained results. The correlation coefficients for all extracted watermarks after all attacks are given in Table 3.

6.3. Ambiguity attacks

In a recent paper, Ting et al. [19] shows that the reference scheme proposed by Liu et al. [16] fails to achieve its objective of being a robust
watermarking scheme. Their attack consists of two stages: in the first stage, the procedure to find out the modified pixel values have been given. In the second stage, they show how to exploit the modified pixel values to attack the robustness of the scheme. The description of the first stage is given below

(1) Since watermarked image is publicly available, the reference image, $X_w'$ is found by taking 1-level DWT and by setting all high frequency to zero.

(2) With the computed $X_w'$, the value of $X'$ is also known, because $X' = X_w'$ otherwise Eq. (2) (from Section 2) of Liu's extraction process would not work. This has empirically verified by the authors with the help of MATLAB.

(3) If we observe the embedding equation (Eq. (1) from Section 2) of the Liu's algorithm, it reveals that the value of modified pixel is either $x'(i,j) + \alpha$ or $x'(i,j) - \alpha$. Hence, they just scan all the pixels of $X_w'$ and check whether it equals to $x'(i,j) + \alpha$ or $x'(i,j) - \alpha$. Hence, in this way, embedding position is known.

Now, our proposed scheme withstand this ambiguity attack. To form the reference image, setting high frequencies to zero will not work. In the proposed scheme, the keys to form the reference image are:

(1) The level of decomposition.

(2) The value of $K$, i.e. which sub-band is used for making reference image.

(3) As the value of the wavelet coefficients change, the directive contrast will also change. This has also been empirically verified in the MATLAB.

(4) Value of $P$, i.e. how many wavelet coefficients are retained.

(5) The singular values of the reference image are used to embed the watermark instead of embedding them in wavelet coefficients.
Since watermarked image is publicly available, intruders can try to make reference image from the watermarked image. The problem is to determine the level of decomposition. Let us assume that they know the level of decomposition, still they require the information about the sub-band used for making the reference image. Even if the intruders have checked all the four sub-bands to make the reference image but without knowing the value of $P$, one cannot get the reference image and $P$ is only known to the person, who is the maker of reference/watermarked image. So the proposed watermarking scheme stands with the first stage of ambiguity attack. The second stage of ambiguity attack depends completely on the first stage. Hence this algorithm stands with ambiguity attack.

7. Conclusions

A semi-blind reference watermarking scheme is presented in which the watermark is a visually meaningful gray scale logo instead of a noise type Gaussian sequence. The embedding is done by modifying the singular values of reference image with the singular values of noise type Gaussian sequence. The embedding is done by modifying the watermark is a visually meaningful gray scale logo instead of a noise type Gaussian sequence. The embedding is done by modifying the singular values of reference image with the singular values of noise type Gaussian sequence. The embedding is done by modifying the singular values of reference/watermarked image. So the proposed watermarking scheme stands with the first stage of ambiguity attack. The second stage of ambiguity attack depends completely on the first stage. Hence this algorithm stands with ambiguity attack.

Acknowledgements

One of the authors, Gaurav Bhatnagar, gratefully acknowledges the financial support of the Council of Scientific and Industrial Research, New Delhi, India through his Junior Research Fellowship (JRF) scheme (CSIR Award no.: 09/143(0559)/2006-EMR-I) for his research work. The author, R. Balasubramanian, gratefully acknowledges the financial support of Sponsored Research and Industrial Consultancy (SRIC), Indian Institute of Technology Roorkee, India under the grant numbers MHR 03-05-(802,418,807,412). He also acknowledges the financial support of Department of Science and Technology(DST), India under his fast track project for young scientist (DST-302-MTD) to carry out this research work.

References

Balasubramanian Raman is an Assistant Professor and head of the Computer Vision, Graphics and Image Processing Laboratory in the Department of Mathematics at the Indian Institute of Technology Roorkee since February 2006. He was a Lecturer of Mathematics in IIT Roorkee from September 2004 to February 2006. He worked as a faculty of the Computer Science and Information Systems at Birla Institute of Technology and Science, Pilani, India in 2003–04. He worked as a Post Doctoral Associate at the Electrical and Computer Engineering Department (ECE), and member of the Visualization Research laboratory (VIZ Lab), at Rutgers, The State University of New Jersey, USA from July 2002 to April 2003. He was also a Post Doctoral fellow of Computer Engineering and Computer Science (CECS), and member of the Computational Intelligence Research Laboratory (CIRL), at the University of Missouri-Columbia (MU), Missouri, USA, from October 2001 to June 2002. He received his Ph.D. in Mathematics (2001) from the Indian Institute of Technology, Madras, India. He received his B.Sc. and M.Sc. in Mathematics from the University of Madras in 1994 and 1996 respectively. He is listed in Marquis Who’s Who in the World 2006, 2007 and 2008 respectively. So far he has published 13 International Journals, 32 Conference Proceedings, a Book Chapter and a Technical report. His areas of research include Computer Vision, Graphics, Satellite Image Analysis, Scientific Visualization, Imaging Geometry, Reconstruction problems, Bio-metrics and Water marking.