Image Watermarking in LWT Domain Based on Nonnegative Matrix Factorization and Singular Value Decomposition

Pranab Kumar Dhar
Department of Computer Science and Engineering
Chittagong University of Engineering and Technology (CUET), Chittagong-4349, Bangladesh
E-mail: pranabdhar81@gmail.com

Tetsuya Shimamura
Graduate School of Science and Engineering
Saitama University, 255 Shimo-okubo, Sakura-ku, Saitama 338-8570, Japan
E-mail: shima@sie.ics.saitama-u.ac.jp

Abstract—We present a blind watermarking method in lifting wavelet transform (LWT) domain based on nonnegative matrix factorization (NMF) and singular value decomposition (SVD) for image copyright protection. The watermark image is preprocessed first using a Gaussian map in order to enhance the confidentiality. LWT is then applied to the original image to get sub-bands and the low frequency sub-band is divided into blocks. NMF is performed on each of these blocks to get the nonnegative matrix and weight matrix. Weight matrix of each block is decomposed into three matrices using SVD. The largest singular value of each weight matrix is selected for embedding watermark using a quantization function. Simulation results indicate that the proposed method shows high robustness against different attacks. Moreover, it outperforms state-of-the-art methods in terms of invisibility and robustness.

Keywords—copyright protection; lifting wavelet transform; nonnegative matrix factorization; singular value decomposition.

I. INTRODUCTION

The recent development in computers and multimedia technology, digital (audio, image, and video) contents are easily transmitted and distributed via internet. This has become a serious threat for multimedia content owners. Thus, there is significant interest in copyright protection of digital contents. Digital watermarking is widely used for protecting digital contents from unauthorized copying. It is a process of embedding watermark into the digital data to show authenticity and ownership. This technique has several applications such as content authentication, data indexing, medical safety, broadcast monitoring, copyright protection, and so on. A comprehensive survey on image watermarking can be found in [1]. Most image watermarking methods utilize the spatial domain [2]-[3] or the transform domain such as discrete cosine transform (DCT) [4]-[5], fast Fourier transform (FFT) [6], and discrete wavelet transform (DWT) [7]-[8]. The spatial domain methods can be implemented easily and they have low computational cost. But, they are generally less robust to image processing operations. The transform domain methods are usually robust to common image processing operations; however, they have high computational cost. Conventional wavelet transform provides good results for its multi resolution characteristics and good reconstruction. However, it is mainly calculated using convolution operation, resulting in high computation. In addition, the storage requirements also increase because of the generated floating numbers. Therefore, the lifting wavelet transform (LWT) is introduced to improve the efficiency [9]. Recently, singular value decomposition (SVD) is widely utilized in image watermarking [10]-[12]. However, detection process of these methods is non blind and robustness results need further improvement. To overcome this limitation, we introduce a blind image watermarking method in LWT domain using SVD and non negative matrix factorization (NMF). The main characteristics of our proposed method include (i) it utilizes the LWT, NMF, and SVD jointly, (ii) it uses Gaussian map, containing the chaotic characteristic to enhance the confidentiality of the proposed method, (iii) watermark data is inserted into the largest singular value of each weight matrix obtained from each block of the low frequency LWT coefficients of the original image (iv) watermark extraction technique is blind. Experimental results demonstrate that the proposed watermarking method is not only robust to various attacks such as Gaussian noise, cropping, JPEG compression, and mean filtering, but also has superior performance to the state-of-the-art methods [10]-[12] in terms of invisibility and robustness.

The rest of the paper is organized as follows. Background information including LWT, NMF, and SVD is discussed in Section II. The proposed watermarking method including watermark preprocessing, watermark embedding process and detection process is introduced in Section III. Experimental results are presented in Section IV. Some concluding remarks are given in Section V.

II. BACKGROUND INFORMATION

A. Lifting Wavelet Transform

The LWT is designed for reducing the storage requirement and computational cost. It has different unique features compared with conventional wavelet: (i) it permits an in-place implementation of the fast wavelet transform therefore, it can be computed more effectively and requires low memory space, (ii) it is easy to design non-linear wavelet transforms, (iii) it has...
the frequency localization features which can overcome the limitation of the conventional wavelet transform. The key idea of the lifting wavelet is to create a new wavelet with better features using the conventional wavelet. Lifting wavelet scheme consists of three stages: split/merge, prediction, and update. The detail of the lifting scheme is shown in [9].

B. Singular Value Decomposition

Let \( A \) be an arbitrary matrix of size \( m \times m \). The SVD of matrix \( A \) is represented in the form \( A = U S V^T \), where \( U \) and \( V \) are unitary matrices of size \( m \times m \) and \( S \) is a diagonal matrix with non negative elements of size \( m \times m \). The diagonal elements of \( S \) are the singular values (SVs) of \( A \), which are assumed to be arranged in decreasing order. The columns of \( U \) are the left singular vectors and the columns of \( V \) are the right singular vectors of \( A \).

C. Nonnegative Matrix Factorization

NMF was designed to find a representative basis vector with nonnegative element [13], which overcomes the limitation of SVD. In many applications, negative elements may contradict physical realities. Let \( A \) be an arbitrary matrix of size \( m \times m \) with NMF of the form \( A = B H \), where \( B \) is an \( m \times r \) nonnegative matrix, containing the NMF basis vector and \( H \) is an \( r \times m \) nonnegative weight matrix, containing the associate coefficients.

III. PROPOSED WATERMARKING SCHEME

Let \( A = \{ a(k, l), 1 \leq k \leq M, 1 \leq l \leq L \} \) be the original image and \( W = \{ w(i), 1 \leq i \leq I \} \) be a binary watermark data that embeds into the original image.

A. Watermark Preprocessing

To increase the confidentiality of the proposed method, firstly, watermark data will be preprocessed. It uses a Gaussian map that contains the chaotic characteristics to encrypt the binary wavelet sequence for enhancing the confidentiality of the proposed method. It can be defined as follows:

\[
y(i + 1) = \exp\left(-a(y(i))^2\right) + b
\]

where \( y(1) \in (0,1) \), \( a \) and \( b \) are real parameters (map’s initial condition). Then \( y(i) \) is mapped using the following rule:

\[
z(i) = \begin{cases} 1 & \text{if } y(i) > T \\ 0 & \text{otherwise} \end{cases}
\]

where \( T \) is a predefined threshold. Finally \( w(i) \) is encrypted by \( z(i) \) with the following rule:

\[
u(i) = z(i) \oplus w(i), \quad 1 \leq i \leq I
\]

where \( \oplus \) is a exclusive-or (XOR) operation and \( u(i) \) is the encrypted watermark data. After this operation, the original watermark is encrypted and can not be found by random search. In this study, the value of \( y(1) \), \( a \), and \( b \) are used as secret key \( K \).

B. Watermark Embedding Process

The watermark embedding process is described as follows:

1) A single-level LWT is performed on the original image \( A \) to obtain the four sub-bands \{LL, LH, HL, HH\}, where LL sub-band contains the approximate coefficients and LH, HL, HH sub-bands contain the details coefficients.
2) LL sub-band is divided into non-overlapping blocks \( C = \{ C_i \}, 1 \leq i \leq I \) of size \( m \times m \).
3) NMF is applied to each block \( C_i \) of the LL sub-band. NMF is represented as:

\[
C_i = B_i H_i
\]

where \( B_i \) is a non negative matrix, containing the NMF basis vectors and \( H_i \) is a weight matrix containing the associate coefficients.
4) SVD is performed to decompose each matrix \( H_i \) into three matrices: \( U_i, S_i, \) and \( V_i \). The SVD is given by the following equation:

\[
H_i = U_i S_i V_i^T
\]

5) The proposed method embeds watermark bits into the largest singular value \( S_i(1,1) \) of each matrix \( S_i \) using a quantization function. This is because the largest singular value contains the most perceptual significant component of an image. Let \( R_i = \text{round}\left(\frac{S_i(1,1)}{Q}\right) \), where \( Q \) is a quantization coefficient. The embedding equation is given as follows:

\[
S_i'(1,1) = \begin{cases} R_i + C - (R_i \mod M), & \text{if } u(i) = 1 \\ R_i + C - ((R_i + C) \mod M), & \text{if } u(i) = 0 \end{cases}
\]

where \( M = 2C, C \) is an integer, mod is the modulo operation, and \( S_i'(1,1) \) is the modified largest singular value.
6) Reinsert each modified largest singular value \( S_i'(1,1) \) into matrix \( S_i \) and inverse SVD is performed to get the modified weight matrix \( H_i' \) which is represented as

\[
H_i' = U_i S_i' V_i^T
\]

7) Inverse NMF is applied to get the modified block \( C_i' \) which is represented as

\[
C_i = B_i H_i'
\]

8) After substituting each modified block \( C_i' \) into LL sub band a single-level inverse LWT is applied to get the watermarked image \( A' \).

C. Watermark Detection Process

The proposed watermark detection process does not need the original image to extract the watermark. The detection process is described in the following steps:

1) A single-level LWT is performed on the attacked watermarked image \( A' \) to obtain four sub-bands \{LL, LH, HL, HH\}.
2) LL sub-band is divided into non-overlapping blocks \( C = \{ C_i \}, 1 \leq i \leq I \) of size \( m \times m \).
3) NMF is applied to each block \( C_i \) of the LL sub-band to obtain the non negative matrix \( B_i' \) and the weight matrix \( H_i' \).
4) SVD is performed to decompose each matrix \( H_i' \) into three matrices: \( U_i', S_i', \) and \( V_i' \).
5) Calculate \( R_i' \) of each \( S_i'(1,1) \).
6) Encrypted watermark data is extracted by the following equation:

\[ u^*(i) = \begin{cases} 1 & \text{if } (R_i \mod 2) = 1 \\ 0 & \text{otherwise} \end{cases} \]  

(9)

7) Perform chaotic decryption using the secret key \( K \) to find the binary watermark data with the following rule:

\[ w^*(i) = z(i) \oplus u^*(i) \]  

(10)

IV. SIMULATION RESULTS AND DISCUSSION

We conducted several experiments to evaluate the performance of the proposed method. In our experiment, four different images (Lena, Baboon, Monet, and Balloon) of size 128\times128 were used as original image. After applying single-level LWT on the original image, four sub-bands \{LL, LH, HL, HH\} of size 64\times64 were obtained. LL sub-band is divided into 4\times4 non-overlapping blocks. Therefore, 256 blocks are obtained from LL sub-band. Then, NMF is applied to each of these blocks. SVD is applied to weight matrix \( H_i \) of each block. The largest singular value \( S(1,1) \) of each weight matrix \( H_i \) is selected for embedding watermark. Therefore, the length of the watermark data is 256. Fig. 1 shows four different 128\times128 original images used in this study.

Fig. 1. Four different original images used in the study: (a) Lena, (b) Baboon, (c) Monet, and (d) Balloon

A. Imperceptibility

The visual quality of the watermarked image is done by calculating the peak signal-to-noise ratio (PSNR) which is represented as:

\[ \text{PSNR} = 10 \log_{10} \left( \frac{255^2}{MSE} \right) = 10 \log_{10} \left( \frac{255^2}{1/MM \sum_{i=1}^{M} \sum_{j=1}^{N} (A - A')^2} \right) \]  

(12)

Fig. 2 shows the qualitative evaluation of the watermarked images using the proposed method. Table I shows the PSNR comparison between the proposed and several recent methods for same images. From this comparison, we observed that the proposed method provides better result than all other methods in terms of PSNR.

Fig. 2. Invisibility of watermarked images using proposed scheme: (a) Lena (b) Baboon (c) Monet, and (d) Balloon

B. Robustness

To test the similarity between the original watermark \( W \) and the extracted watermark \( \hat{W} \), the normalized correlation coefficient (NC) is calculated which is represented as follows:

\[ NC(W, \hat{W}) = \frac{\sum_{i=1}^{M} w(i) \cdot \hat{w}(i)}{\sqrt{\sum_{i=1}^{M} w(i)^2 \cdot \sum_{i=1}^{M} \hat{w}(i)^2}} \]  

(11)

In order to test the robustness of the proposed watermarking method, different attacks such as white Gaussian noise, JPEG compression, cropping, and mean filtering were performed on the watermarked images.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>30.23</td>
<td>31.56</td>
<td>36.78</td>
<td>41.35</td>
<td></td>
</tr>
<tr>
<td>Baboon</td>
<td>30.54</td>
<td>32.68</td>
<td>37.21</td>
<td>40.24</td>
<td></td>
</tr>
<tr>
<td>Monet</td>
<td>30.83</td>
<td>32.82</td>
<td>37.48</td>
<td>38.75</td>
<td></td>
</tr>
<tr>
<td>Balloon</td>
<td>31.56</td>
<td>31.72</td>
<td>36.62</td>
<td>39.43</td>
<td></td>
</tr>
</tbody>
</table>

For noise attack, white Gaussian noises with zero mean and different variances (100, 300, 600, and 900) were added to the watermarked ‘Lena’ image which is shown in Fig. 3. Table II shows the NC values of the proposed and several recent methods against white Gaussian noise attack. From this comparison, we observed that the proposed method achieves better robustness than these methods.

Fig. 3. Watermarked Lena images after white Gaussian noise attack

<table>
<thead>
<tr>
<th>N(μ, σ²)</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>N(0, 100)</td>
<td>0.9538</td>
</tr>
<tr>
<td>N(0, 300)</td>
<td>0.9662</td>
</tr>
<tr>
<td>N(0, 600)</td>
<td>0.9438</td>
</tr>
<tr>
<td>N(0, 900)</td>
<td>0.9817</td>
</tr>
</tbody>
</table>

For mean filtering attack, watermarked images were filtered by 3\times3 mean (Gaussian) filter which is shown in Fig. 5. Table IV shows the NC values of the proposed scheme and the several recent methods against mean filtering attack. From this comparison, we observed that the proposed method has better robustness than these methods.

Table IV shows the NC values of the proposed scheme and the several recent methods against mean filtering attack. From this comparison, we observed that the proposed method has better robustness than these methods.

<table>
<thead>
<tr>
<th>N(μ, σ²)</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>N(0, 100)</td>
<td>0.9538</td>
</tr>
<tr>
<td>N(0, 300)</td>
<td>0.9662</td>
</tr>
<tr>
<td>N(0, 600)</td>
<td>0.9438</td>
</tr>
<tr>
<td>N(0, 900)</td>
<td>0.9817</td>
</tr>
</tbody>
</table>
For cropping attack, 25% of the images were removed from each watermarked images which is shown in Fig. 6. Table V shows the NC values of the proposed and several recent methods against cropping attack. From this comparison, we observed that the proposed method shows higher robustness than these methods.

Overall, the proposed method shows superior performance than the state-of-the-art methods in terms of invisibility and robustness. This is because watermark data is embedded into the largest singular value of each weight matrix obtained from each block of the LL sub-band of the original image.

![Different watermarked images after applying mean filtering attack: (a) Lena (b) Baboon (c) Monet, and (d) Balloon](image1)

![Different watermarked images after applying cropping attack: (a) Lena (b) Baboon (c) Monet, and (d) Balloon](image2)

![Different watermarked images after applying mean filtering attack: (a) Lena (b) Baboon (c) Monet, and (d) Balloon](image3)

![Different watermarked images after applying cropping attack: (a) Lena (b) Baboon (c) Monet, and (d) Balloon](image4)