Digital Color Image–Adaptive Watermarking using Blind Source Separation

Sangeeta D. Jadhav¹ and Anjali S. Bhalchandra²

¹Asst Prof Electronics & Telecommunication, AIT, Pune (MS), India, E-mail: djsangeeta@rediffmail.com
²Prof & HOD, Electronics & Telecommunication, GEC, Aurangabad, (MS), India

ABSTRACT: In a digital watermarking scheme, it is not convenient to carry the original image all the time in order to detect the owner’s signature from the watermarked image. Moreover, for those applications that require different watermark for different copies, it is preferred to utilize some kind of watermark-independent algorithm in extraction. This paper presents a digital color image watermarking scheme using Blind Source Separation to embed the watermark by manipulating the least significant levels of the blue channel of the host color image so as not to bring about a perceptible change in the marked image. The novelty of our scheme lies in determining the mixing matrix for BSS model, based on the smooth and textured metric based on energy content of the image. This makes our method image adaptive to embed color image into color images. Meanwhile the ICA (Independent Component Analysis) algorithm is introduced in extraction procedure, through which the watermark can be derived efficiently. The proposed method, undergoing different experiments, has shown its robustness against many attacks.

Key Words: Watermark, Blind Source Separation, ICA

1. INTRODUCTION

With the development of network and multimedia techniques, data can now be distributed much faster and easier. Unfortunately, engineers still see immense technical challenges in discouraging unauthorized copying and distributing of electronic documents [1]. Different kinds of handwritten signatures, seals or watermarks have been used since ancient times as a way to identify the source or creator of document or picture. However, in digital world, digital technology for manipulating images has made it difficult to distinguish the visual truth. One potential solution for claiming the ownership is to use digital watermarks. A digital watermark is a transparent, invisible information pattern that is inserted into a suitable component of the data source by using a specific computer algorithm. In nature, the process of watermark embedding is the same as some special kind of patterns or under-written images are added into the host image, we can consider it as a mixture of host image and watermark image, thus without host image the watermark detection is equal to blind source separation in the receiver. Blind digital watermarking does not need the original images or video frames in the detection stage, thus it is the only feasible way to do watermarking in many multimedia applications, such as data monitoring or tracking on the internet, notification of copyright in playing DVD’s. In particular some watermarking schemes require access to the ‘published’ watermarked signal that is the original signal just after adding the watermark. These schemes are referred as semi-blind watermarking schemes. Private watermarking [2] and non-blind-watermarking mean the same: the original cover signal is required during the detection process. In the internet distribution application the owner can always distribute the multimedia data by assigning different watermarks to different users in order to prevent illegal redistribution of data by a legal user. In such scenario the watermark detection /extraction algorithms requiring the information of watermark location and strength or the original watermark should fail since the users do not know.

Image watermarking techniques proposed so far can be categorized based on the domain used for watermarking embedding domain. The first class includes the spatial domain methods [16]. These embed the watermark by directly modifying the pixel values of the original image. The second contains Transform domain techniques, Discrete Fourier Transform (DFT) [17] Discrete Wavelet Transform (DWT) [9, 12, 15] Discrete Cosine Transform (DCT) [14, 10] other is to change the image coefficients in the frequency domain.
The third class is the feature domain technique, where region, boundary and object characteristics are taken into account [13]. The main directions that have been traced in the design of the watermarking techniques are either acting on all the host image or operating on certain selected pixel blocks [18]. The first class includes the works of Adib et al. [3] have proposed to use the blue channel as the embedding medium. In [5], the authors have benefited from a new decomposition of the color images by the use of hyper complex numbers, namely the Quaternion and they achieved their watermarking/data-hiding operation on the component of the quaternion Fourier Transform. A watermarking technique based on the color quantization has been proposed in [6] for block based techniques, the selection of block for embedding is key dependent. Host image is divided into 8x8 blocks and each bit of the binary encoded watermark is embedded in each such block. Different attacks on watermarking have been described in [19]. In the recent past, significant attention has been drawn to Blind source Separation by Independent Component Analysis [4, 7, 8, and 6] and has received increasing care in different image data applications such as image data compression, recognition, analysis etc. The technique of BSS has been extended to the field of watermarking images. In this paper, a new color image adaptive watermarking technique is proposed, which adopts Independent Component Analysis (ICA) for watermark detection and extraction process. Watermark embedding will be performed in the blue channel, as it is less sensitive to human visual system. The paper is structured as follows: section 2 describes the proposed watermarking method and section 3 discusses the practical implementation and ways for achieving better results. Section 4 gives evaluation and analysis and finally section 5 mentions conclusions.

2. PROPOSED WATERMARKING METHOD

In this paper, we discuss a new robust hybrid watermarking approach for still image watermarking in which the watermark embedding/extracting process consist of the consideration of Blind Source Separation technique and RGB decomposition.

2.1. Watermark Embedding

As shown in Figure 1, the effective watermark embedding consists of mainly three phases. In first phase the blue channels of the host image and watermark image are extracted and the blue channel is divided into the sub-images of size equal to the size of watermark. In this paper the size of host image selected is 512*512 (M x M) and size of watermark image is 64*64 (N x N) so that M >> N.

In order to determine the sub-image of interest , the host image is divided into 64*64 (N x N) blocks and a sliding square window containing Nb number of such blocks in both the horizontal and vertical directions (a tentative sub-image) is considered. It has been shown that the energy of textured portion of image is high. Based on the energy metric, the two blue channel sub-images of size 64*64, one representing the smooth portion and other the textured one, are selected.

In second phase, the BSS model (Figure 1) is used to embed the watermark in the blue channel.

Figure 2 depicts a simplest BSS model assumes the existence of ‘n’ independent components S1, S2, S3……..Sn [S(t)], and the same number of linear and instantaneous mixtures of these sources, X1, X2,……..Xn [X(t)] that is in vector matrix notation form the mixing matrix model can be represented as -

\[
x = A* s
\]

(1)

Where A is square (n x n) mixing matrix.
This mixing matrix $A$ is selected to mix the sub-images with watermark to form two mixtures (watermarked sub-image). These mixtures will be identical to the sub-images selected from the host image. Thus the mixing operator ‘$A$’ has to be appropriately chosen such that the human vision can not determine that the message is contained inside. $W$ is the demixing matrix which is estimated later by BSS algorithm [20] to separate out the sources.

In this paper we have proposed image adaptive method to calculate mixing matrix to keep the watermark image hidden in the host image. The mathematical preliminaries used to find the mixing matrix is described below.

By using logarithmic scale as our estimated mixing coefficients, has advantage of removing the indeterminacy in the equations of mixing as specified in equation (1)

$$x = A^* s$$

Now for any kind of mixing we need to work on the coefficient of “$A$” and the changing rate of coefficients determines the best selection of coefficient.

As if we look at the below equation:

$$r = v \times \frac{d}{dA} \text{(controlling parameter)}$$ (2)

Now the above equation depicts how “Controlling parameter” is changing w.r.t “$A$”. The variable “$r$” defines the rate at which “$A$” should be change to get appropriate mixing matrix. The controlling parameter in this paper is ‘Energy’ of the image.

In case of non linear scale the estimation we can drive out are much easier to converge. As compared to a linear function which gives the fixed equally spaced response the non linear functions provide with more variable points. Variable points make the estimation easier and get easily converged.

One of the characteristic of functions like logarithm is they have axes as their asymptotes.

The implication of above property is that we don’t have to take care for null results.

In third phase one of the marked blue channels is fused with the initial host’s red and green channels to form a compound watermarked sub-image. This sub-image will be implanted at its first location, in the host image called watermarked image and is open to the public. The remaining watermark blue channel is kept secret by the copyright owner. It will constitute the secret key corresponding to the location at which the watermark is fused with the original host image.

A watermark embedding is summarized in the following steps.

**Step-1:** Take the host and watermark color images, respectively of size $(M \times M)$ and $(N \times N)$ with $M \gg N$. Select their blue channels.

**Step-2:** Select two $(N \times N \times 3)$ blocks, one in smooth area and the other in textured regions.

**Step-3:** Obtain the mixing matrix using equation (2) for the two selected sub-image blocks $S_1$ and $S_2$.

**Step-4:** For each block constructs the marked color sub-image by using one of the marked blue channel sub-images. The compound sub-image (watermarked sub-image) is encrusted into the corresponding blocks of the earlier chosen region in the host image and the other secret blue channels must be kept for a prospective use in the watermark extraction process.

**(B) Watermark Extraction and Authentication**

In the case where watermarked image is tampered, the alteration can be detected and localized for copyright protection. It is also possible to perform the ownership authentication.

For the watermark extraction and the ownership authentication, the source image block and the watermark are recovered here using Blind Source Separation based on joint digitalization algorithm [20] to recover the host image block and watermark image block.

The extraction process can be summarized in the following steps.

**Step-1:** Extract the two marked blocks from the tampered watermarked image by using the first part of the key which is the position key.
**Step 2:** Obtain the blue channels of the extracted blocks.

**Step 3:** Apply a PCA whitening process on associated blue channel and the corresponding secret blue one.

**Step 4:** Post processing has to be done on the whitened blue channel.

### 3. PRACTICAL IMPLEMENTATION

Both the images (host and watermark) used are color images. The color Lena (512 x 512) is utilized as the test image and (64*64) Peppers as the signature one. The blue channels of both the images are extracted. The extracted blue channel of host image (Lena’s image) is divided into blocks of size 64*64. Based on the energy metric, the two blue channel sub-images of size 64*64, one representing the smooth portion and other the textured one, are selected. The Mixing matrix is to be selected correctly to produce watermarked images similar to the host one. Logic is developed to form a mixing matrix based on the energy criterion of the images forming the mixture.

### 4. EVALUATION AND ANALYSIS

In this paper, the algorithm is demonstrated by a color lena.jpg image of size 512*512 pixels as an original image and another with a color image of size 64*64 pixels as watermark.

A series of attacks are tested to verify the robustness of our algorithm include median filtering, adding salt and pepper noise, adding Gaussian noise, JPEG compression, and taking wavelet transform etc.

Mean Square Error (MSE), PSNR (Peak signal to Noise Ratio) and NC (Normalized Cross-Correlation) are used to estimate the quality of extracted watermark.
The equations used are defined as below:

\[ MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [r(i, j) - r^*(i, j)]^2 \]  

(3)

Where \( r(i, j) \) represents pixel at location \((i, j)\) of the original watermark and \( r^*(i, j) \) represents the pixel at location \((i, j)\) of recovered watermark. \( M, N \) denotes the size of the pixel.

\[ PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right) \]  

(4)

\[ NC = \frac{\sum_{m=1}^{M} \sum_{n=1}^{N} W(m,n) \times W^*(m,n)}{\sqrt{\sum_{m=1}^{M} \sum_{n=1}^{N} W^2(m,n) \times \sum_{m=1}^{M} \sum_{n=1}^{N} W'^2(m,n)}} \]  

(5)

Where \( W \) is original watermark and \( W^* \) is recovered watermark with zero mean value each.

In addition to above performance parameters, the parameters like entropy, energy etc are also noted to study the effect of attack on recovered watermark.

### Table 1

<table>
<thead>
<tr>
<th>Attacks</th>
<th>PSNR</th>
<th>MSE</th>
<th>NC</th>
<th>Entropy</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>No attack</td>
<td>26.80</td>
<td>135.5</td>
<td>0.71</td>
<td>3.94</td>
<td>0.24</td>
</tr>
<tr>
<td>Gaussian noise</td>
<td>26.85</td>
<td>135.0</td>
<td>0.51</td>
<td>3.52</td>
<td>0.16</td>
</tr>
<tr>
<td>Salt and Pepper noise</td>
<td>26.35</td>
<td>150.3</td>
<td>0.72</td>
<td>3.37</td>
<td>0.28</td>
</tr>
<tr>
<td>Median filter</td>
<td>26.46</td>
<td>146.7</td>
<td>0.83</td>
<td>3.66</td>
<td>0.28</td>
</tr>
<tr>
<td>Averaging filter</td>
<td>26.39</td>
<td>149.0</td>
<td>0.85</td>
<td>3.68</td>
<td>0.30</td>
</tr>
<tr>
<td>Compression</td>
<td>26.80</td>
<td>135.5</td>
<td>0.71</td>
<td>3.93</td>
<td>0.24</td>
</tr>
<tr>
<td>Wavelet transform</td>
<td>26.69</td>
<td>139.3</td>
<td>0.84</td>
<td>3.56</td>
<td>0.26</td>
</tr>
</tbody>
</table>

**5. CONCLUSIONS**

In this paper, we proposed a digital color image watermarking technique using Blind Source Separation theory along with RGB decomposition to embed / extract watermark.

The novelty of our scheme lies in determining the mixing matrix for BSS model, based on the smooth and textured metric based on energy content of the image. This makes our method image adaptive to embed color image into color images. Meanwhile the ICA (Independent Component Analysis) algorithm is introduced in extraction procedure, through which the watermark can be derived efficiently. The proposed method, undergoing different experiments, has shown its robustness against many attacks as specified in Table 1. Our algorithm has a clear math background and easy in determining the mixing matrix for BSS model.

**REFERENCES**


