A Novel Blind Color Image Watermarking Technique in Hybrid Domain Using LSB Approach and Discrete Slantlet Transform

Harith R. Hasan¹, Ghazali Bin Sulong², Ali Selamat³

Faculty of Computing, Universiti Teknologi Malaysia, 81310, Skudai, Johor, Malaysia

Email: ¹hrhr1980@yahoo.com, ²ghazali@spaceutm.edu.my, ³aselamat@utm.my

ABSTRACT

This paper proposes a blind color image watermarking technique in hybrid domain which combines LSB approach and Discrete Slantlet transform (DST). The proposed technique utilizes two interrelated watermarks namely, main watermark (MW) and sub-watermark (SW), which is a statistical information of the MW. Firstly, the RGB cover image is converted to YCbCr color space. Then the Cb component is selected for embedding the MW by utilizing the first three least-significant-bits of eight bit-plane in spatial domain. Secondly, the Cr component is selected and converted into the transform domain using DST, and is subsequently decomposed into three levels viz. HL1, LL2 and LL3 sub-bands. The SW is then embedded onto the LL3. Experimental results show that the performance of the proposed technique is very encouraging with average PSNR of 43db, and NCC value of more than 0.93 for both extracted watermarks after performing five severe attacks. It also reveals that capacity has increased to more than 12.5%.

Keywords: Blind color image watermarking, Hybrid domain, Robustness, Imperceptibility, Discrete slantlet transform (DST).

1. INTRODUCTION

Due to the rapid growth of Internet and multimedia technologies in recent years, digital watermarking has become one of the hottest topics in multimedia signal processing research. This trend can be attributed to the need to protect multimedia digital contents against unauthorized replication, manipulation, and other copyright violations. Since the last decade, many digital watermarking algorithms have been proposed for owner or distributor identification and copyright protection of digital multimedia assets. Digital watermarking schemes can be categorized as non-blind and blind approaches. In non-blind watermarking approaches the information for cover image and statistical information about watermarked image are known prior to watermark detection and extraction [1].
In blind watermarking approaches, extraction of the watermark image is performed without original image’s information [1,2]. Nevertheless generally, the blind approaches are more difficult than the non-blind schemes in extraction stage especially after attacks. Moreover, it is still better-off in terms of security [3]. For most application, security is considered as a vital aspect of digital watermarking schemes and so the watermarked information must be robust against intentional and unintentional attacks. For this reason, some studies propose repeated embedding for the same watermark, however, it increases the degradation effects of the host image, which is a major drawback in multiple watermarking [4].

2. BACKGROUND & RELATED WORKS

Digital watermarking techniques can be categorized into two domains: the spatial domain and the transform domain [1,5,6]. The spatial domain watermarking is said to be of lower computational complexity [7,8,9], and is advantageous with respect to capacity and imperceptibility [10]. On the other hand, the transform domain is more superior in terms of robustness. The combination of the two domains is termed as the hybrid domain.

Transform based watermarking technique is well-known for its robustness against many types of attacks. In order to embed a watermark image, a transformation algorithm is applied to decompose the host image. Then, modifications are made to its coefficients. Possible transformation techniques include the Discrete Fourier Transform (DFT) [14], Discrete Cosine Transform (DCT) [15,16], and Discrete Wavelet Transform (DWT) [1,5,11,12,13,19,20]. On the other hand, spatial domain watermarking has since the 90’s been the fundamental scheme. This domain makes use of selected bit-planes in a given host image for the watermark embedding process, consequently, some pixels of the host image are directly modified with respect to the image pixel values [3,17,18]. A bit-plane of a digital image is a set of bits which have the same position in the respective binary numbers. For example, the 8-bit representation of pixel values represents eight bit-planes. The 1st bit-plane consists of the set of the most significant bits (MSB), while the 8th bit plane consists of the least significant bits (LSB). The remaining bit-planes (2\textsuperscript{nd} - 7th) are referred to as the intermediate significant bits (ISB) [21,22,25].

The hybrid based watermarking stems from a combination of spatial and transformation domains watermarking. With the hybrid domain, the embedding process is executed twice on the host image, first in the spatial domain and followed by transform domain, or vice-versa. Generally, hybrid based watermarking techniques increase the capacity, imperceptibility and robustness of watermarking, and consequently increases the security of the watermarked information.
In 2003, a hybrid watermarking technique was proposed by Frank and Wu [23]. In their work the cover image for the watermarking was partitioned into several parts, each part was subdivided into eight pixels. The watermark image was also partitioned, but in two parts, one part to embed the cover image in the transform domain, while the other part for embedding the cover image in the spatial domain. They also utilized lower frequency DCT coefficients of the cover image as the background in which the watermarked image is embedded. On the other hand, the LSB bit–plane was used as the background for embedding the other part of the watermarked image. It is evident that the approach is robust against cropping attacks, but this technique used the same component of cover image for embedding both in spatial and transform domains. As a result the embedded watermark has lost its vital information. It is also observed that the technique is not robust against jpeg 2000, Gaussian noise, and Speckle attacks.

Saba et al [24] proposed an invisible watermarking scheme in spatial and frequency domains. In their work different watermarking attacks were injected to the watermarked image. The fast Fourier transform (FTT) was used to transform the cover image to the frequency domain, where the central frequencies were selected for data insertion in a ring-like fashion. In spatial domain, the encrypted data was then inserted in the LSB. It is observed that their approach is not robust against a number of attacks.

In 2009, Dejun et al [5] proposed a conversion of the cover image from the spatial to transform domain. The LL sub-band of the image was used as the background for embedding the watermark. Then, the ISB (4th bit-plane) of the cover image is used as a background for embedding the watermark in the spatial domain. The same watermark image was then formatted using the Arnold transform so that the spatial relationship of the visual recognizable part of the watermarked image can be distributed. Although their technique achieved good robustness and imperceptibility; however, its capacity is limited and computationally complex.

Perumal and Kumar [13] proposed a DWT-based watermarking technique using thresholds on intermediate bit values. In their work, they utilized four stages in the embedding process, which are: 1) the computation of DWT, 2) determination of thresholds based on intermediate bit values, 3) execute watermark embedding in ISB and 4) computation of inverse DWT. The L-level DWT transform was performed on the host image to obtain discrete wavelet components. Subsequently, a triple or a quad of pixels was utilized instead of a pixel pair, and then, the bits of the digital watermark bit-stream were embedded within the ISB bit values. The transformed image was then converted to the watermarked image via L-level inverse DWT conversion. However, performance of the method is poor in terms of both computational cost and robustness.

This paper focuses on capitalizing on the advantages of two aforementioned domains in realizing a more efficient watermarking approach. In subsequent subsection, a brief discussion on Discrete Slantlet Transform (DST) is presented.
3. DISCRETE SLANTLET TRANSFORM

The discrete wavelet transform (DWT), which is used for embedding through filter bank iteration, is one of the most popular transforms, but it requires a large number of iterations to achieve a discrete time basis for an optimal result [26]. Therefore, the discrete slantlet transform (DST) is adopted in this paper because it is not based on filter bank iteration; rather, it uses different filters for each scale. For a two-channel case the Daubechies filter is the shortest filter which makes the filter bank orthogonal and has K zero moments. For K=2 zero moments the iterated filters lengths equal 10 and 4 but the slantlet filter bank with K=2 zero moments has filter length 8 and 4. Thus the two-scale slantlet filter bank has a filter length which is two samples less than that of a two-scale iterated Daubechies-2 filter bank. This difference grows with the increased number of stages. Each filter bank has a scale dilation factor of two and provides a multi-resolution decomposition. The slantlet filters are piecewise linear. Even though there is no tree structure for slantlet it can be efficiently implemented like an iterated DWT filter bank. Therefore, computational complexities of the slantlet are of the same order as of the DWT, but slantlet transform gives better performance in terms of denoising and compression of the signal [27].

4. PROPOSED METHOD

The proposed technique utilizes two interrelated watermarks namely, main watermark (MW) and sub-watermark (SW), which is a statistical information of MW. The technique begins with conversion of RGB cover image into YCbCr color space. Then, the Cb component is selected for embedding the MW by utilizing the first three least-significant-bits of eight bit-plane in spatial domain. Next, the Cr component is selected and converted into the transform domain using DST, and later decomposed it into three levels viz. HL1, LL2 and LL3 sub-bands. The SW is then embedded onto the LL3. The advantage of using Cb and Cr separately with two types of watermarks is to ensure the integrity of the watermarked image beside the imperceptibility, robustness and capacity. A new embedding technique is proposed in spatial domain by using logical operations to improve the imperceptibility. On the other hand, a novel technique is applied in transform domain using the DST for embedding the SW. Two block diagrams are given in Fig. 1 and Fig. 2 below that represent the flow of the abovementioned methodology.
Fig. 1: Embedding stage of the watermarking technique
Pre-processing stage: At first, the RGB color image is converted to YCbCr. This color space is considered less sensitive to the human visual system (HVS), more robust and higher imperceptibility than the RGB color space [25].

Then Cb and Cr components are selected as the background for embedding the watermark image. A walk-through of the pre-processing stage is shown in Fig. 3. The image transformation from RGB to YCbCr color space is adopted from [26]:

Fig. 2: Extraction stage of the watermarking technique
Fig. 3: A flowchart of the Pre-processing.

Embedding stage: It consists of two parts. For the first part, the embedding in spatial is performed: The MW is normalized from 8 bits to 4 bits by utilizing the first four most-significant-bits in order to maximize the capacity of Cb before the embedding is taken place. The normalization process is given in Fig 4.

e.g.: \( P_1 = 198 \)

```
1 1 0 0 0 1 1 0
```

Normalize to first four most significant bits

```
1 1 0 0 0 0 0 0
```

Fig. 4: Normalization of MW from 8 bits to 4 bits
Meanwhile, the Cb is divided into groups of 8-pixels: The first four pixels of each group are selected for embedding, while other pixels stay without any changes. Then, each pixel of the MW is sequentially embedded onto the first three least-significant-bits of the selected pixels of Cb. The process is repeated until all the pixels of MW are embedded. Fig. 5 and Algorithm 1 depict the abovementioned embedding process.

**Fig. 5:** The embedding procedure
Algorithm 1: The embedding algorithm

Data: Cb component, W Watermark image
Result: CbW watermarked component

Cpt = 0;
for $p = 0 \rightarrow W.width$ do
    for $q = 0 \rightarrow W.high$ do
        for $i = 1 \rightarrow 4$ do
            $w = W[p,q]$;
            $x = \text{cpt} \mod \text{Cb.width}$;
            $y = \text{cpt} \mod \text{Cb.width}$;
            $V = \text{Cb}[x,y]$;
            switch the value of $i$ do
                case 1 value
                    $M = 254$; $N = 7$; $N1 = 128$; break;
                case 2 value
                    $M = 253$; $N = 5$; $N1 = 64$; break;
                end
                case 3 value
                    $M = 251$; $N = 3$; $N1 = 32$; break;
                end
                case 4 value
                    $M = 254$; $N = 7$; $N1 = 128$; break;
                end
            endsw
            $w = (w \& N1)$;
            $V = (V \& M) + (\text{shift.R.} (w, N))$;
            CbW[x,y] = V;
            cpt = cpt + 1;
            $i \leftarrow i + 1$
        end
        cpt = cpt + 4;
        $q \leftarrow q + 1$
    end
    $p \leftarrow p + 1$
end

Where:

- **CPT** is an index for determine the location of selected pixels for embedding.
- **W.width** and **W.high** are width and height of the watermark MW;
- **Cb.Width** is the width of the Cb.
- **w** represents the value of MW pixel to be embedded.
- **V** denotes the value of selected pixel in the Cb.
- **M** and **N1** are the mask used to determine the binary location.
- **N** represents the shift value.

Fig. 6 illustrates the embedding stage when the MW is embedded in 1st, 2nd and 3rd bit-planes of the selected pixels of the Cb to create a Cb-watermarked image.
For the second part, the embedding is performed on Cr component using DST. Firstly, the SW is created from the MW by reducing its size from (128 X 256) pixels to (64 X 64) pixels. Then, SW is converted from gray-scale to a binary image, and is subsequently embedded onto the Cr. The embedding process is illustrated in Fig. 7.
The DST decomposes the Cr from spatial domain to transform domain by changing its coefficient values. Three levels of DST are applied on the Cr. Level 1 is further divided into four frequency sub-bands, which are LL1, HL1, LH1, and HH1. The HL1 sub-band is then selected and level 2 is applied on it for further subdivision to four parts, which are LL2, HL2, LH2 and HH2. At this point the LL2 sub-band is then selected and level 3 is applied on it for further division to four more parts, which are LL3, HL3, LH3 and HH3. After all these divisions, the LL3 is finally selected for embedding the SW. The watermarked image is obtained by using the following equation:

\[ LL3 (i,j) = \alpha \times W(i,j) \]  

(1)

Where
\( \alpha \) denotes a strength factor, \((\alpha \in [0,1])\), where \( \alpha = 0.5 \) is chosen empirically;

\( W(i,j) \) represents a watermark image.

Next, 3-level of IDST is applied to create Cr-watermarked image (CrW). The embedding step is depicted in Fig. 8.

![Diagram showing the embedding process in transform domain](image)

**Fig. 8:** Embedding process in transform domain

Upon completion of the embedding phase, CrW, CbW and Y components are merged, and is then converted to RGB color space to obtain a watermarked image.
Finally, an extraction process is performed to extract the watermarks SW and MW. The same procedure as mentioned above is applied except it is done in reversal order. The extraction process is given by Algorithm 2 and Fig. 9:

**Algorithm 2**: The extraction process

```
Data: CbW watermarked component
Result: W Watermark image
Cpt = 0;
for p = 0 → W.width do
    for q = 0 → W.height do
        Z = 0;
        for i = 1 → 4 do
            x = cpt Div CbW.width;
            y = cpt mod CbW.width;
            V = CbW[x,y];
            switch the value of i do
                case 1 value
                    M = 1; N=7; break;
                case 2 value
                    M = 2; N=5; break;
                end
                case 3 value
                    M=4; N=3; break;
                end
                case 4 value
                    M=1; N=7; break;
                end
            endsw
        Z = Z + ShiftL ((V & M), N);
        cpt = cpt + 1;
        i ← i + 1
    end
    cpt = cpt + 4;
    W[p,q] = Z;
    q ← q + 1
end
p ← p + 1
```
4. RESULTS AND DISCUSSION

The proposed technique is applied on the standard dataset RGB color images of 512 x 512 pixels namely, Lena, Baboon and Peppers as host images obtained from URL: http://sipi.usc.edu. Meanwhile, a grayscale image of UTM logo sized 128 x 256 pixels is used as the main watermark image, MW. Five different attacks viz. JPEG 2000, salt and pepper, speckle, Gaussian, and Poisson are also applied to measure the robustness.

4.1. Performance evaluation

Two measurements are used to evaluate the performances of the proposed method namely, the Peak Signal-to-Noise Ratio (PSNR) and Normalized Cross Correlation (NCC). The PSNR is used to measure the ratio of image quality between the original host image and watermarked image. PSNR value above 30 db is considered as the perceptual fidelity value [28]. The following formulae are used to calculate the PSNR value:

\[
PSNR = 10 \cdot \log_{10} \left( \frac{MAX^2_i}{MSE} \right) \\
= 20 \cdot \log_{10} \left( \frac{MAX_i}{\sqrt{MSE}} \right)
\]
\[ MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \]  

(3)

Where

\( m \) and \( n \) denote the image size of watermarked and host images; \( I(i,j) \) represents pixel\((i,j)\) value of host image; \( K(i,j) \) denotes pixel\((i,j)\) value of the watermarked image; and \( MAX \) denotes the image maximum intensity, which is usually equal to 255.

The NCC, on the other hand, is used to determine the quality of the watermarked image after the extraction [29,30], and is defined as:

\[ NCC = \frac{\sum_x \sum_y (W_{x,y} \times W'_{x,y})}{\sqrt{\sum_x \sum_y (W_{x,y})^2}} \]  

(4)

Where \( W_{x,y} \) is the pixel value of the original watermark image at \((x,y)\) coordinate, and \( W'_{x,y} \) is the pixel value of the extracted watermark image in the same position as that of the original watermark image.

4.2. Experimental results prior to attack

Table 1 and Fig. 10 to Fig. 12 illustrate the experimental results before the attack is taken place.

<table>
<thead>
<tr>
<th>Host Image</th>
<th>Watermark Image</th>
<th>PSNR</th>
<th>NCC of MW</th>
<th>NCC of SW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>UTM Logo</td>
<td>43.9866</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Lena</td>
<td>UTM Logo</td>
<td>46.6235</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Peppers</td>
<td>UTM Logo</td>
<td>45.5652</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Fig. 10: Baboon with UTM Logo

Fig. 11: Lena with UTM Logo

Fig. 12: Peppers with UTM Logo
4.3. Experimental results after attack insertion

Experimental results after insertion of the attacks are given in Table 2 to Table 6 below.

**Table 2: NCC values after JPEG 2000 attack**

<table>
<thead>
<tr>
<th>Host Image</th>
<th>(MW) (128X256)</th>
<th>(SW) (64X64)</th>
<th>NCC(MW)</th>
<th>NCC(SW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9443</td>
<td>1</td>
</tr>
<tr>
<td>Lena</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9465</td>
<td>1</td>
</tr>
<tr>
<td>Peppers</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9480</td>
<td>1</td>
</tr>
</tbody>
</table>

**Table 3: NCC values after Salt and Pepper attack**

<table>
<thead>
<tr>
<th>Host Image</th>
<th>(MW) (128X256)</th>
<th>(SW) (64X64)</th>
<th>NCC(MW)</th>
<th>NCC(SW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9790</td>
<td>0.9984</td>
</tr>
<tr>
<td>Lena</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9814</td>
<td>0.995</td>
</tr>
<tr>
<td>Peppers</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9734</td>
<td>0.9971</td>
</tr>
</tbody>
</table>

**Table 4: NCC values after Speckle attack**

<table>
<thead>
<tr>
<th>Host Image</th>
<th>(MW) (128X256)</th>
<th>(SW) (64X64)</th>
<th>NCC(MW)</th>
<th>NCC(SW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9373</td>
<td>0.9609</td>
</tr>
<tr>
<td>Lena</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9352</td>
<td>0.9432</td>
</tr>
<tr>
<td>Peppers</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9397</td>
<td>0.9633</td>
</tr>
</tbody>
</table>

**Table 5: NCC values after Gaussian attack**

<table>
<thead>
<tr>
<th>Host Image</th>
<th>(MW) (128X256)</th>
<th>(SW) (64X64)</th>
<th>NCC(MW)</th>
<th>NCC(SW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9417</td>
<td>0.9806</td>
</tr>
<tr>
<td>Lena</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9355</td>
<td>0.9871</td>
</tr>
<tr>
<td>Peppers</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9429</td>
<td>0.9868</td>
</tr>
</tbody>
</table>

**Table 6: NCC values after Poisson attack**

<table>
<thead>
<tr>
<th>Host Image</th>
<th>(MW) (128X256)</th>
<th>(SW) (64X64)</th>
<th>NCC(MW)</th>
<th>NCC(SW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baboon</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9395</td>
<td>1</td>
</tr>
<tr>
<td>Lena</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9330</td>
<td>1</td>
</tr>
<tr>
<td>Peppers</td>
<td>UTM Logo</td>
<td>Binary UTM Logo</td>
<td>0.9421</td>
<td>1</td>
</tr>
</tbody>
</table>

The above results revealed that average PSNR value of more than 45db was achieved, which is considered very high with respect to high capacity of the main watermark used. The results also showed that the NCC values prior to attack for the extracted watermarks MW and SW equaled 1.00, which indicates that the watermarks are not affected at all (i.e. identical with their original copies). In addition, when attacks were inserted, almost similar performance was achieved. This means that the proposed method has a strong robustness that can withstand all the prescribed attacks.
5. CONCLUSION

In this paper, a novel blind-based color image watermarking technique using the hybrid domain is proposed. The proposed technique takes into account imperceptibility, robustness and capacity, which are a vital aspect of effective watermarking. The high NCC and PSNR values obtained from the experiments show that the proposed approach which utilized the Cb and Cr components derived from YCbCr color space, and applied separately in spatial and transform domains, increases the imperceptibility, robustness and capacity. Its resilience against severe attacks such as JPEG 2000, salt and pepper, speckle, Gaussian, and Poisson is clearly evident.

ACKNOWLEDGEMENT

This research is funded by the Malaysian government through the Universiti Teknologi Malaysia’s GUP grant (Ref. No. UTM.J.13.01/25.10/3/03H7, Q.J130000.2528.03H70) that managed by the RMC UTM. The financial support and services rendered are really appreciated.

REFERENCE


BIOGRAPHY

Harith Raad Hasan was born in Aug, 20, 1980 Iraq. He received his M.Sc. Computer Science 2005 University of Al-Mustansiria, Baghdad .Iraq, B.Sc. Computer Science 2002 University of Al-Mustansiria, Baghdad .Iraq. Currently he is a Ph.D. student in Universiti of Technologi Malaysia (UTM), Johor, Malaysia. He is a member of the IEEE and the IEEE Computer Society. He is a reviewer in Digital Signal Processing (DSP).

Ghazali Bin Sulong received his BSc degree in statistics from National University of Malaysia, in 1979, and MSc and PhD in computing from University of Wales, Cardiff, United Kingdom, in 1982 and 1989, respectively. He is currently a professor at the Faculty of Computing, Universiti Teknologi Malaysia. His research interest includes Biometric - fingerprint identification, face recognition, iris verification, ear recognition, handwritten recognition, and writer identification; object recognition; medical image segmentation, enhancement and restoration; human activities recognition; data hiding - digital watermarking and steganography; image encryption; image compression; image fusion; image mining; digital image forensics; object detection, segmentation and tracking.

Ali Selamat has received a B.Sc. (Hons.) in IT from Teesside University, U.K. and M.Sc. in Distributed Multimedia Interactive Systems from Lancaster University, U.K. in 1997 and 1998, respectively. He has received a Dr. Eng. degree from Osaka Prefecture University, Japan in 2003. Currently, he is the Dean of Research Alliance in Knowledge Economy (K-Economy RA) UTM. He is a professor at Faculty of Computer Science & IS UTM. Previously he was an IT Manager at School of Graduate Studies (SPS), UTM. He is also a head of Software Engineering Research Group (SERG), K-Economy Research Alliance, UTM. He is the editors of International Journal of Digital Content Technology and its Applications (JDCTA) and International Journal of Advancements in Computing Technology (IJACT). His research interests include software engineering, software agents, web engineering, information retrievals, pattern recognitions, genetic algorithms, neural networks and soft-computing.