REVERSIBLE VISIBLE WATERMARK TECHNIQUE IN DCT COMPRESSED DOMAIN

Kazuki Minemura and KokSheik Wong

Faculty of Comp. Science & Info. Technology,
University of Malaya, Malaysia.
kazuki.minemura@gmail.com, koksheik@um.edu.my

ABSTRACT

Many watermark algorithms were proposed for protecting digital media from unauthorized use. Visible watermark scheme indicates the copyright of a digital media by embedding an inconspicuous but recognizable pattern into the media. However, the embedding process often results in serious distortion in the protected content, and the embedding process is not reversible. This paper proposes a reversible visible watermarking method for JPEG compressed image. A contrast adaptive strategy is proposed to maintain both transparency and recognizable sign. This method can also guarantee complete restoration and global protection. Experimental results show that the proposed method outperforms related methods in terms of quality preservation of the reconstructed image.

Index Terms—visible watermark, contrast-adaptive, transparency, JPEG, DCT

1. INTRODUCTION

Visible digital watermark techniques [1-8] have recently been utilized to protect multimedia content from unauthorized use. Although they are applied in different applications and possess the same importance, some of them are not completely reversible, i.e., the original multimedia content cannot be reconstructed from its watermarked counterpart. This paper proposes a novel solution for visible watermark mechanism in JPEG image that is completely reversible.

In this paper, our research focus on digital image because it is one of the mostly considered type of media in our daily life. For commercial consideration, valuable images are digitized and posted over the Internet by resource provider. Naturally, people can browse and download these media freely. Thus, protecting the digital media from illegal use is an important issue. Visible watermark mechanisms [1][2][3] are proposed to indicate the copyright of digital image by embedding an inconspicuous but recognizable logo into the image. The embedded visible watermark, however, can seriously distort the protected image. Thus, removable visible watermark (RVW) mechanisms are proposed to resolve this issue [4]. In addition to the prevention of unauthorized use, removable watermarking method allows authorized users to remove the visible watermark and reconstruct an unmarked version of the image with acceptable quality. Hu and Jeon proposed an improved method in which the embedded visible watermark (i.e., logo) can be completely removed [5]. Nevertheless, this visible watermark can only protect a local area of the image. It fails to satisfy the global protection requirement of a visible watermark mechanisms as stipulated in [6][7]. Mohanty proposed an adaptable visible watermarking method by classifying block in DCT (discrete cosine transform) domain [8]. Although it can survive unintentional modifications or malicious attacks, the method is irreversible.

The main concerns in designing an RVW mechanism are transparency and restoration [6][7]. Transparency focuses on how the strength of the watermark influences the perceptual quality of the host image. To obtain good perceptual translucency from a smooth test image, we must lower the strength of the watermark. On the other hand, to ensure visibility of the watermark in image of high spatial activity, we must increase the strength of the watermark, which may obscure the image. Restoration addresses the quality of the reconstructed image. Without loss of generality, the host image is seriously distorted after a visible logo is embedded into it. RVW methods must permit authorized users to restore watermarked images to an unmarked version with sufficiently high quality. Otherwise, the reconstructed image may become too severely distorted and hence of low (commercial) value.

Conventional methods considered crossed domain approach to realize removable visible watermarking in digital image. In particular, watermark is embedded based on the statistical features induced by the image in frequency domain while the final output is stored in spatial domain. In this work, we proposed a completely reversible watermarking method in JPEG compressed image that operates solely in the DCT domain. To ensure perfect restoration, we propose a contrast-adaptive strategy to consider strength of the watermark logo during embedding. In particular, the proposed scheme considers an adaptive weight that allows resource provider to adjust the strength of the watermark according to the visual requirement of the protected image. Experimental results show that the proposed scheme is more capable of restoring watermarked image to its original counterpart at...
higher visual quality when compared to the existing RVW methods considered.

2. JPEG COMPRESSION

A grayscale image is divided into non-overlapping blocks each of size 8 × 8 pixels and each block is transformed using the discrete cosine basis [9]. The coefficients are then quantized using the divisors determined by the quality factor. The quantized AC coefficients undergo zigzag ordering and entropy encoding. At the same time, the DC coefficients are predicted from their immediate left neighbors and the prediction errors are entropy coded. For the proposed method, we shall be focusing an the manipulation of the DC coefficients, where each of them encodes the average intensity of the block to which it belongs.

3. THE ESSENTIALS

The features and requirement of digital watermark are listed in [6][7]. In particular, the authors considered: (a) Restoration, (b) Transparency, (c) Global Protection, (d) Multiple Authorizations, and (e) Robustness. In this work, we consider the first three requirements.

4. EMBEDDING PROCEDURE

The proposed reversible visible watermarking method includes two subroutines: weight estimation and watermark embedding.

4.1. Weight Estimation Subroutine

Assume that the logo to be embedded (i.e., visible watermark) \( M \) is a binary image and let \( DC(m,n) \) denote the original DC value located at the \( (m,n) \)-th block for \( m = 1, 2, \ldots, M \) and \( n = 1, 2, \ldots, N \) for an image of dimension \( 8M \times 8N \) pixels. According to the requirements of RVW mechanisms, the embedded visible watermark should be as translucent as possible. In addition to ensuring that the visible watermark is recognizable, we aim at maintaining quality of the image to be protected. In particular, we follow a simple rule where we increase the strength (i.e., weight) of the watermark to highlight the logo in bright region and reduce the strength accordingly at dark region. We estimate the weight as follows:

Step 1: we compute the \( (m,n) \)-th DC coefficient value \( X \) and the mean value of its neighboring DC values \( \bar{X} \) as follows:

\[
X(m,n) = DC(2m,2n)
\]

\[
\bar{X}(m,n) = \frac{DC(2m-1,2n-1) + DC(2m,2n-1) + DC(2m-1,2n)}{3}
\]

Step 2: The integer difference \( d_{m,n} \) between the DC coefficient values \( X \) and \( \bar{X} \) is calculated as

\[
d_{m,n} = |X(m,n) - \bar{X}(m,n)|
\]

Step 3: We obtain the variance \( \sigma_{m,n} \) of the coefficient values \( X \) and \( \bar{X} \) by computing

\[
\sigma_{m,n} = \frac{d_{m,n} - d_{\min}}{d_{\max} - d_{\min}}
\]

where \( d_{\min} \) and \( d_{\max} \) are the minimum and maximum difference values among all \( d_{m,n} \)'s, respectively.

Step 4: The weight \( w_{m,n} \) for the watermark bit \( M_{m,n} \) is defined as

\[
w_{m,n} = w_u + w_v \times \sigma_{m,n}
\]

The secret value factor \( w_u \) adjusts the strength of the visible watermark by exploiting the human visual system (HVS) while \( w_v \) controls the strength of the significant texture (i.e. the variance \( d_{m,n} \)) of the host images.

4.2. Watermark Embedding Subroutine

Since the content energy of watermark \( M \) mainly gathers in the dark regions, we must highlight these regions of \( M \) in the watermarked image to emphasize its visibility. In our proposed method, we only embed the dark regions of \( M \) to protect copyright of the image. The bright regions shown in Fig. 2 (which posses less energy) are not embedded into the original image. Thus, we can reduce the number of alterations in the original image to preserve quality of the watermarked image while enhancing visibility of the watermark. Obeying the above concept, if a watermark bit \( M_{m,n} = 0 \), we employ the corresponding weight \( w_{m,n} \) to adjust the \( (m,n) \)-th and its neighboring DC coefficient values by the following equation:

\[
DC'(2m+i,2n+j) = DC(2m+i,2n+j) - w_{m,n} \text{ for } i, j \in \{0,1\}
\]

DC shows a DC coefficient which is limited between [-1024, 1023] in JPEG compression. Therefore \( w_u \) and \( w_v \) have to meet following equation.
These modified DC coefficients are utilized to generate the watermarked image. The resource provider therefore can issue $G'$ to the individual user along with the secret factors $w_u$ and $w_v$ and logo $M$. Moreover, to avoid unauthorized reconstruction of the original image, the secret parameters $w_u$ and $w_v$ can be encrypted by the individual user’s secret key prior to transmission. With weight $w_{m,n}$, the watermarked image $G'$ is capable of highlighting the energy of the watermark. Specifically, each weight is adjusted based on variance of each block strength (i.e., weight) of the image to be watermarked. That is, the perceptual quality of the watermarked image is sensitively adapted according to the watermark logo, feature of the host image, and user-defined $w_u$ and $w_v$.

5. EXPERIMENTAL RESULTS AND DISCUSSIONS

For RVW mechanisms, the greatest concerns are the transparency of the watermarked image and the quality of the restored image. In this section, we demonstrate the viability of the proposed method. In particular, we compare related well-known RVW schemes to the proposed method. Structural similarity (SSIM) [10] is utilized to measure the image quality of the watermarked and restored images with respect to the JPEG compressed unwatermarked image. The size of the test images and the visible watermark are $512 \times 512$ and $32 \times 32$ pixels, respectively. Ten standard test images (i.e., Airplane, Baboon, Elaine, House, Lake, Lenna, Milkdrop, Peppers, Sailboat and Tiffany) are considered to verify the basic performance of the proposed reversible visible watermarking method. The quality factor is set at 75.

5.1. Transparency Analysis

We examine the strength of the visible watermark in various test images. As shown in Fig. 3, when we set the secret factors to $w_u = 60$ and $w_v = 80$, transparency of the watermark logo is sufficient to maintain visible detail of the host image while protecting the image. That is, potential buyers can browse for the desired images since each host image is not seriously obscured. Using Airplane image as the representative example, we illustrate the effect of using different values of $w_u$ to generate a suitable watermarked image. Given a fixed $w_v$, we change the value of $w_u$ to adjust the strength of the watermark. As displayed in Fig. 4, the increase of $w_u$ results in a more visible watermark logo. Moreover, the transparency of the watermark is still acceptable for all values of $w_u$ considered. Furthermore, we adopt the secret factor $w_v$ in Eq.(5) to highlight the significant feature of the original image. That is, if the protected image is of high spatial activity (i.e., complex), then $w_v$ can be utilized to increase the strength of wa-
5.2. Analysis on Reversibility

In general, distortion of the restored image is often caused by the embedded watermark. The quality of the restored image is an important concern in evaluating a RVW mechanism. SSIM of value unity implies that a perfect reconstruction is achieved, and anything below unity signifies that there are some discrepancies between the original and the reconstructed images. As illustrated in Fig. 5, the SSIM value for all restored images for the proposed method is 1 after the watermark is removed. For our simulation with the value $w_u \in [20, 100]$ and $w_v = 80$, the proposed method always achieves perfect reconstructions. Fig. 6(b) and (c) present the watermarked image and reconstructed images, respectively, with $w_u = 60$ and $w_v = 80$. Compared with Fig. 6(a), the recovered image shown in Fig. 6(c) is exactly the same as the original image. This indicates that proposed method is capable of removing the embedded watermark logo such that the recovered image is completely identical to the original image. Therefore, the proposed scheme can realize perfect restoration.

5.3. Analysis on Robustness

The robustness of the proposed method against common watermark attacks is examined in this section. StirMark [11][12] has a variety of watermark attacks but the difference in visual appearance is most significant after applying the Median filter [3]. Since the embedded watermark is visible, it is able to withstand common attacks such as rotation, shearing, and resizing. For that, we only focus on the results of Median filter. Here, median filtering is carried out using window of size $3 \times 3$ pixels and $5 \times 5$ pixels in StirMark [11][12]. Due to space limitation, only the results for $5 \times 5$ are shown. Fig. 7 shows the watermarked image for $w_u \in \{20, 40, 60, 80\}$ and
$w_v = 80$ after filtering. These images still have outline of the embedded watermark logo. Similar results are observed for the case of $3 \times 3$ window. Therefore, the proposed method is robust against Median Filter.

5.4. Functional Comparison

Since the proposed method operates solely in the DCT domain, it is of lower complexity than any of the cross-domain approaches. The proposed method also requires less memory to operate since the operations are carried out on a block-by-block basis. Complete reversibility is an important feature in RVW method and the proposed method offers this feature. Table 1 compares the operational function between the proposed method and those of the existing methods. It observed that the proposed method offers more features than the existing methods considered.

6. CONCLUSIONS

A novel reversible visible watermarking method was proposed in the DCT compressed domain. DC coefficients were manipulated adaptively according to the watermark logo and the host image. Transparency and reversibility were simultaneously achieved. Simulation results showed that the proposed method outperforms the existing methods considered in terms of the reversibility.

To recover the original image from the watermarked counterpart without extra storage for side information will be the main focus of our future works. We also want to apply the proposed to video.

7. REFERENCES


### Table 1. Functionality comparison among related works

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Reversibility</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Transparency</td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Muti-Authorization</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>Underflow/Overflow</td>
<td>No/No</td>
<td>No/No</td>
<td>No/No</td>
<td>No/No</td>
</tr>
<tr>
<td>Global/Local Protection</td>
<td>Global</td>
<td>Local</td>
<td>Global</td>
<td>Global</td>
</tr>
<tr>
<td>Operating domain</td>
<td>DCT</td>
<td>Spatial</td>
<td>Cross</td>
<td>Cross</td>
</tr>
<tr>
<td>Output format</td>
<td>JPEG</td>
<td>RAW</td>
<td>RAW</td>
<td>RAW</td>
</tr>
</tbody>
</table>


