Abstract

For a multi-user-based watermarking system, a new scheme for providing the function of secret sharing is proposed. A user-key generating procedure is introduced to generate one master key and several normal keys. By using either of these normal keys, a secret watermark is obtained from the cover image. By referring to the original watermark and all the generated secret watermarks, a public watermark is created and embedded into the cover image. The proposed scheme does not require the original image to be presented during extracting. To reveal the genuine watermark from the watermarked image, except the super-user can extract it out directly by using the master key, the normal users who share the secret can only achieve it by presenting the shadow watermarks extracted by using their own keys.

1. Introduction

With the development and the popularity of the digital technology, some issues like copyright protection, tampering identification, ownership authority etc. are getting popularity nowadays. Among the techniques for solving the problems mentioned above, digital watermarking technology [1] is very popular where many researchers have been putting considerable amount of attention in recent years.

Although a variety of watermarking schemes have been proposed, few of them are focusing on the applications of sharing secrets with multi-users. Wang et al. [2] proposed a vector quantisation (VQ) [3] based watermarking scheme, which is the base of this paper, to introduce the concept of watermarking into a multi-user system.

In this paper, we propose another multi-user-based watermarking scheme with a hierarchical key design procedure. It generates several secret watermarks by quantifying the cover image and obtains a public watermark by referring to the original watermark and all the secret watermarks. The public watermark is embedded into the cover image by modifying the discrete cosine transform (DCT) coefficients of the cover image [4], and the watermarked image is then delivered to the related users to share the secret. Unlike the traditional secret sharing scheme, the proposed hierarchical key design provides the super user the power to obtain the secret directly by using the master key.

2. Secret and Public Watermarks

2.1. Secret Watermark Extraction

Let $X$ be a cover image, $C = \{c_i | 1 \leq i \leq L\}$ be a codebook with $L$ codewords therein (the dimension of the codeword is $k$), and $key = \{g_i \in [0,1] | 1 \leq i \leq L\}$ be a user key which defines the codewords in $C$ belong to either group-0 or group-1.

By using the key and the steps below, a secret watermark $W_s$ can be extracted out from the cover image $X$:

(i) Divide $X$ into $M$ non-overlapping blocks $\{x_1, x_2, \ldots, x_M\}$ with dimension $k$.

(ii) For each of the blocks, the nearest codeword search [3] is performed to obtain the nearest codeword from $C$.

(iii) Determine the groups where the obtained codewords are belonging by referring to $key$.

(iv) Collect the group information as $W_s$.

We summarize the above steps as:

$$W_s = f(X, key).$$

Here \( f_Q \) is the quantisation function, \( f_Q^{-1} \) is the inverse function of \( f_Q \), and \( W_S \) is the secret watermark associating with \( \text{key} \).

The examples of extracting secret watermarks from the image of Lena by using three different keys are shown in Figure 1.

\[ \text{key} = f_Q^{-1}(X, W_S). \]  
(2)

Figure 1. The extracted secret watermarks from the image of Lena by using three random-generated keys.

2.2. Public Watermark Generating

In order to share the original watermark with \( n \) users and to make the system securer, an encoding procedure for generating a public watermark is introduced. The public watermark is embedded into the cover image.

Let \( W \) be the original watermark and \( \{W_{S1}, W_{S2}, \ldots, W_{Sn}\} \) be the set of the obtained \( n \) secret watermarks while using \( \{\text{key}_1, \text{key}_2, \ldots, \text{key}_n\} \), respectively. A public watermark \( W_P \) can be generated by:

\[ W_P = (W + \sum_{i=1}^{n} W_{Si}) \mod 2. \]  
(3)

An example of generating the public watermark by referring to the three secret watermarks in Figure 1 and the original watermark in Figure 2 (a) is shown in Figure 2 (b).

Figure 2. (a) The original watermark and (b) the generated public watermarks.

3. Key Design

In our multi-user-based system, let \( \{\text{key}_1, \text{key}_2, \ldots, \text{key}_n\} \) be the set of \( n \) normal keys and \( \text{key}_0 \) be a master key. The normal keys can be defined or generated randomly by the users or by the key manager, but the master key can only be generated by the key manager while applying the proposed algorithm below.

Let \( \{W_{S0}, W_{S1}, W_{S2}, \ldots, W_{Sn}\} \) be the obtained secret watermarks while using \( \{\text{key}_0, \text{key}_1, \text{key}_2, \ldots, \text{key}_n\} \), respectively. Here due to the master key \( \text{key}_0 \) is still unknown, \( W_{S0} \) cannot be obtained. Thus, we define the relationship between \( W_{S0} \) and \( \{W_{S1}, W_{S2}, \ldots, W_{Sn}\} \) as:

\[ W_{S0} = (\sum_{i=1}^{n} W_{Si}) \mod 2. \]  
(4)

Using Equation (2), the master key \( \text{key}_0 \) can be obtained then.

4. Watermarking Scheme

In the proposed watermarking scheme, the hidden watermark can be extracted from the watermarked image directly without the need of the original image. By using the master key, the original watermark can be extracted out directly; otherwise, only a shadow watermark is extracted. A recovery procedure is introduced to recover the original watermark by combining all the shadow watermarks together.

4.1. Embedding Procedure

To embed the watermark into a cover image, the DCT-based watermarking algorithm proposed in [4] is employed. Figure 3 shows the block diagram and the steps of it are illustrated below briefly.

![Figure 3. The block diagram of the DCT-based watermark embedding procedure.](image)

For a given cover image \( X \), we first decompose it into \( N \) non-overlapping blocks with size 8x8. The DCT is then executed to all the blocks to generate the DCT coefficients. Here let \( Y \) denote the set of the transformed results of all blocks in \( X \), and \( Y = \{Y_1, Y_2, \ldots, Y_N\} \). The size of \( Y_i \) \((1 \leq i \leq N)\) is 64. The binary watermark \( W_P \) is also decomposed into \( N \) non-overlapping blocks with length \( p \) pixels. By referring to a user key \( K = \{K_1, K_2, \ldots, K_N\} \), where
For any $i \in [1, N]$, $p$ DCT coefficients can be selected from each block of $Y$ for embedding.

For the $j$-th ($1 \leq j \leq p$) bit of the $i$-th ($1 \leq i \leq N$) block in $W_p$ to be embedded into the corresponding block $Y_i$, the equations below are applied to adjust the DTC coefficients:

(i) If the bit is a bit-1, we have:

$$Y_i[K_j] = \begin{cases} Y_i[K_j] \times R[j] & \text{if } Y_i[K_j] \times R[j] \geq 0; \\ Y_i[K_j] + 1 & \text{otherwise.} \end{cases}$$  

Here $Y_i[0]$ is the DC value of the DCT coefficients of current block, $R$ is a reference table defined by the user, and $Y_i[K_j]$ is the $K_j$-th DTC coefficient which the watermark bit will be embedded within.

(ii) If the bit is a bit-0, then:

$$Y_i[K_j] = \begin{cases} Y_i[K_j] / R[j] & \text{if } Y_i[K_j] \times R[j] \geq 0; \\ Y_i[K_j] & \text{otherwise.} \end{cases}$$  

After all the watermark bits have been processed, the modified DCT blocks are collected as $Y'$, and the inverse DCT is executed to it to generated the watermarked image $X'$.

### 4.2. Extracting Procedure

In our watermarking system, to obtain an output watermark, the embedded public watermark and the user-key-based secret watermark have to be obtained firstly. A public watermark $\hat{W}_p$ can be extracted out from the watermarked image by inversing the embedding steps in Section 4.1 and by use of the equation below. The bits hidden in the related DCT coefficients are determined as 0 or 1:

$$Y_i[K_j] = \begin{cases} 1 & \text{if } Y_i[K_j] \times R[j] \geq Y_i[0]; \\ 0 & \text{otherwise.} \end{cases}$$  

Secondly, by applying the procedure in Section 2.1, a secret watermark $\hat{W}_s$ can be extracted out without any difficulty if a user key $key_i$ is presented. Then, the output watermark $\hat{W}_i$ is obtained by:

$$\hat{W}_i = (\hat{W}_p \oplus \hat{W}_s).$$  

Here if $key_i$ is a master key ($i=0$), then $\hat{W}_i$ will be the original watermark; otherwise, $\hat{W}_i$ will be a shadow watermark.

### 4.3. Watermark Recovery

To recover the original watermark from all the extracted shadow watermarks $\{\hat{W}_1, \hat{W}_2, ..., \hat{W}_r\}$, the method listed below is used:

$$\hat{W} = \begin{cases} (\sum_{i=1}^{r} \hat{W}_i) \mod 2, & \text{if } n \text{ is odd;} \\ (\hat{W}_p + \sum_{i=1}^{r} \hat{W}_i) \mod 2, & \text{if } n \text{ is even.} \end{cases}$$  

### 5. Simulation Results

In our experiments, the image of Lena and the image of Baboon were used as the cover images. The image shown in Figure 2(a) was used as the original watermark. The sizes of the cover images and the original watermark are $512 \times 512 \times 8$ bit/pixel and $128 \times 128 \times 1$ bit/pixel respectively. All the normal keys were generated randomly, and the settings of $n=3$, $k=16$, and $M=16384$ were used. Focusing on the popularity of transferring JPEG-format images via Internet, the JPEG compression with different quality factors (QF) was employed to test the robustness. In this paper, the peak signal to noise ratio (PSNR) and the bit correct ratio (BCR) [2] were employed to evaluate the quality of the watermarked results and the robustness of the system, respectively.

Table 1 lists the PSNR values while using different images as the cover images with different values of $L$. Table 2 and Table 3 list the extracted results under the JPEG attacks with different quality factors while using Lena and Baboon as the cover images respectively. Figure 5 shows the extracted results while applying JPEG with QF=50% to the watermarked image. Here the image of Lena was used as the cover image and $L=64$.  

![Figure 4. The block diagram of the watermark extracting procedure.](image-url)
Table 1. PSNR values of the test results.

<table>
<thead>
<tr>
<th></th>
<th>L=32</th>
<th>L=64</th>
<th>L=128</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>33.03 dB</td>
<td>32.86 dB</td>
<td>33.02 dB</td>
</tr>
<tr>
<td>Baboon</td>
<td>26.53 dB</td>
<td>26.54 dB</td>
<td>26.50 dB</td>
</tr>
</tbody>
</table>

Table 2. BCR values of the test results while using Lena as the cover image.

<table>
<thead>
<tr>
<th></th>
<th>L=32</th>
<th>L=64</th>
<th>L=128</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG (Q=30%)</td>
<td>89.75%</td>
<td>84.95%</td>
<td>78.57%</td>
</tr>
<tr>
<td>JPEG (Q=50%)</td>
<td>94.32%</td>
<td>90.73%</td>
<td>86.99%</td>
</tr>
<tr>
<td>JPEG (Q=70%)</td>
<td>93.73%</td>
<td>89.54%</td>
<td>84.77%</td>
</tr>
</tbody>
</table>

Table 3. BCR values of the test results while using Baboon as the cover image.

<table>
<thead>
<tr>
<th></th>
<th>L=32</th>
<th>L=64</th>
<th>L=128</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPEG (Q=30%)</td>
<td>86.17%</td>
<td>79.63%</td>
<td>74.66%</td>
</tr>
<tr>
<td>JPEG (Q=50%)</td>
<td>90.39%</td>
<td>85.50%</td>
<td>81.59%</td>
</tr>
<tr>
<td>JPEG (Q=70%)</td>
<td>89.94%</td>
<td>84.78%</td>
<td>80.54%</td>
</tr>
</tbody>
</table>

Figure 5. The extracted watermarks: (a) public watermark, (b) watermark 1 while using $key_1$, (c) watermark 2 while using $key_2$, (d) watermark 3 while using $key_3$, (e) watermark while using the master key $key_0$, and (f) the reconstructed watermark.

6. Discussion

Some issues which affect the performance or relate to the scheme are listed below:

(i) From Table 2 and Table 3, we observe that a smaller value of $L$, which means a larger degree of quantisation, leads to stronger robustness.

(ii) The security of our system is linked to the length of the key (which is $L$), the $K$ for choosing which DCT coefficients for embedding, and the reference table $R$.

(iii) Due to the method of generating the secret watermark, the value of $L$ affects the encoding and decoding time of the system.

(iv) In some cases, although the issue of key delivery is concerned, it is beyond the focus of this paper.

7. Conclusion

In this paper, for sharing secrets with multi-users, a new watermarking scheme with hierarchical key design is proposed. The user in the first-class level can extract out the genuine watermark directly using the master key. In the second-class level, the users who share the same secret can only obtain the original watermark while the extracted shadow watermarks are presented. Unlike some schemes to embed all the shadow watermarks into the cover image, the proposed scheme only embeds one, which provide better perceptible quality. The robustness under the JPEG attacks is good enough even a high compression rate (quality factor is 30%) is occurred.

In conclusion, the proposed method is novel and useful, and to introduce the use of different level of keys into the watermarking system is the main contribution of this paper.

References


