A Survey of Digital Image Watermarking Based on different Techniques

Rashel Sarkar¹, Sameema²

¹Assistant Professor, Dept. of Computer Science and Engg, P.A. College of Engineering, Mangalore
²Lecturer, Dept. of Information Science and Engg, P.A. College of Engineering, Mangalore

Abstract-- Digital watermarking is the process that embeds data called a watermark into a multimedia object such that the watermark can be detected or extracted later to make an assertion about the object. Several software implementations of the proposed algorithms are available, but very few attempts have been made for protecting intellectual property. Embedded watermark will allow identifying the owner of work hardware implementation. This concept is applicable to digital video and audio also.

The goal of this implementation is to survey the different techniques for Digital Watermarking.


I. INTRODUCTION

The earliest forms of information hiding can actually be considered to be highly crude forms of private-key cryptography, the “key” in this case being the knowledge of the method being employed (security through obscurity). Today, crypto-graphical techniques have reached a level of sophistication such that properly encrypted communications can be assumed secure well beyond the useful life of the information transmitted. In fact, it’s projected that the most powerful algorithms using multi kilobit key lengths could not be comprised through brute force, even if all the computing power worldwide for the next 20 years was focused on the attack. Of course the possibility exists that vulnerabilities could be found, or computing power breakthroughs could occur, but for most users in most applications, current cryptographic techniques are generally sufficient. Why then pursue the field of information hiding? Several good reasons exist, the first being that “security through obscurity” isn’t necessarily a bad thing, provided that it isn’t the only security mechanism employed. Steganography for instance allows us to hide encrypted messages in mediums less likely to attract attention. This becomes particularly important as the technological disparity between individuals and organizations grows. Governments and businesses typically have access to more powerful systems and better encryption algorithms then individuals.

Hence, the chance of Individual’s messages being broken increases which each passing year. Reducing the number of messages intercepted by the organizations as suspect will certainly help to improve privacy. This paper will begin with a quick background on cryptography and steganography, which form the basis for a large number of digital watermarking concepts. The paper will then move on to a discussion of what requirements a watermarking system must meet, as well as methods for evaluating the strengths of various algorithms. The remainder of the paper will focus on various watermarking techniques and the strengths and weaknesses of each. This paper will focus almost exclusively on the watermarking of digital images; however most of these same ideas could easily be applied to the watermarking of digital video and audio.

II. BACKGROUND

First we start with a few definitions. Cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. Through the use of a “key” the receiver can decode the encrypted message (decrypting) to retrieve the original message.

Steganography improves on this by hiding the fact that a communication even occurred. The message m is imbedded into a harmless message c which is defined as the cover-object. The message m is then embedded into c, generally with use of a key k that is defined as the stego-key. The resulting message is then embedded into the cover-object c, which results in stego-objects, ideally the stego-object is indistinguishable from the original message c, appearing as if no other information has been encoded. This can all be seen below in figure 2.1.
Watermarking is very similar to steganography in a number of respects. Both seek to embed information inside a cover message with little to no degradation of the cover-object. Watermarking however adds the additional requirement of robustness. An ideal steganographic system would embed a large amount of information, perfectly securely with no visible degradation to the cover object. An ideal watermarking system however would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness.

III. CHOICE OF WATERMARK-OBJECT

The first question we need to ask with any watermarking or stenographic system, is what form will the embedded message take? The most straightforward approach would be to embed text strings into an image, allowing an image to directly carry information such as author, title, date and so forth. The drawback however to this approach is that ASCII text in a way can be considered to be a form of LZW compression, which each letter being represented with a certain pattern of bits. By compressing the watermark-object before insertion, robustness suffers.

Due to the nature of ASCII codes, a single bit error due to an attack can entirely change the meaning of that character, and thus the message. It would be quite easy for even a simple task such as JPEG compression to reduce a copyright string to a random collection of characters. Rather then characters, why not embed the information in an already highly redundant form, such as a raster image? Not only do images lend themselves to image watermarking applications, but the properties of the HVS can easily be exploited in recognition of a degraded watermark.

IV. VARIOUS WATERMARKING TECHNIQUES

• Least Significant Bit Modification (LSB)

The most straightforward Watermarking technique is to embed the watermark image into the least-significant-bits of the cover object [3]. Given the extraordinarily high channel capacity of using the entire cover image for transmission in this technique, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark would be considered a success.

LSB substitution however despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. Furthermore, once the algorithm is implemented, the embedded watermark could be easily modified by an intermediate party.

An improvement on basic LSB substitution would be to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given “seed” or key [4]. LSB modification proves to be a simple and fairly powerful tool for stenography, however lacks the basic robustness that watermarking applications require.

• Correlation Technique

The correlation watermarking technique for watermark embedded is to exploit the correlation properties of additive pseudo-random noise patterns as applied to a cover image [5]. A pseudo-random noise (PN) pattern W(x, y) is added to the cover image I(x, y), according to the Equation (1) given below:

\[ I_w(x, y) = I(x, y) + k \ast W(x, y) \]  

In Equation 1, k denotes a gain factor, and Iw the resulting watermarked image. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image. To retrieve the watermark image, the same pseudo-random noise key is used and the correlation between the noise pattern and the promising watermarked image is computed. If the correlation exceeds a certain threshold (T), the watermark is detected, and a single bit is set. This technique can easily be extended to multiple-bit watermark by dividing the image up into blocks, and performing the above procedure independently on each block [6].

• Common Division Multiple Access (CDMA)

In CDMA Watermarking technique, pseudo-random sequence is embedded as a watermark into the transform coefficients of the cover image. CDMA technology provides multiple access multiplexing, possesses large capacity and strong anti-interference capability. CDMA used in digital watermarking technology increases the watermark embedding capacity and also enhance the watermark robustness [7].

• Discrete-Cosine-Transform (DCT)

The classic and still most popular technique in Frequency domain is Discrete-Cosine-Transform (DCT1).
The DCT1 allows an image to be broken up into different frequency bands, making it much easier to embed Watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they do not have important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies) [9]. One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. The middle-band frequencies ($F_M$) of an 8x8 DCT block as shown in Figure 4.1.

**Figure 4.1 Definitions of DCT Regions [9]**

- **DCT2**

DCT2 is a Comparison-Based technique where correlation is performed on mid-band frequency of cover image using two PN sequences one for "0" and another for "1" for Watermarking. Next two locations $B_i(u_1, v_1)$ and $B_j(u_2, v_2)$, are chosen from the $F_M$ region for comparison [11]. Rather than arbitrarily choosing these locations, extra robustness to compression can be achieved if the choice of coefficients on the recommended image is quantized as shown in Table 1. If two locations are chosen such that they have identically quantized values, then scaling of one coefficient is performed while the other one is also scaled by the same factor preserving their relative size.

<table>
<thead>
<tr>
<th>$F_M$</th>
<th>$F_L$</th>
<th>$F_H$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Based on the Table 1, the coefficients (4, 1) and (3, 1) or (2, 1) and (2, 2) make suitable comparison as their quantization values are equal. The block encodes a “1” if $B_i(u_1, v_1) > B_j(u_2, v_2)$; otherwise “0” is encoded. The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [11].

The swapping of such coefficients will not alter the watermarked image as it is generally believed that DCT coefficients of middle frequencies have similar magnitudes. The robustness of the watermarked image is improved by adding a watermark “strength” constant ‘$k$’, such that $B_i(u_1,v_1) - B_j(u_2,v_2) > k$. Coefficients that do not meet this criteria are modified by using the random noise to satisfy the relation. Increasing $k$ thus reduces the chance of detecting errors at the expense of additional image degradation [12].

Another possible technique is to embed a PN sequence ($W$) into the middle frequencies of the DCT block. The given DCT block ($x$, $y$) is modulated by using the Equation (2) as shown below:

$$I_{w,x,y}(u,v) = \begin{cases} 
I_{x,y}(u,v) + k \ast W_{x,y}(u,v), & u,v \in F_M \\
I_{x,y}(u,v), & u,v \notin F_M 
\end{cases} \quad (2)$$

For each block ($x$, $y$) of the image, the DCT for the block is first calculated. In that block, the middle frequency components $F_M$ are added to the PN sequence ($W$), multiplied by a gain factor ($k$). Coefficients in the low and middle frequencies are copied over to the transformed image unaffected. Each block is then inverse-transformed to give final watermarked image [13].

<table>
<thead>
<tr>
<th>16</th>
<th>11</th>
<th>10</th>
<th>16</th>
<th>24</th>
<th>40</th>
<th>51</th>
<th>61</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>12</td>
<td>19</td>
<td>26</td>
<td>58</td>
<td>60</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>13</td>
<td>24</td>
<td>40</td>
<td>57</td>
<td>69</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>17</td>
<td>22</td>
<td>29</td>
<td>51</td>
<td>87</td>
<td>80</td>
<td>62</td>
</tr>
<tr>
<td>18</td>
<td>22</td>
<td>37</td>
<td>56</td>
<td>68</td>
<td>109</td>
<td>103</td>
<td>77</td>
</tr>
<tr>
<td>24</td>
<td>35</td>
<td>55</td>
<td>64</td>
<td>81</td>
<td>104</td>
<td>113</td>
<td>92</td>
</tr>
<tr>
<td>49</td>
<td>64</td>
<td>78</td>
<td>87</td>
<td>103</td>
<td>121</td>
<td>120</td>
<td>101</td>
</tr>
</tbody>
</table>

Table 1 Quantization values used in compression scheme [11].
The watermarking procedure becomes more adaptive by slightly altering the embedding process to the method shown in Equation 3.

$$I_{w,u,v}(u,v) = \begin{cases} I_{x,u,v} + \alpha |W_i|, & u,v \in HL, LH \\ 0, & otherwise \end{cases}$$

(3)

The slight modification scales the strength of the watermarking based on the size of the particular coefficients being used. Larger $k$'s can thus be used for coefficients of higher magnitude in effect strengthening the watermark in regions that it can afford.

To detect the watermark, the image is broken up into same number of blocks and Discrete Cosine Transformation is performed on these blocks. The same PN sequence is then compared to the middle frequency values of the transformed block. If the correlation between the sequences exceeds some threshold (T), “1” is detected for that block; otherwise “0” is detected. Again $k$ denotes the strength of the watermarking, where increasing $k$ increases the robustness of the watermark at the expense of quality [12].

- **Discrete Wavelet Transform (DWT)**

Another possible domain for watermark embedding is that of the wavelet domain. The Discrete Wavelet Transform (DWT) separates a cover image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated for multiple “scale” wavelet decomposition, as in the 2 scale wavelet transform shown below in Figure 4.2

Human Vision System appreciates the Watermark image recovered by DWT as compared to DCT. DWT allows higher energy watermarks in regions that the Human Vision System (HVS) is known to be less sensitive to, such as the high resolution detail bands (LH, HL, HH). Embedding watermarks in these regions increases the robustness of watermarked image, with little or no additional impact on image quality [14]. The similar embedding technique can be used in the DCT [16], the embedding of a CDMA sequence in the detail bands is given according to the Equation 4.

$$I_{w,u,v} = \begin{cases} W_i + \alpha |W_i| x_i, & u,v \in HL, LH \\ W_i, & u,v \in LL, HH \end{cases}$$

(4)

Where $W_i$ denotes the coefficient of the transformed image, $x_i$ the bit of the watermark to be embedded, and $\alpha$ is the scaling factor. To detect the watermark image, the same pseudo-random sequence is generated and its correlation with the two transformed detail bands is determined. If the correlation exceeds some threshold $T$, the watermark is detected. It can be easily extended to multiple bit messages by embedding multiple watermarks into the image. As in the spatial version, a separate seed is used for each PN sequence, which is then added to the detail coefficients as per Equation (4). During detection, if the correlation exceeds (T) for a particular sequence “1” is recovered; otherwise “0”. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered [13].

V. CONCLUSION

This study has introduced a number of techniques for the watermarking of digital images, as well as touching on the limitations and possibilities of each. Although only the very surface of the field was scratched, it was still enough to draw several conclusions about digital watermarking.

LSB substitution is not a very good candidate for digital watermarking due to its lack of even a minimal level of robustness. LSB embedded watermarks can easily be removed using techniques that do not visually degrade the image to the point of being noticeable. Furthermore if one of the more trivial embedding algorithms is used, the encoded message can be easily recovered and even altered by a 3rd party.

Another observation is that transform domains are typically better candidates for watermarking than spatial, for both reasons of robustness as well as visual impact.
Embedding in the DCT domain proved to be highly resistant to JPEG compression as well as significant amounts of random noise. We were able to produce a watermarking technique with moderate robustness, good capacity, and low visual impact. This holds true in general for watermarking; robustness can be improved significantly when the subsequent degradation techniques are known. This holds particularly true in the case of compression techniques, where the compression algorithms are well known.

The wavelet domain as well proved to be highly resistant to both compression and noise, with minimal amounts of visual degradation. This is all the more impressive when one considers that the wavelet technique described here is one of the most primitive currently known. More sophisticated wavelet-domain techniques will almost certainly improve on both of these, and hopefully lower its computational requirements. The wavelet domain may be one of the most promising domains for digital watermarking yet found.

Although not discussed here, the counters proposed to these attacks typically rely on discovering the exact rotation, or shifting used in the attack, and then transforming the image back into its pre-attack state. Typically these techniques are computationally pricey, and unpredictable. This remains one of the major problems in the development of robust digital watermarking for digital images.

REFERENCES


