A New Approach Dual watermarking in digital image through sub-sampling technique and its simulation

Smita kumari¹, Vimal Shukla², Ramji Gupta³

¹ M.Tech. Scholar, Computer Science Engineering, KNP Institute, M.P., India
² Assistant Professor, Computer Science Engineering, KNP Institute, M.P., India
³ Research Scholar, Electronics & Communication Engineering, MANIT, M.P., India

Abstract
This paper presents a novel dual watermarking mechanism for digital media that embeds a recognizable pattern into the spatial domain and an invisible logo into the frequency domain. Undoubtedly, visible watermarking is important for protecting online resources from unauthorized reproduction. Due to the visibility of embedded patterns, however, watermarked digital media are vulnerable to the inpainting attack and common signal processing operations. Utilizing hybrid strategies, the images can be made immune to these attacks. In particular, the new mechanism allows legal subscribers to restore an unmarked image, whereas other dual watermarking schemes do not. This feature makes it suitable for protecting artistic and valuable media.

Key Words: Dual watermarking, spatial domain, frequency domain.

1. INTRODUCTION

The internet is an excellent distribution system for the digital media because of its inexpensiveness and efficiency. The enormous popularity of the World Wide Web in the early 1990's demonstrated the commercial potential of offering multimedia resources through the digital networks. The digital images can be readily shared, easily used, processed and transmitted for the commercial purpose, which causes serious problems such as unauthorized use and manipulation of digital content. As a result, there is a need for authentication techniques to secure digital images. Since commercial interests seek to use the digital networks to offer digital media for profit, they have a strong interest in protecting their ownership rights. Digital watermarking has been proposed as one way to accomplish this [2].

Digital watermarking is a technique which embeds additional information into the digital content in order to secure it. A digital watermark is a digital signal or pattern inserted into a digital image that can be detected or extracted later to make some affirmation about the host image. Since this signal or pattern is present in each unaltered copy of the original image, the digital watermark may also serve as a digital signature for the copies[3],[4]. A given watermark may be unique to each copy (e.g. to identify the intended recipient), or be common to multiple copies (e.g. to identify the document source). In either case, the watermarking of the document involves the transformation of the original into another form. This distinguishes digital watermarking from digital fingerprinting, where the original file remains intact and a new created file 'describes' the original file's content. Digital watermarking is also to be contrasted with public-key encryption, which also transform original files into another form. It is a common practice nowadays to encrypt digital documents so that they become unviewable without the decryption key. Unlike encryption, however, digital watermarking leaves the original image (or file) basically intact and recognizable. In addition, digital watermarks, as signatures, may not be validated without special software. Further, decrypted documents are free of any residual effects of encryption, whereas digital watermarks are designed to be persistent in viewing, printing, or subsequent re-transmission or dissemination [5].

1.1 Elements of Watermarking System

A watermarking system can be viewed as a communication system consisting of three main elements: an embedder, a communication channel and a detector. Watermark information is embedded into the signal itself, instead of being placed in the header of a file or using encryption like in other security techniques, in such a way that it is extractable by the detector. To be more specific, the watermark information is embedded within the host signal before the watermarked signal is transmitted over the communication channel, so that the watermark can be detected at the receiving end, that is, at the detector [11].

A general watermarking system is illustrated in Fig. 1.1 the dotted lines represent the optional components, which may or may not be required according to the application. First of all, a watermark \( W_o \) is generated by the watermark generator possibly with a secret watermark generation key \( K_o \). The watermark \( W_o \) can be a logo, or be a pseudo-random signal. Instead of directly embedding it into the host signal, the watermark \( W_o \) can be pre-coded to optimize the embedding process, i.e. to increase robustness against possible signal processing operations or imperceptibility of the watermark. This is done by an information coder which may require the original signal \( S_o \). The outcome of the information...
coding component is denoted by symbol $W$ that, together with the original signal $S_o$ and possibly a secret key $K$, are taken as input of the embedder. The secret key $K$ is intended to differentiate between authorized users and unauthorized users at the detector in the absence of $K_g$. The embedder takes in $W$, $S_o$ and $K$, so as to hide $W$ within $S_o$ in a most imperceptible way with the help of $K$, and produce the Watermarked signal $S_w$. Afterwards, $S_w$ enters into the communication channel where a series of unknown signal processing operations and attacks may take place. The outcome of the communication channel is denoted by the symbol $S'_w$. At the receiving end, the detector works in an inversely similar way as the embedder, and it may require the secret key $K_g$, $K$, and the original signal $S_o$. Then the detector reads $S'_w$ and decides if the received signal has the legal watermark [7][8].

2. WATERMARKING INSERTION

The dual watermarking approach embeds the removable watermarks in both the spatial and frequency domain of the subsampled host image. The visible watermark indicates the ownership of the protected image through visual perception[9]. Even if the visible watermarked image incurs tampering, we can retrieve the invisible watermark to prove the copyright of the image. Only an authorized user can remove the dual watermark to obtain an unmarked image with high fidelity. Fig 2.1 presents and overview of the proposed dual scheme. Take that the protected image $O$ is a grayscale image with $N \times N$ pixels. Let $M_f$ and $M_s$ be the binary logo images that will be embedded in frequency and spatial domains respectively.

**Step 1:**
First apply the sub sampling technique to the host image $O$ for obtaining four sub images $O_1$ $O_2$ $O_3$ $O_4$ with $N/2 \times N/2$ pixels according to the following algorithm. By this sub-sampling technique we will get 4 sub-images, which are highly correlated, and the slight variation among those figures cannot be perceptible.

**Step 2:**
Resize the spatial domain logo $M_s$ exactly to the size of $N/2 \times N/2$ according the dimension of the sub images. And make it a binary image, in order to make the value of every pixel either 0 or 1. By making the value either 0 or 1, it becomes easy to insert the watermark image in the host image. The spatial domain logo to be inserted into the host image is displayed in the figure 2.2

**Step 3:**
Select a weight matrix $W$ for inserting the spatial domain binary logo into the sub images of size 1*4 $W$ = [w1 w2 w3 w4]

**Step 4:**
Only the dark pixels of the binary logo are used to insert the watermark, so that the host image is less modified and the processing time for the insertion will be less.

**Step 5:**
Resize the frequency domain watermark logo $M_f$ according to the spatial domain logo $M_s$, so that the insertion of these logos will not be overlapped, and make $M_f$ a binary image. As mentioned above that the dark pixels of the spatial domain logo are embedded to the host image, so in order to ward off any overlapping of both logo, first identify the left-top most dark pixel of the spatial domain logo. Then according to that dimension adjust dimension of the frequency domain logo. The figure 2.3 shows the frequency domain watermark logo.

![SMITA](https://via.placeholder.com/150)

**Fig -2.1:** A general watermarking system

![KNP](https://via.placeholder.com/150)

**Fig -2.2:** Spatial Domain Logo To Be Inserted

![SMITA](https://via.placeholder.com/150)

**Fig -2.3:** Frequency Domain Logo To Be Inserted
Step 6:
For the insertion of the invisible watermark, choose two sub-images randomly, and transform those into frequency domain by the help of discrete cosine transform (DCT). Choose a suitable value for the watermark weight. And insert the invisible watermark according to the following algorithm. Here the value of watermark weight is taken as 15, in order to make a suitable balance between the two conflicting requirement of perceptual quality and robustness. Then transform those sub-images back into spatial domain. Simultaneously the watermark can be inserted in the other two sub images. This insertion of dual watermark will be according to the schematic diagram of fig 2.4. Here the sub-image 1 and 2 has been chosen for the watermark insertion.

![Schematic of Insertion of Dual Watermarking](image)

**Fig 2.4: Schematic of Insertion of Dual Watermarking.**

Step 7:
Do the reverse sub-sampling process to merge all the four watermarked sub-images. Now we get the dual watermarked image.

3. WATERMARKING EXTRACTION

Step 1:
First apply the sub sampling technique to the watermarked image O’ for obtaining four sub images O’1 O’2 O’3 O’3 with N/2*N/2 pixels according to the following algorithm.

Step 2:
The dimension of the spatial domain logo and frequency domain logo has been calculated in the same manner, as calculated at the time of insertion.

Step 3:
Only the authenticated user of image can extract the spatial domain logo, because only he has the access to the secret weight matrix W[w1 w2 w3 w4].

Step 4:
Only the authenticated user knows the random way in which the frequency domain logo has been inserted at the time watermark insertion. By taking the two sub-images in which the logo has been inserted at the time of watermark embedding, and taking the discrete cosine transform (DCT). The watermark weight is known to the authorized user only. The value of watermark must be same as it was at the time of insertion. Otherwise the frequency domain logo cannot be removed.

Step 5:
Now bye doing the reverse sub-sampling process we will get the original image, with a acceptable level of error. Here the error comes due the assumption that the four sub-images are highly correlated. But in fact there are some deviations. So at the time of extraction of frequency domain logo the difference of pixel value will not be zero where the watermark is not inserted, instead a low value comes. And another reason is the imperfection of the processing system, and due to the noise also the error comes.

Step 6:
By subtracting the recovered image from the original image the error can be calculated. Generally the error is displayed in percentage. So the resultant image must have all the pixel value zero, and any deviation from that regarded as error. then percentage of error should be calculated.

4. RESULT

The algorithm explained above is applied on different images and simulated on MATLAB. The simulation results are summarized in table 1. In which error pixel results are shown for different images after applying dual digital watermarking and then watermarking extraction on receiver end. Results are calculated from input images and recovered image. The average error is 2.98, and which is acceptable range. Image1 and Image2 are shown in figures from 4.1 to 4.6 with recovered images.

![Original Image 1](image)

**Fig 4.1: Original Image 1**
5. CONCLUSIONS

The dual watermarking mechanism is practical for advanced protection of the ownership of multimedia over the Internet. The new scheme utilizes visible and invisible watermarking to provide visual ownership identification and to achieve the robustness requirement. Furthermore, the removability of the proposed scheme is promising to preserve valuable images with high fidelity. Even if someone knows the algorithm through which the watermark has been inserted, still the watermark cannot be removed without knowing the weight coefficients matrix for the spatial domain and the weight coefficient for the frequency domain, which is provided to the authorized user only.

Table 1: Error table for simulation result

<table>
<thead>
<tr>
<th>Images</th>
<th>Percentage of error at weight coefficient W=[0.2 0.2 0.3 0.3]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image1</td>
<td>2.9236</td>
</tr>
<tr>
<td>Image2</td>
<td>2.7754</td>
</tr>
<tr>
<td>Image3</td>
<td>3.0349</td>
</tr>
<tr>
<td>Image4</td>
<td>3.1094</td>
</tr>
<tr>
<td>Image5</td>
<td>3.0301</td>
</tr>
<tr>
<td>Image6</td>
<td>2.9970</td>
</tr>
<tr>
<td>Image7</td>
<td>3.0023</td>
</tr>
</tbody>
</table>

REFERENCES


