A Method for Watermark Casting on Digital Images
By Ioannis Pitas

Presenters:
Jeremy Stout
Lin Zhiang

CS 591K: Multimedia Systems
November 21, 2002
What is a Digital Watermark?

A digital watermark is a signal, usually an image or pixel pattern, which is superimposed over another image. This allows the owner of a digital image to mark it in a usually nonperceptible manner.
The Four Demands of Digital Watermarking

1. The visual perception of the image should remain unaltered, and the watermark unnoticed.

2. We are in a position to detect a certain digital watermark by examining the alterations made by the superposition.

3. A great number of different watermarks, all distinguishable from each other, can be produced.

4. Distortion or removal of the digital watermark through general image operations and manipulation should be extremely difficult, or impossible.
Uses of Watermarking

- Copyright Enforcement
- Authenticity Checking
- Protection against copying and retransmission.
- Many Others…
A Method for Watermarking

For a digital image, watermarking is applied either in the frequency or spatial domain. The method that is about to be described in this article is based on statistical detection theory, and it is applied in the spatial domain.
A digital watermark $S$ is a specific binary pattern of size $N \times M$ where the number of "ones" equals the number of

$$S = \{ s_{nm}, \, n \in \{0, 1, \ldots, N-1\}, \, m \in \{0, 1, \ldots, M-1\} \}$$

where $s_{nm} \in \{0, 1\}$
Splitting Image $I$ into Subsets

By using $S$, we can split $I$ into two subsets of equal size.

Remember that:
$I = \{x_{nm}, \ n \in \{0, 1, \ldots, N - 1\}, \ m \in \{0, 1, \ldots, M - 1\}\}$

where $x_{nm} \in \{0, 1, \ldots, L - 1\}$ is the intensity level of $nm$ and $L$ is the total number of intensity levels.

By using $S$ as follows, we get the following two sets:

$A = \{x_{nm} \in I, \ s_{nm} = 1\}$ \quad and \quad $B = \{x_{nm} \in I, \ s_{nm} = 0\}$
Obtaining the Watermarked Image:

Each of the subsets, A and B, contain N x M / 2 pixels and \( I = A \cup B \).

The digital watermark is superimposed by changing the elements of the subset A by the positive factor k:

\[ C = \{ x_{nm} + k, \ x_{nm} \in A \} \]

The watermarked image is given by

\[ I_a = C \cup B \]
Satisfaction of Basic Demands

1. **Imperceptibility of the Watermark**
The quantity $k$ that is added to the pixel $x_{nm} \in A$ to produce set $C$ is sufficiently small that the ratio $k/x_{nm}$ remains small and its visual perception is negligible.

2. **Detection of the Watermark**
It is desired that sets $C$ and $B$ being intermixed as much as possible with the expectation of giving better results. The following will describe how a person can detect a watermark after intermixing.
Watermark Detection Process

Let \( w = c - b \) where \( w \) is the difference of the means.

This will allows us to obtain our test statistic:

\[
q = \frac{w}{\sigma_w}
\]

where

\[
\sigma_w = \frac{s_c^2 + s_b^2}{P}
\]

and

\[
P = \frac{(N \times M)}{2}
\]
Depending on the value $w$ has, different plots will be taken on by $q$. This will help us in detecting the watermark. Here is a plot of $q$. 

![Diagram showing two normal distributions with shaded areas indicating signature existence or non-existence. The distributions are labeled with critical values $t_{1-\alpha}$ and $k/\hat{\sigma}_w$.](image)
As seen above, the two graphs overlap and errors can be introduced when attempting to detect a watermark. Thus, a watermark can only be detected with some degree of certainty.

The interval that will minimize the errors from the overlap is given by:

\[ t_{1-\alpha} = \frac{k}{2\sigma_w} \]

To detect the watermark, \( w \) must first be calculated and then \( \sigma_w \). We then obtain \( q \) and test it against \( t_{1-\alpha} \). If \( q < t_{1-\alpha} \), then there is no watermark, else, there is one. This is based on looking at the graphs.
Number of Different Possible Watermarks

Since the watermark for a digital image in this method is the same size as the image, this means that the number of watermarks that can be applied on an image of size \( N \times M = 2P \) equals the number of ways \( P \) can be selected out of \( 2P \) items. Thus, the number of watermarks \( N_s \) is given by:

\[
N_s = \binom{2P}{P} = \frac{2P!}{(P!)^2} \approx \frac{2^{2P}}{\text{Square Root}(\pi \times P)}
\]

(This is based on Stirling’s Formula)

For example, a 32 x 32 (\( P = 512 \)) image can have as many as \( 4.48 \times 10^{300} \) different watermarks applied to it.
Immunity to Subsampling

One form of watermark circumvention is subsampling an image. In order to detect if a watermarked image has been subsampled, the original watermark $S$ has to be subsampled as well. By comparing the altered watermark with the image in question, an analysis can be performed. This analysis will have more error introduced into it, but not enough to make watermark detection impossible.
Conclusions

1. Through testing, it was determined that this method is resistant to JPEG compression up to ratios of 4:1.
2. Research casting watermark in DCT domain.

Limitations

1. Method only works for gray-scale level images.
2. No other tests were employed to see if this method could be circumvented.
3. Limited resistance to JPEG compression.
Uses of the Method

This method has been used as the foundation for the following projects:

1. Using Digital Watermarking on Color Images
2. Basis for more advanced Methodologies.
3. Basis for Adaptive Watermarking

Our Suggestion

Further testing to see if method can withstand cropping and other image manipulation techniques.