A METHOD FOR SIGNATURE CASTING ON DIGITAL IMAGES

I. Pitas

Department of Informatics
University of Thessaloniki
Thessaloniki 54006, Greece
E-mail: pitas@zeus.csd.auth.gr

ABSTRACT

Signature (watermark) casting on digital images is an important problem, since it affects many aspects of the information market. We propose a method for casting digital watermarks on images and we analyze its effectiveness. The satisfaction of some basic demands in this area is examined and a method for producing digital watermarks is proposed. Moreover, immunity to subsampling is examined and simulation results are provided for the verification of the above mentioned topics.

1. INTRODUCTION

The following analysis is a suggested approach in solving a quite interesting and demanding problem: *casting digital watermarks on digital images*. By the term "digital watermark", we mean a signal which is superimposed on the digital image, in such a way that:

1. The visual perception of the image remains unaltered and the watermark is unnoticed.

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

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

4. The detection of the digital watermark through general image operations and manipulations should be extremely difficult and, preferably, impossible.

The satisfaction of the above mentioned demands provides a way to superimpose an "invisible" watermark on images. This signal completely characterizes the person who applied it and, as a result, proves the origin of the image.

The benefits of such a method are numerous. The copyright owners of digital images have a way of protecting their products against illegal copies. An owner of an image database, for example, can use watermark casting on his images and, in the case of unauthorized replications of his products, prove his copyright ownership. Television channels are presently protected merely by their logo signs on a corner of the video signal. The digital watermark can ensure them against illegal recordings and retransmissions. On the other hand, the existence of the watermark on images can be used as an authentication tool as well.

Watermarks are applied either in the frequency or in the spatial domain [1,2]. The approach we follow in this paper is based on statistical detection theory and it is applied in the spatial domain.

2. DIGITAL WATERMARK DESCRIPTION AND SATISFACTION OF BASIC DEMANDS

We consider the case where a $N \times M$ gray level image I has to be transformed to a $N \times M$ image I_s, containing a digital watermark S. S is actually a specific binary pattern of size $N \times M$ where the number of "ones" equals the number of "zeros":

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

where $s_{nm} \in \{0,1\}$.
We consider that the original image I is represented as:

$$I = \{x_{nm}, n \in \{0,1,\ldots,N-1\}, m \in \{0,1,\ldots,M-1\}\} \tag{2}$$

where $x_{nm} \in \{0,1,\ldots,L-1\}$ is the intensity level of pixel (n,m) and L is the total number of intensity levels. We can split I into two subsets of equal size $P = N \times M)/2$, as follows:

$$A = \{x_{nm} \in I, \ s_{nm} = 1\} \tag{3}$$

$$B = \{x_{nm} \in I, \ s_{nm} = 0\} \tag{4}$$

S is superimposed by changing the elements of the subset A by the positive integer factor k:

$$C = \{x_{nm} \oplus k,\ \ x_{nm} \in A\} \tag{5}$$

The signed image is given by:

$$I_s \ = \ C \cup B \tag{6}$$

In the following, we shall use the symbols: $\bar{a}$, $\bar{b}$ and $\bar{c}$ to denote the mean values of the subsets A, B, C, and the symbols s_a, s_b and s_c will denote the *sample* variances:

We should now show that the basic demands mentioned in section I are satisfied by the proposed method.

First Demand

The quantity k that is added to the pixel $x_{nm} \in A$ to produce the set C in equation (5) is actually sufficiently small, so that the ratio k/x_{nm} remains small and its visual perception is negligible according to Weber's law. Especially, if the members of the subsets C and B do not form a recognizable pattern, then the picture does not seem distorted in any way.

Second Demand

The central key is the examination of the difference of the mean values of the two image subsets C and B. First we calculate the mean values $\bar{c}$ and $\bar{b}$ and then apply the theory of Hypothesis Testing [5,6] for the determination of the difference $\bar{w} = \bar{c} - \bar{b}$ of the two mean values. Our test statistic is [6]:

$$q = \frac{\bar{w}}{\hat{\sigma}_{\bar{w}}} \tag{7}$$

where $\hat{\sigma}^2_{\bar{w}} = (s_c^2 + s_b^2)/P$. The Null and the Alternative Hypotheses, respectively, are:

H_0: There is **no** watermark in the image ($\bar{w} = 0$).

H_1: There **is** a watermark in the image ($\bar{w} = k$).

Under the Null Hypothesis, the test statistic q follows Student distribution with zero mean and $(2P-2)$ degrees of freedom which can be very well approximated by the normal distribution.

When the Alternative Hypothesis holds, the test statistic q is distributed according to the so-called non-central Student distribution with mean equal to $\frac{k}{\sigma_{\bar{w}}}$. For a large number of samples the distribution of q can be approximated by a normal distribution having unit variance and mean equal to $\frac{k}{\sigma_{\bar{w}}}$. Furthermore, $\hat{\sigma}_{\bar{w}}$ can be used instead of $\sigma_{\bar{w}}$.

The possible detection are the following:

Type I Error: Accept the existence of a watermark, although there is none.

Type II Error: Reject the existence of a watermark, although there is one.

If $t_{1-\alpha}$ is the t-percentile that minimizes *both* errors, then

$$k = \lceil 2\hat{\sigma}_{\bar{w}} t_{1-\alpha} \rceil \tag{8}$$

As a result, during the watermark casting (or superposition) of the image, we can give as input the degree of certainty $(1-\alpha)$ which we want to have during the later phase of the detection of the watermark.

Watermark Casting (superposition)

We calculate s_a^2 and s_b^2 and use them to calculate $\hat{\sigma}_{\bar{w}}$. We calculate k from equation (8). However, the quantization imposed by this equation changes slightly the level of certainty to $1-\alpha'$. Moreover, the assumption $s_c = s_a$ is made. This is not exactly correct due to clippings in the case when the terms $x_{nm} + k$ result in numbers outside the range $\{0, \ldots, L-1\}$. Finally, we create the signed image I_s by substituting the subset A of I with the subset C.

Watermark Detection

We calculate $\bar{c}$, $\bar{b}$ and use them to calculate $\bar{w}$. We calculate s_c, s_b and use them to calculate $\hat{\sigma}_{\bar{w}}$. We create the test statistic q from equation (7) and test it against $t_{1-\alpha}$. If $q < t_{1-\alpha}$, we give the answer "there is no watermark", else "there is a watermark".

Third Demand

We now move to the examination of the number of "different" watermarks provided by the above mentioned scheme. Moreover, it is now time to suggest a method of creating watermark domains S. The most general method is to employ random sets S for this purpose. Such domains can be easily created by pseudo-number generators.

Let us consider the case when two watermarks have X out of P pixels in common (partial overlap). When we try to detect one of these watermarks, while this image was signed by using the other, we will get:

$$\bar{w}' = \bar{c}' - \bar{b}' = (\bar{a} - \bar{b}) + \left(2\frac{X}{P} - 1\right)\ k \tag{9}$$

If

$$q = \frac{(\bar{a} - \bar{b})}{\hat{\sigma}_{\bar{w}'}}\ ,\ h = \frac{(2\frac{X}{P} - 1)\ \ k}{\hat{\sigma}_{\bar{w}'}} \tag{10}$$

where q is the test statistic we would get if we examined the clear image, then the probability of a wrong answer is given by:

$$\mathrm{Prob}(q + h > t_{1-\alpha}) \tag{11}$$

Let us denote by: $N(x, \mu, \sigma^2)$ the cdf of a normally distributed random variable x with mean value μ and variance σ^2. The distribution of q is given by

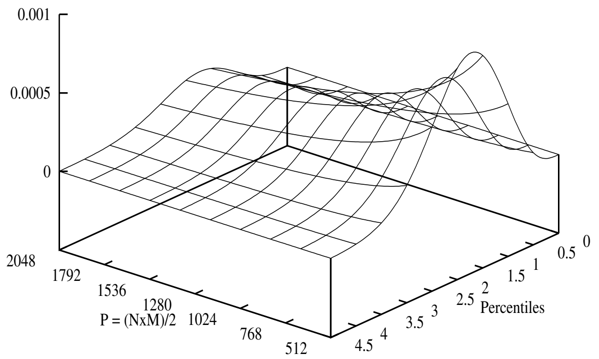

Figure 1: Uncertainty imposed by watermark similarity

$N(q, 0, 1)$. We can find also that the distribution of h is $N(h, 0, \frac{k^2}{2P\hat{\sigma}^2_{\bar{w}'}})$. Since q and h are independent random variables, the distribution function of their sum is given by the convolution of their distribution functions which is also a normal distribution, having mean value the sum of means and variance the sum of variances [7,6]. So we find :

$$t_{1-\alpha'} = t_{1-\alpha} \left(1 + \frac{\hat{\sigma}^2_{\bar{w}}}{\hat{\sigma}^2_{\bar{w}'}} \cdot \frac{2t^2_{1-\alpha}}{P}\right)^{-\frac{1}{2}} \tag{12}$$

It is obvious that $t_{1-\alpha'} < t_{1-\alpha}$, which means that our degree of certainty has indeed decreased. Moreover, the superposition of a watermark, as described so far, has the nature of additive noise. As a result, the overall variance of the image is increased, which means that $\hat{\sigma}_{\bar{w}} < \hat{\sigma}_{\bar{w}'}$. We, therefore, obtain an upper and a lower limit of $t_{1-\alpha'}$:

$$\frac{t_{1-\alpha}}{\sqrt{1 + \frac{2t^2_{1-\alpha}}{P}}} < t_{1-\alpha'} < t_{1-\alpha} \tag{13}$$

We shall try to estimate the uncertainty imposed due to the second watermark by using these upper and lower limits. This uncertainty is given by the function:

$$f(x) = N(x, 0, 1) - N\left(x\,(1 + 2x^2/P)^{-\frac{1}{2}}, 0, 1\right) \tag{14}$$

for $x = t_{1-\alpha}$. $F(x)$ has a maximum value, which is approximated by the formula:

$$x = \sqrt{\frac{3P}{P-6}} \simeq \sqrt{3} \tag{15}$$

This result can be verified by Figure 1, where we show the function $f(x; P)$ for such values of x and P that are used in the cases of percentiles and images, respectively.

In Figure 2a we can see a graphical representation of the normalized ambiguity imposed by a similar watermark: $f(t_{1-\alpha})/N(t_{1-\alpha}, 0, 1)$ for $t_{1-\alpha} = \sqrt{3}$. Moreover, a value of $t_{1-\alpha}$ given by (15) is highly improbable to be used in practice, since it provides only 95.83% degree of certainty. Instead, a value $t_{1-\alpha} = 4$ is more typical, if we want to be very sure about the existence of watermarks. Figure 2b presents the normalized ambiguity for $t_{1-\alpha} = 4$. It is easy to understand that the problem of similar watermarks does not really increase our initial uncertainty seriously, since for images as small as 32×32 ($P = 512$) this uncertainty increases by only a factor of $2 \cdot 10^{-5}$ ($t_{1-\alpha} = 4$), and for typical images of size 256×256 ($P = 32768$) this factor is $2.6 \cdot 10^{-7}$.

3. IMMUNITY TO SUBSAMPLING

We consider the case of the mean value subsampling, where every four pixels are substituted by their mean value. So we get the subsampled image I_{sub} with size $\frac{N}{2} \times \frac{M}{2}$.

In order to apply the detection algorithm on I_{sub}, we first make a subsampled version of our $N \times M$ watermark, using the following method:
Let $s_1, s_2, s_3, s_4 \in S$ denote the 4 neighboring pixels to be subsampled and let $u = s_1 + s_2 + s_3 + s_4$ be their sum. The sample s, which will substitute s_1, s_2, s_3, s_4 has the following form:

i) If $u = 0$ or $u = 1$ then $s = 0$
ii) If $u = 3$ or $u = 4$ then $s = 1$
iii) If $u = 2$ then $s = 0$ or $s = 1$ with equal probabilities

When we examine the subsampled image with this watermark, errors are introduced. In the signed part of the image 8 different kinds of 2×2 squares can exist:

i) 1 block containing 4 signed pixels
ii) 4 block containing 3 signed pixels
iii) 3 block containing 2 signed pixels

Similar statements hold for the unsigned part of the image. As a result, when calculating $\bar{w}$, we shall have:

$$\bar{w} = \bar{a}' - \bar{b}' + 3k/8 \tag{16}$$

We use $\bar{a}'$ and $\bar{b}'$ because they are not really the original $\bar{a}$ and $\bar{b}$, since there was an intermixing due to subsampling.

If we want to detect the watermark, assuming undisturbed $\hat{\sigma}_{\bar{w}}$ and the probability of the correct answer to be exactly the initial degree of certainty $(1 - \alpha)$, the following must hold:

$$\text{Prob}(\frac{\bar{a}' - \bar{b}' + 3k/8}{\hat{\sigma}_{\bar{w}}} > t_{1-\alpha}) = 1 - \alpha \tag{17}$$

Thus, $k = \frac{8}{3} \cdot 2\hat{\sigma}_{\bar{w}} t_{1-\alpha}$. Equation (17) implies that, if we want to have $(1 - a)$ degree of certainty in the subsampled image, we should use equation (8) to calculate k, but finally apply the weight $k' = \frac{8}{3}\,k$. In this case, the

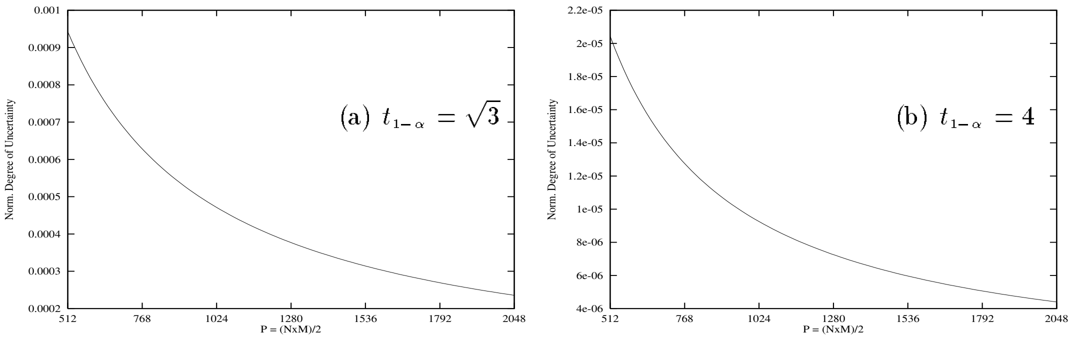

Figure 2: Normalized Uncertainty due to watermark Similarity

degree of certainty for the original image is obviously increased, giving a value $1 - \alpha'$ which is defined by:

$$t_{1-\alpha'} = \frac{k'}{2\hat{\sigma}_{\bar{w}}} = \frac{8}{3} t_{1-\alpha} \qquad (18)$$

From the above discussion we understand that, if we want to have an immune watermark after i consecutive subsamplings, by induction, the weights $k' = \left(\frac{8}{3}\right)^i k$ must be used.

4. SIMULATION RESULTS AND CONCLUSIONS

In this paper we propose a novel method for casting digital watermarks on images. This is basically done by adding a predetermined small luminance value to randomly selected image pixels. The luminance values are small enough to be undetected by the human eye. The seed of the random pixel generator is essentially the copyright holder watermark. We also propose a scheme for watermark detection that is based on statistical detection theory criteria. Although watermark domains may overlap, we have proven that the watermarks are easily distinguishable. We have also proven that the proposed watermark scheme is rather immune to subsampling. Unlike other watermark casting schemes proposed recently, our method is based on solid mathematic background given by statistical detection theory. The theoretical study has been verified by numerous simulation experiments.

We tested the above mentioned algorithm on two images, namely "car" and "lenna". We applied 3,000 different watermarks upon them, asking for the minimum certainty. Due to the quantization of k (shown in (8)), for $k = 1$, the degrees of certainty $(1 - \alpha)$ were 84.1% and 90.5% respectively. The simulation results were very close to these values, namely 84.1% and 90.96%. We repeated the same simulation, but with unsigned images this time, and obtained certainties 83.96% and 91.8% respectively.

One important issue that was tested by simulation was the watermark resistance to JPEG compression. It was found that the method, as presented here, is resistant to compression ratios up to 4:1. This is already an interesting result, if we take into account that the proposed watermark casting method essentially adds high frequency noise to the image.

Acknowledgements The work reported in this paper was partially supported by the European Community project ACCOPI.

5. REFERENCES

[1] E. Koch, J. Zhao, "Towards robust and hidden image copyright labeling", *Proc. IEEE Workshop on Nonlinear Signal and image processing*, I. Pitas editor, pp. 452-455, 1995.

[2] O. Bruyndonckx, J.J. Quisquater, B. Macq, "Spatial method for copyright labeling of digital images", *Proc. IEEE Workshop on Nonlinear Signal and image processing*, I. Pitas editor, pp. 456-459, 1995.

[3] I. Pitas, T. Kaskalis, "Applying Signatures on digital images", *Proc. IEEE Workshop on Nonlinear Signal and image processing*, I. Pitas editor, pp. 460-463, 1995.

[4] R.G. van Schyndel, A.Z. Tirkel, C.F. Osborne, "A digital watermark", *Proc. IEEE International conference on Image Processing*, vol. 2, pp. 86-89, 1995.

[5] E. L. Lehmann, "*Testing Statistical Hypotheses*", Wiley, 1987.

[6] A. Papoulis, "*Probability & Statistics*" Prentice Hall, 1991.

[7] A. Papoulis, "*Probability, Random Variables and Stochastic Processes*", McGraw-Hill, 1991.