DIGITAL WATERMARKING THROUGH FILTERING

Pauli Kuosmanen*, Jaakko Astola†, Kári Davíðsson‡and Katriina Halonen§
Tampere University of Technology
Signal Processing Laboratory
P.O.Box 553, FIN-33101 Tampere, Finland

ABSTRACT

A new method for signature embedding and detection for digital signals is introduced. The method uses local characteristics in the signal to conceal the signature, also called the watermark in the signal. The watermark follows therefore closely the signal characteristics and is difficult to detect without knowing the right parameters of the embedding procedure.

1. INTRODUCTION

Watermarking of images has been a popular topic in the recent past, and it is likely that it will gain more popularity. The need for good watermarking method comes from the vast popularity of the Internet World Wide Web and the emergence of all digital television broadcasting system. Defending copyrights of digital material (such as audio, images and video) is difficult. Copying and distribution is easy without losing quality of the data. Circumventing copyright information in "header data" is easy. The only solution is to embed the copyright information in the data itself. The copyright information becomes then the signature of the data or the watermark. This must then be done in such a way that the signature is hard to see and detect with wrong parameters but relatively easy to detect given the correct parameters.

2. SIGNATURE METHOD

Consider a binary image, our signature [1, 2] S of size $H \times K$. We call the one valued pixels in S signature pixels. We want to impose S on our image I of size $M \times N$ using a filter mask F of size $U \times V$. For a given filter F and image I we have two conditions for this method to work,

- $U < \lfloor \frac{M}{H} \rfloor, V < \lfloor \frac{N}{K} \rfloor$
- The origin of F must be zero.

Basically what we do is to place the filter mask regularly in the image, at pixels that correspond to the signature pixels. We filter the corresponding pixel and replace the original with the result. To prevent a signed pixel from being a affected by another signed pixel we make the first of the above conditions. The second constraint comes naturally when the detection algorithm is introduced. Given these conditions the signature algorithm can be formulated as:

Require: $I_{M\times N}$, $S_{H\times K}$, $F_{U\times V}$, $F_{\text{origin}} = 0$, $U < \lfloor \frac{M}{H} \rfloor, V < \lfloor \frac{N}{K} \rfloor$.

1: tmp $\leftarrow S \uparrow_x \lfloor \frac{M}{H} \rfloor$. {$\uparrow_x$ is upsampling in direction x.}
2: $\bar{S} \leftarrow$ tmp $\uparrow_y \lfloor \frac{N}{K} \rfloor$ {We now have an upsampled version of the original signature.}
3: $\tilde{I} \leftarrow$I
4: Form a column vector m out of the filter mask F. {With some fixed scanning.}
5: **for all** 1 valued pixels $\bar{S}_{i,j}$ in $\bar{S}$ **do**
6: Place F in $\tilde{I}$ so that its center is at (i,j) in $\tilde{I}$.
7: Find a group of neighbors in $\tilde{I}$ coinciding with F.
8: Form a row vector f out of this group of neighbors. {With the same scanning as in step 4.}
9: $\tilde{I}_{i,j} \leftarrow f \cdot m$. {$\cdot$ is the dot product operator.}
10: **end for**{$\tilde{I}$ is the signed image.}

3. DETECTION METHOD

Now we have a method for embedding a signature S in an image I with a filter F. We must, though, be able to detect the signature again. It is easy to verify the existence of a signature by comparing it with the original, but in practice it is not a reasonable requirement to have permanent access to the original. It must be possible to verify the existence of the signature without knowing the original image.

Using the fact that the filter F has a hole at the origin

*pqo@cs.tut.fi
†jta@cs.tut.fi
‡d154402@cs.tut.fi
§kha@cs.tut.fi

it is possible to verify the existence of a signature by filtering the whole image $\tilde{I}$ with F and picking out all the pixels that have probably been signed already. By doing this we are able to recover the possible signature. We may also get some false detections, i.e. pixels in $\tilde{I}$ that are classified as signature pixels but are not. By performing pattern search, e.g., using correlation, we can verify if the signature is there in an automatic way. The detection algorithm can then be summarized as,

Require: $\tilde{I}$ possibly signed, F, $\bar{S}$ the upsampled version of S, d the deviation factor.

1: $C_1 \leftarrow$ Filter $\tilde{I}$ with F.
2: $tmp \leftarrow \mathrm{abs}(\tilde{I} - C_1)$.
3: **for all** pixels (i, j) in tmp **do**
4: $\quad \hat{\tilde{S}}_{i,j} \leftarrow 1 - t_d(tmp_{i,j})$
5: **end for**{$\hat{\tilde{S}}$ is the output of detection phase 1. }
6: $C_2 \leftarrow$ Correlate $\hat{\tilde{S}}$ and $\bar{S}$ and normalize. {C_2 is the output of detection phase 2. }
7: $Max \leftarrow \max(C_2)$.
8: $R = t_{0.99}(Max)$.

Ensure: $R = 1$ if $\bar{S}$ in $\tilde{I}$, $R = 0$ otherwise.

Here the function $t_d(x)$ is the thresholding operator,

$$t_d(p) = \begin{cases} 1, & p > d, \\ 0, & p \leq d. \end{cases}$$

Note that basically step 1 in the detection algorithm is doing the same things as steps 5 to 10 in the embedding algorithm, except that we are doing it for all pixels in the image $\tilde{I}$ in the detection but in embedding only for a selected number of pixels, depending on the signature.

4. MULTIPLE ENCODING

A simple extension to the embedding and detection algorithms is multiple encoding. Instead of just changing one pixel in the image for each signature pixel we will change "many" pixels. In order to do so we introduce a "complex" filter mask with several outputs, where each output is defined by a "simple" filter mask (Figure 1). The complex filter mask can be any structure meeting a similar condition as the filter mask in previous sections, i.e., the origin of one simple filter mask may not contribute to the output of another simple filter mask, including itself, i.e., the origins must be zero valued. This ensures that the detection filter mask is working in the same environment as the embedding filter mask in the case of distortionless storage/distribution of the signed image. The multiple encoding can be seen as a repetitive use of the encoding algorithm with different filter masks. The decoding algorithm is generalized

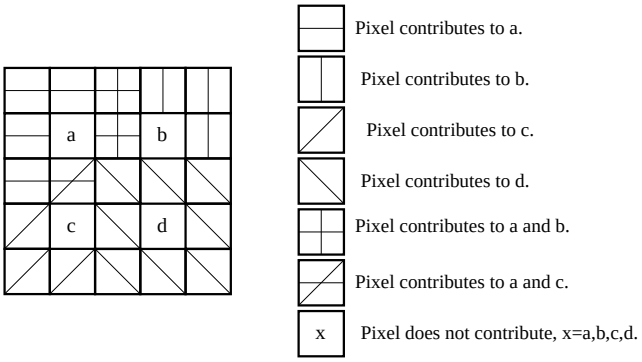


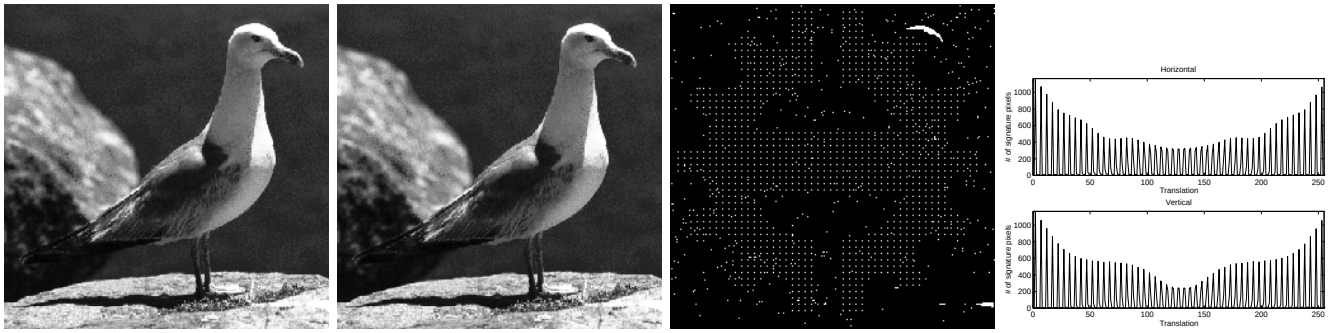
Figure 1: One example of a "complex" filter mask constructed with two simple filter masks.

somewhat, i.e., we require detection for all simple filter masks within the complex filter mask in order to classify the pixel at the center of the complex filter mask as signed. The potential gain of doing multiple encoding in this way is that by using different filters for each of the simple filter masks we get a different behavior. For example, the complex filter mask with simple filter masks a and b might be chosen in such a way that a signature embedded with a tolerates lowpass filtering while signature embedded with b tolerates highpass filtering of the signed image. For distorting storage/distribution, i.e. channels with low pass filtering we will not require detection for all simple filter masks in the complex filter mask is not required for classification of the corresponding pixel. For distortionless channels multiple encoding helps us to detect the signature in a cleaner manner.

The obvious drawback of doing multiple encoding in this manner is that a pirate can concentrate on finding one of the simple filter masks. If the pirate succeeded in finding one of the masks she has an approximate location of the logo, i.e., within half of the dimensions of the complex mask and can then concentrate to find the rest of the coefficients of the complex filter mask.

5. RESULTS

For this experiment we used a 50×50 "TTKK" logo as a signature. We embedded this logo using several filter structures as the embedding filter in the "Seagull" image (Figure 2(a)). The filter masks used for the experiment are simple filter masks, except one, which is a 5×5 complex filter mask with four centers (Figure 1). The structures are denoted as A, B, C, D and E for the simple filter masks and F denotes the complex mask. All the simple filter masks, A, B, C, D, and E are scaled



(a) The original "Seagull" image.

(b) The signed "Seagull" image.

(c) The result of detection phase 1.

(d) The horizontal and vertical scan lines through $(1,1)$ of the result of detection phase two.

Figure 2: Typical result for signature embedding. The embedding and detection filter is the 3×3 mean filter mask with hole in the center, mask C. The logo is 50×50 "TTKK" logo. Results comparable to line three in Table 1.

mean filters, with factors $0.90, 0.99, 1.00, 1.01$, and 1.1 respectively. The origin is at the center of the filter mask. The complex filter mask F is composed of four filter masks, of which one (mask d in Figure 1) is the simple filter mask C, the mean filter. The other simple masks are chosen such that the sum of their weights is unity and none of the masks are equal.

We measure the performance of the method as how much the method distorts (MAE and MSE measures) the image. How well the detection algorithm detects a signature if it is there and how well it rejects signature if there is no signature in the image is given by four numbers $f_{x,y}, x, y \in \{0,1\}$, where $f_{x,y}$ denotes the number of occurrences of x when y was expected.

The method distorts the image little. The mean filter mask C has the smallest distortion while the complex filter mask F has the largest distortion (Table 1). This is understandable because the complex mask changes four times more pixels than the simple filter masks. If compared to the energy of the image, $E_{\text{gull}} \approx 5192$ the distortion is small. The S/N ratio for the complex mask is $\approx 25dB$.

As we can see (Table 1) the ability to detect the signature depends on the filter structure. That is, some filters are not as well suited for signature embedding than others, e.g., filter mask C detects some extra pixels in detection (Figure 2(c)). This means also that in embedding not all pixels in the image are changed. From the results (Table 1) we see that a small scaling of the mean filter mask allows us to detect the logo in a clean manner as does the complex filter mask. The mean filter mask, mask C, gives a few false detected pixels. We can see from Table 1 that detection with a wrong filter is not possible in the case of simple mask embedding. Using the complex mask and with some luck, i.e., guessing one of the simple mask we are able to detect the logo (here one of four) with offset, i.e. at $(2,2)$ instead of the correct position $(1,1)$ (last line in Table 1) (Figure 3(c)). As we said before this can aid the pirate in locating the logo, but still the pirate must first find the coefficients of one of the simple filter masks in the complex filter mask. This is not an easy task. The signed pixels are so similar to the unsigned pixels, because the signature is strongly dependent on the original image.

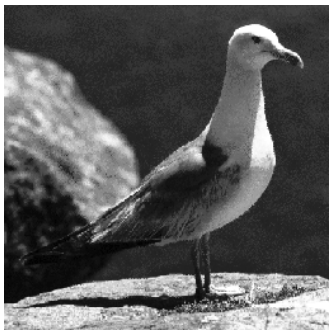
The filters used for embedding must be chosen in such a way that the probability for a pixel to change in filtering is high. This means that for different types of images, different filters must be used. For "real" images this is not a problem because they always contain noise, which will make the probability of change higher. We see in Figure 3(b) that there are "holes" in the logo pattern. This means that the corresponding pixel does not change when signed or filtered with a given mask. Pixels with that property will also introduce errors in the detection phase one (Figure 2(c)). For computer generated images or images that are very smooth, averaging filters used in this paper will not do in most cases. A different filtering method must then be used.

6. CONCLUSIONS

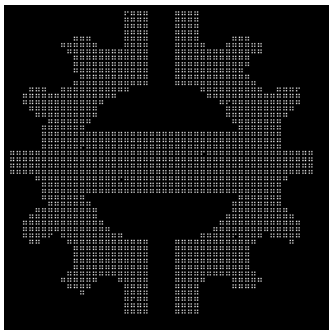
A new alternative in signature embedding/watermarking and its detection was introduced.

Table 1: Comparison of the method with various filter structures in terms of distortion for the signed image and error rates in detection. The signature was embedded at $(1,1)$ in the image. The signature was the 50×50 TTKK logo.

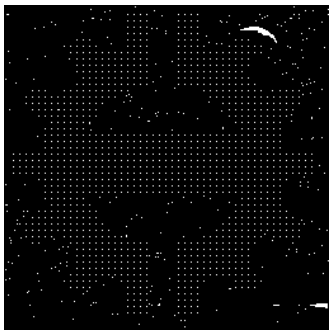
Emb. Mask	Det. Mask	MAE	MSE	$f_{1,1}$	$f_{0,0}$	$f_{0,1}$	$f_{1,0}$	Max. corr.	Where
A	A	0.20	4.89	1165	64371	0	0	1165	1,1
B	B	0.14	3.08	1165	64371	0	0	1165	1,1
C	C	0.14	3.07	1165	63827	0	544	1165	1,1
D	D	0.14	5.08	1165	64371	0	0	1165	1,1
E	E	0.21	5.06	1165	64371	0	0	1165	1,1
F	F	0.66	17.2	1165	64371	0	0	1165	1,1
A	B	0.20	4.89	0	65536	0	0	-	-
B	C	0.14	3.08	0	64998	0	538	24	134,224
C	D	0.14	3.07	0	65536	0	0	-	-
D	E	0.14	5.08	0	65536	0	0	-	-
E	F	0.21	5.06	0	65536	0	0	-	-
F	C	0.66	17.2	0	63975	0	1561	1165	2,2



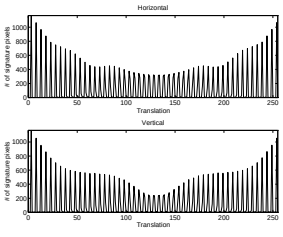
(a) The signed image.



(b) Thresholded absolute difference of the original and signed image.



(c) The result out of detection phase 1.



(d) The horizontal and vertical scan lines through $(2,2)$ of the result of detection phase two.

Figure 3: Embedding result for a complex filter mask and detection results for a chosen simple filter mask. The logo is embedded four times in the image as defined by the complex filter mask, mask F. Detection filter mask was the 3×3 mean filter mask with a hole in the center, mask C. The logo is 50×50 "TTKK" logo. Results comparable to the last line in Table 1.

The main advantages of this method is its simplicity and the fact that it is highly parameterizable. When signing in the spatial domain the signature is impossible to spot. The changes made to the original image follow it closely. The main drawback is that there is one-to-one association between the number of signature pixels in logo and number of pixels changed in the image. This means that the method is vulnerable to processing of the signed image. Multiple encoding, as introduced here is one attempt to increase the robustness of the signature. The method can also be used in conjunction with some invertible transform, like DCT (Discrete Cosine Transform), DFT (Discrete Fourier Transform) or DWT (Discrete Wavelet transform) in order to make the embedding method more robust. When applied in the spatial domain this method is not at all robust, in the sense that small changes to signed image will degrade the ability to detect the signature considerably. Even "small" blurring can have catastrophic effect on the signature. Using the method in DWT domain seem though to be promising but not presented here. In this paper we used FIR filters. There is nothing that prohibits us to use any other filter structure, e.g., nonlinear filters could be used.

7. REFERENCES

[1] J. Astola and P. Kuosmanen. Hiding a security code in an electrical signal. Patent application FI970295, January 1997. In Finnish.

[2] I. Pitas and T. H. Kaskalis. Applying signatures in digital images. In *1995 IEEE workshop on nonlinear signal and image processing*, volume I, pages 460–464. Institute of Electrical and Electronics Engineers, Inc., June 1995.