

Human Visual System Based Watermarking

Robert Schriver

Abstract—We attempt to show a method below of hiding and extracting a watermark in an image in the spatial domain such that we minimize the visual effect of the watermark on the image while still maintaining watermark integrity.

I. INTRODUCTION

Digital watermarking is the attempt to craft an image in such a fashion that if we apply a simple set of transforms, we are able to extract a watermark which will identify the image as our own. Thus, if someone claims the image as theirs, we can demonstrate that they have taken the image from us, and use our embedded watermark as proof of this fact. However, we must try to make this watermark as robust as possible so that if a person modifies your image, you are still able to extract the watermark and prove that it is yours. We also must consider that the watermark should not be visible, so that the content of the image remains.

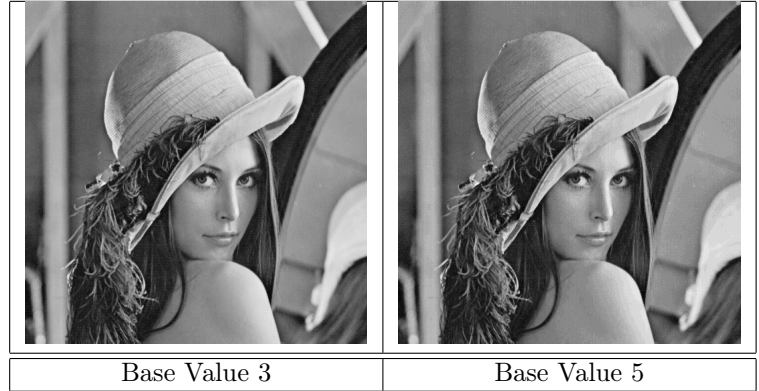
II. BACKGROUND

Much of the paper by Qi et al ¹ describes a technique by which the watermark can be more easily blended into the image. They propose the creation of a Human Visual System Mask, which attempts to hide the watermark in areas of the image where it would be less noticeable. It accomplishes this by combining together three other masks, called the luminance mask, edge mask, and texture mask. The luminance mask is a combination of the background luminance, which is just the average of the surrounding pixels, and the maximum gradient of a series of derivative filters at different angles. This luminance filter highlights large dark areas and high energy components of an image. The edge mask just uses the Canny edge algorithm ², which provides a response even with faint edges. To complete the edge mask, a dilation filter is applied that simply widens the edge mask. The texture filter is simply the difference between the center pixel and the mean of the surround. These mask are all combined and added to the image in a method I will describe in the section below. The actual watermarking algorithm is comparatively simple. A binary message image is generated that is $\frac{1}{16}$ th the size of the image, as well as a 4×4 random watermark with values 1 and -1. If the message bit is a 1, the watermark is added to a corresponding 4×4 block in the image that has the HVS mask applied. If the message bit is 0, then the watermark is subtracted. Since the image block is normalized by the HVS mask during this step, the watermark is embedded in the masked image, and it is more strongly embedded where the HVS mask is larger. To extract the message, we simply de-normalize based on the HVS mask, and then

compare to the watermark we used to embed the message. If it matches, the message bit is a one, and if it doesn't, the message bit is a zero.

III. METHOD

The implementation is mostly just taking the math and translating it into $n \times n$ filters, and since the math was discussed in the previous section I will talk mostly about the results of filter creation and the combination of the HVS masking and the image, as well as some changes which I made that are different than the source paper and the reasons I made those changes. I was able to achieve almost identical masks for all three different filters, which you can see above. The combination of these masks is not strictly multiplication, the minimum of the edge and texture mask is taken and scaled down, and then the maximum of that matrix and the luminance mask is combined to form the final HVS mask. Since the HVS mask will eventually be divided out of the image, there must be no zero values in the matrix, so there must be a base established, which essentially determined the watermarking strength in large uniform black areas. This value is located in the luminance mask, and the paper suggests setting this value to three. However, I found that setting this value slightly higher to 5 enabled much greater embedding strength and gave a higher PSNR for the message when errors were added. The comparison of the HVS Mask and watermarked image between these two values is show below, and the difference between the messages when noise is added is in the results section.



IV. RESULTS




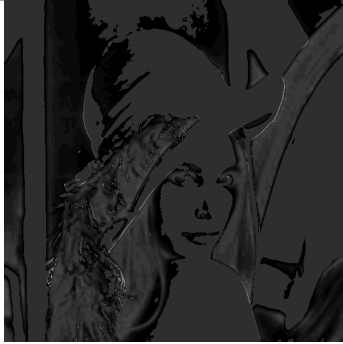
V. DISCUSSION

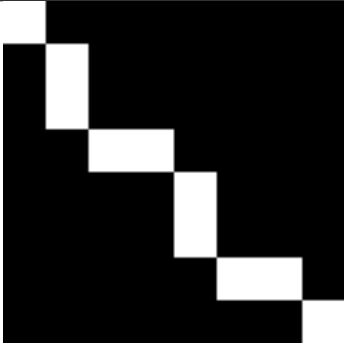


As demonstrated in the results, the watermark is fairly weak against an attack which changes every value in an image. Adding 10 to each pixel in an image is hardly noticeable to the observer, however the result to the watermark is fairly drastic. One interesting thing to note from these attacks is that in the final decoding after adding 10 to each pixel, we begin to see the inverse of the HVS mask coming

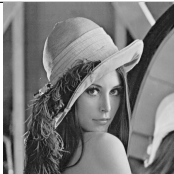



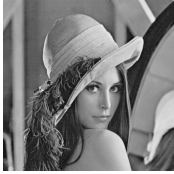



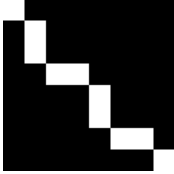

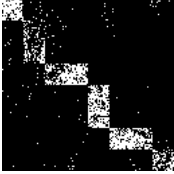
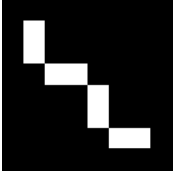
¹ Human visual system based adaptive digital image watermarking; Huiyan Qi, Dong Zheng, Jiying Zhao

² A Computational Approach to Edge Detection; Canny, John

through the message. The HVS encoding phase, at the base, just adds a few pixel counts to the block. If we add a count uniformly in the noising phase, high values in the image will be thresholded by the 255 count max. These high values also correspond to low HVS mask counts. When we decode using the HVS mask, it is likely that this combination of thresholding and the more sensitive HVS mask for that block causes the artifacts that show up. We can also see, however, that the message is basically unaffected by the cropping attack, as would be expected from a block based watermarking algorithm like this. We can see that this watermark is not very resilient against many attacks, and is would be very susceptible to anything which would affect a full 4×4 block at a time. While not shown in the results, the algorithm does not perform well against most filtering operations like blurring. Extrapolating from these results, it is also likely that it would not perform well against a compression attack. However, I believe that the main thrust of this paper was the Human Visual System mask which was developed, which enables better hiding in the spatial domain. This mask could easily be paired with a more robust watermarking technique, which would optimize both hiding and robustness against attack.

			
Luminance Mask	Texture Mask	Edge Mask	HVS Mask

Decoded Message			
PSNR	undef.	1.384	8.612
Alteration	Original	Base Value 3, +10	Base Value 5, +10

Watermarked				
Altered				
Decoded Message				
PSNR	undef.	8.612	11.287	14.670
Alteration Performed	No Alteration	+10 to each pixel	Gaussian Noise, sigma 2	Crop 64 pixel border