A Robust Embedded Data from Wavelet Coefficients

J. J. Chae and B. S. Manjunath

Department of Electrical and Computer Engineering
University of California, Santa Barbara, CA 93106
chaejj@iplab.ece.ucsb.edu, manj@ece.ucsb.edu

ABSTRACT

An approach to embedding gray scale images using a discrete wavelet transform is proposed. The proposed scheme enables using signature images that could be as much as 25% of the host image data and hence could be used both in digital watermarking as well as image/data hiding. In digital watermarking the primary concern is the recovery or checking for signature even when the embedded image has been changed by image processing operations. Thus the embedding scheme should be robust to typical operations such as low-pass filtering and lossy compression. In contrast, for data hiding applications it is important that there should not be any visible changes to the host data that is used to transmit a hidden image. In addition, in both data hiding and watermarking, it is desirable that it is difficult or impossible for unauthorized persons to recover the embedded signatures. The proposed scheme provides a simple control parameter that can be tailored to either hiding or watermarking purposes, and is robust to operations such as JPEG compression. Experimental results demonstrate that high quality recovery of the signature data is possible.

Keywords**:** digital watermarking, data hiding, copyright protection, authentication.

1 INTRODUCTION

As multimedia data becomes wide spread, such as on the internet, there is a need to address issues related to the security and protection of such data [1, 2, 3, 4, 5]. While access restriction can be provided using electronic keys, they do not offer protection against further (illegal) distribution of such data. Digital watermarking is one approach to managing this problem by encoding user or other copyright information directly in the data while not restricting access. Watermarking of image data could be visible, for example, a background transparent signature, or could be perceptually invisible. A visible watermark acts like a deterrent but may not be acceptable to users in some contexts. In order to be effective, an invisible watermark should be secure, reliable, and resistant to common signal processing operations and intentional attacks. Recovering the signature from the watermarked media could be used to identify the rightful owners and the intended recipients as well as to authenticate the data. In this paper we are mainly interested in embedding data such that the signature is invisible in the host image.

Data hiding is a generalization of watermarking wherein perceptually invisible changes are made to the image pixels for embedding additional information in the data [6, 7, 8, 9]. Data hiding could be used to embed control or reference information in digital media for applications such as tracking the use of a particular video for pay-per-use or billing for commercials in audio/video broadcast. Unlike traditional encryption methods where it is obvious that something is encoded, perceptually invisible data hiding in images/video offers an alternative for information transmission wherein it is difficult, if not impossible, for an unauthorized person to detect or decode the hidden content.

Previous work on embedding invisible signatures can be broadly grouped into spatial domain and transform domain methods. Targeted applications include watermarking for copy-right protection or authentication. Typically, the data used to represent the digital watermarks are a very small fraction of the host image data. Such signatures include, for example, pseudo-random numbers, trade-mark symbols and binary images. Spatial domain methods usually modify the least-significant bits of the host image [1, 5], and are, in general, not robust to operations such as low-pass filtering. Much work has also been done in modifying the data in the transform domain. These include DCT domain techniques [2, 3, 6, 7, 9, 11, 12, 13] and wavelet transforms [2, 8].

This paper presents a data embedding scheme that is suitable for both watermarking and image data hiding. While watermarking requires robustness to image manipulation, data hiding requires that there is very little visible distortion in the host image. While much of the previous work used signature data that is a small fraction of the host image data, the proposed approach can easily handle gray-scale images that could be as much as 25% of the host image. In recovering the signature image, it is assumed that the original host image is available.

The proposed scheme distributes the signature information in the discrete wavelet transform (DWT) domain of the host image. Spatial distribution of the DWT coefficients helps to recover the signature even when the images are compressed using JPEG lossy compression. In some of the recent work on using wavelets for digital watermarking, the signatures were encoded in all DWT bands. Such an embedding is sensitive to operations that change the high frequency content without degrading the image quality significantly. Examples of such operations include low pass filtering for image enhancement and JPEG lossy compression. In contract, the proposed scheme here focuses on hiding the signature mostly in the low frequency DWT bands, and stable reconstruction can be obtained even when the images are transformed, quantized (as in JPEG), or otherwise modified by enhancement or low pass filtering operations.

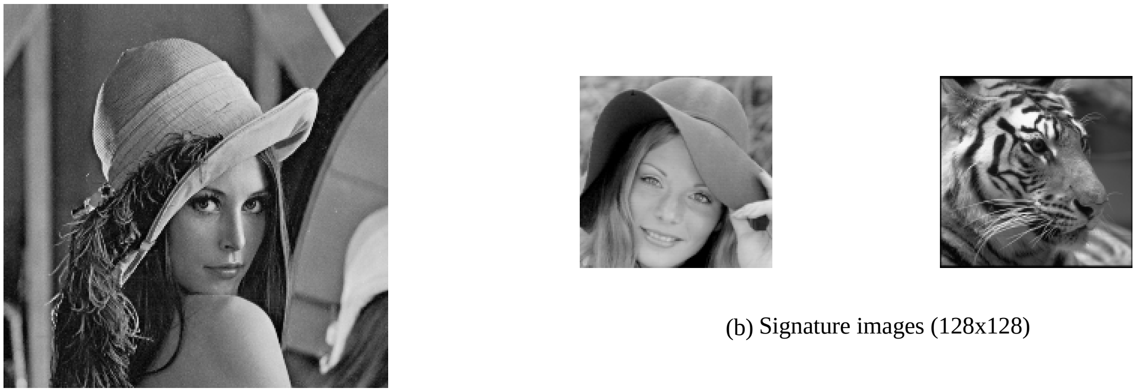
The paper is organized as follows: The next section describes the proposed algorithm in detail and experimental results are provided in Section 3. We conclude with discussions in Section 4.

2 DATA EMBEDDING

As mentioned earlier, a watermark should be robust to typical image processing operations, including lossy compression. Compression techniques, such as JPEG, typically affect the high frequency components. This is also true with most perceptual coding techniques. For these reasons, a digital signature should be placed in perceptually salient regions in the data. For techniques based on frequency domain modifications, this implies embedding the signature in mostly low frequency components. Inserting signature in low frequency components creates problems if one is interested in invisible watermarks. This is particularly true in data hiding applications where the data to be hidden could be a significant percentage of the original data.

We propose the use of a wavelet transform to embed signature information in different frequency bands. All the experiments described below use the discrete Haar wavelet basis, and adopting this method to other wavelet basis is reasonably straightforward. Both the signature data, which in our case is another image, and the host image data, are decomposed using the discrete Haar wavelet transform (DHWT) [14].

In the following discussion it is assumed that the signature image is one quarter the size of the host image, and both images are gray scale, one byte per pixel. An example of a host image and two signature



(b) Signature images (128x128)

(a) Host (256x256)

FIGURE 1. (a) A host image and (b) signature images, hat-girl image and a tiger image.

images used in the experiments are shown in Figure 1. Embedding occurs in the wavelet transform domain as the wavelet coefficients are combined to create a watermarked image. It is assumed that the host image is available for signature image recovery. A schematic of this approach is shown in Figure 2. The basic steps in embedding the signature coefficients into the host image coefficients are:

1. Decompose by one level the host and signature images using the DHWT. This results in four bands, which are usually referred to as the LL, LH, HL, and the HH bands (Figure 2 (a)).
2. Each signature image coefficient is expanded into a 2x2 block as follows (Figure 2).
   - Each coefficient value is linearly scaled to a 24 bit representation (Figure 2 (b)).
   - Let A, B, C represent, respectively, the most significant byte, the middle byte, and the least significant byte in a 24 bit representation. Three 24-bit numbers, A', B', C', are generated with their most significant bytes set to A, B and C, respectively, and with their two least significant bytes set to zero (Figure 2 (c)). Then a 2x2 expanded block is formed as shown in (Figure 2(d)).
3. The host image coefficients are also linearly scaled within each band to a 24 bit representation. The minimum and maximum values in each band will be used in the inverse transformation below.
4. The scaled host image coefficients are now added to the expanded signature transform to form a new fused transform. Let $h(m, n)$ be the $(m, n)^{\mathrm{th}}$ wavelet coefficient of the host image, and let $s(m, n)$ be the $(m, n)^{\mathrm{th}}$ signature coefficient after forming the expanded blocks as described in Step 2 (Figure 2). Note that after expansion each of the bands in the signature wavelet transform is of the same dimension as the host image bands. The fused $(m, n)^{\mathrm{th}}$ coefficient is then computed as:

   $$w(m, n) = \alpha h(m, n) + s(m, n) \tag{1}$$

   where the scale factor α determines the relative percentage of the host and signature image components in the new image.
5. The fused transform coefficients in each band are scaled back to the levels of the host image transform coefficients using the minimum and maximum coefficient values in Step 3.
6. An inverse transform is now computed to give the watermarked image.

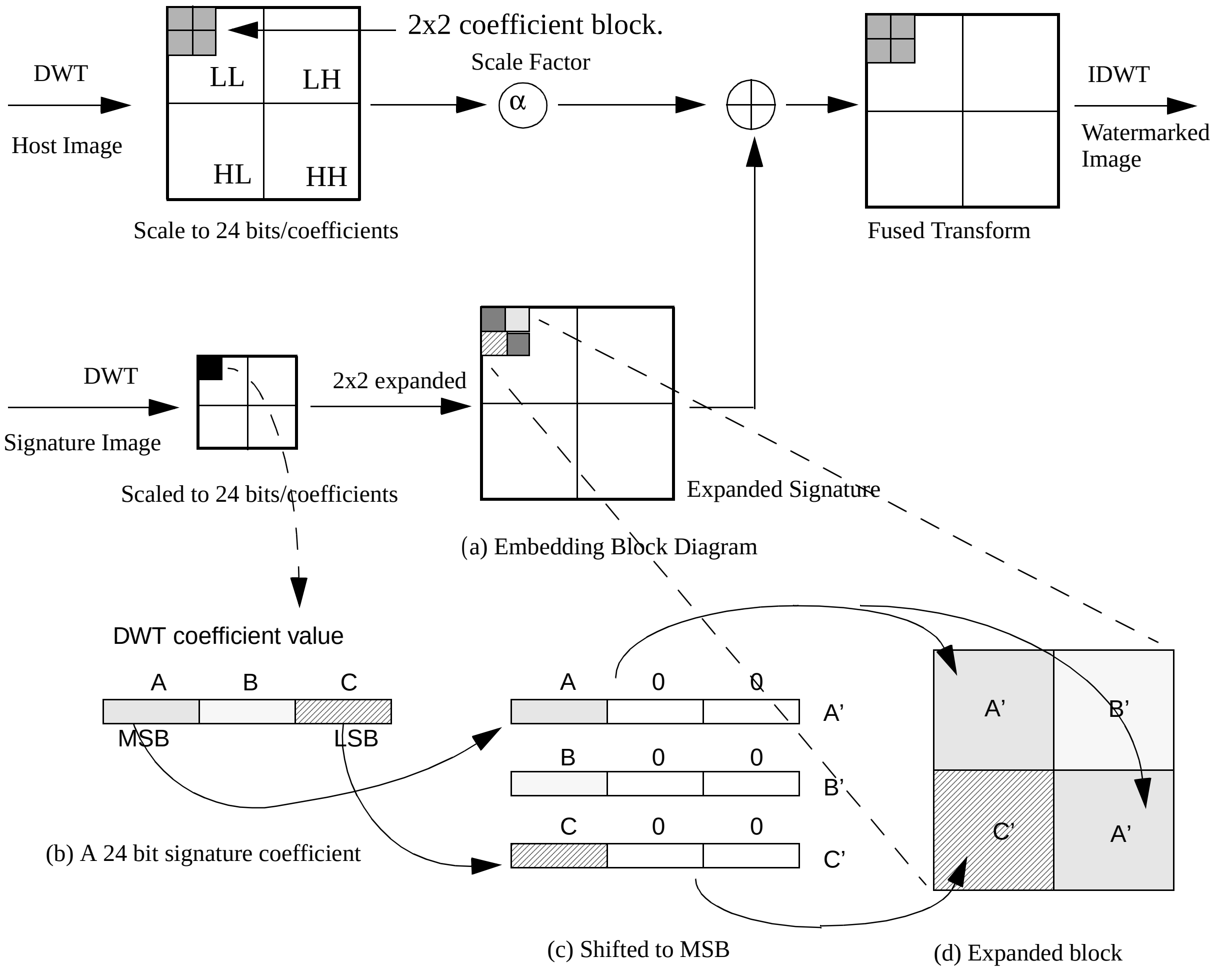
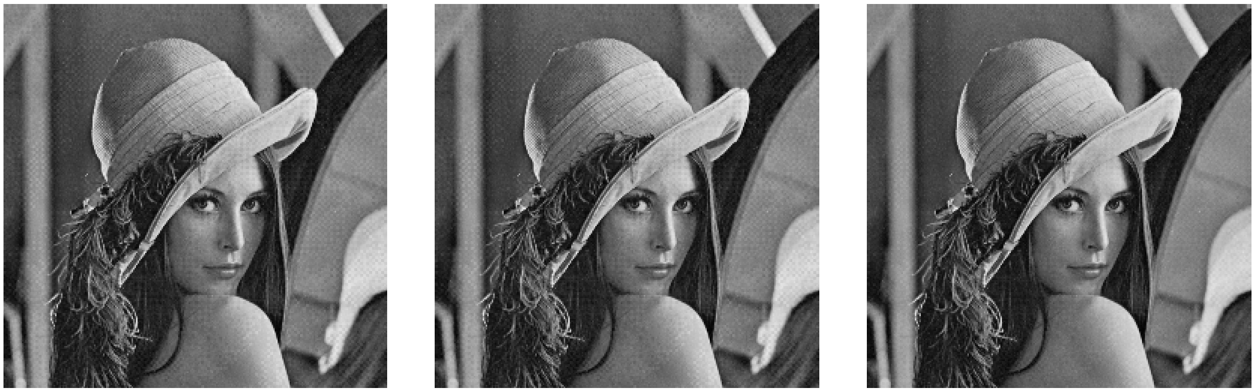


FIGURE 2. (a) A schematic of the data embedding approach. Here the signature image is assumed to be one quarter the size of the host image. See Section 2 for details. (b)-(d) Expanding a single signature coefficient to a 2x2 block of coefficients for embedding in the host image.

3 RESULTS

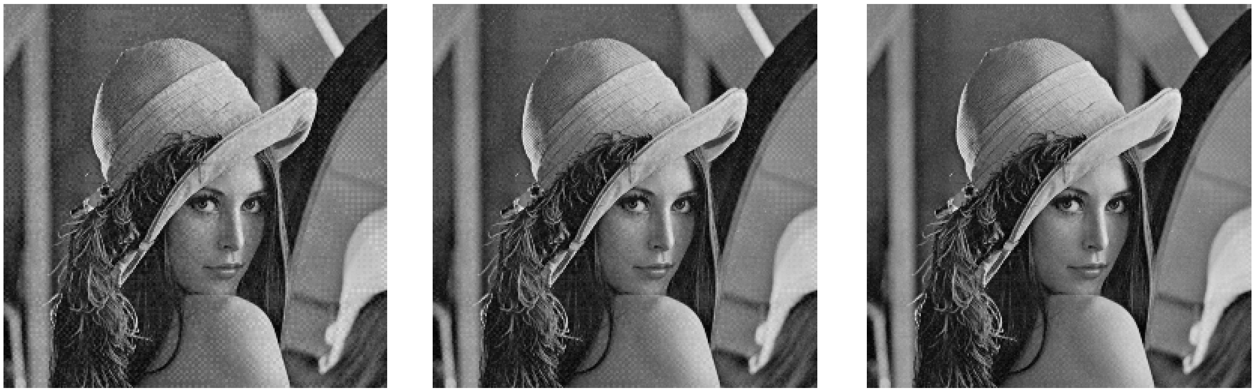
We present here results of embedding 128x128 gray scale (one byte per pixel) signature images in a 256x256 Lena image. Two images, one a “hat girl” picture and the other a picture of a tiger, are used as signature images in the following experiments. Figure 1 shows the host and signature images.

Figure 3 and Figure 4 show the embedded Lena images using different scale factors. Note that the higher the scale factor the better the quality of the embedded image (i.e., less distortion due to embedding). Even if the signature image has much texture information like a tiger picture, the embedded image cannot be visually distinguished from the original host image. Two sets of experimental results are presented. In the first, for data hiding applications, results of signature image reconstruction from JPEG lossy compressed images for varying scale factors are shown. In the second, for watermarking applications, we



(a) $\alpha = 5$ (b) $\alpha = 7$ (c) $\alpha = 11$

FIGURE 3. Embedded images using the hat-girl image as signature at varying scale factors.



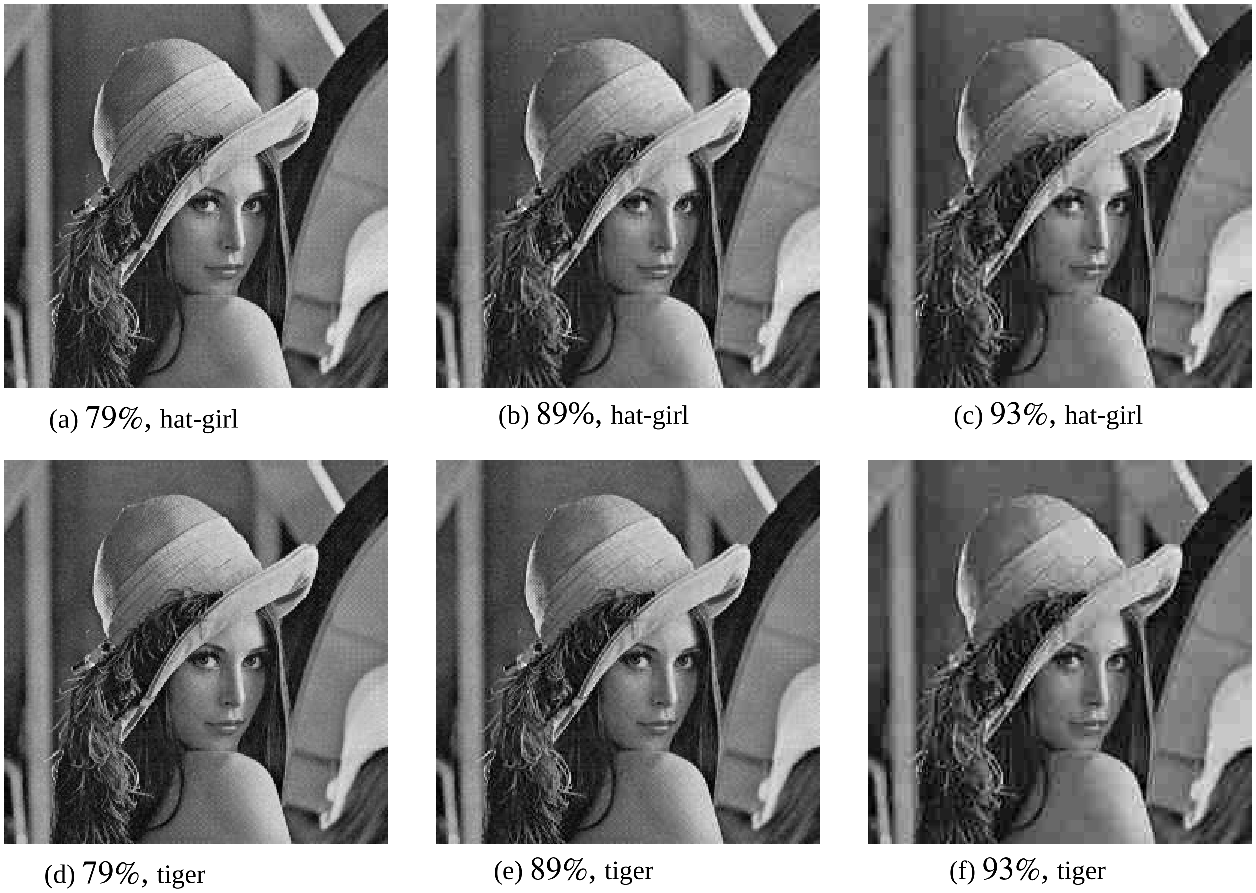
(a) $\alpha = 5$ (b) $\alpha = 7$ (c) $\alpha = 11$

FIGURE 4. Embedded Lena image using the tiger image as signature at varying scale factors.

present results of signature detection from these lossy compressed images. Figure 5 shows the embedded Lena image at various levels of JPEG compression for a scale factor of $\alpha = 7$.

For data hiding purposes it is reasonable to choose a larger scale factor in the Equation (1) as one is not too concerned about degradation due to image processing operations. In hiding one image in another, it is more important to ensure that the quality of the watermarked image is as close to the original as possible, with very little visual distortion. Almost perfect reconstruction is possible when there is no further image processing of the watermarked images. This can be seen from the reconstructed hat-girl and tiger images (at low JPEG compression levels) in Figure 6.

For copyright protection and authentication purposes it is important that the watermarked images are robust to typical image processing operations. Typically the signature data consume significantly fewer bytes than the host image and as such can be spatially distributed. The results we show here are for lossy JPEG compression where the signatures are gray scale images, and it is reasonable to expect that one can obtain much better results if the signatures are binary images of much lower dimensions. Lower values for the scale factor in Equation (1) should be used when it is likely that the images undergo significant distortion. Figure 7 shows recovered signatures for JPEG compression of 93% for varying scale factors. As



(a) 79%, hat-girl (b) 89%, hat-girl (c) 93%, hat-girl

(d) 79%, tiger (e) 89%, tiger (f) 93%, tiger

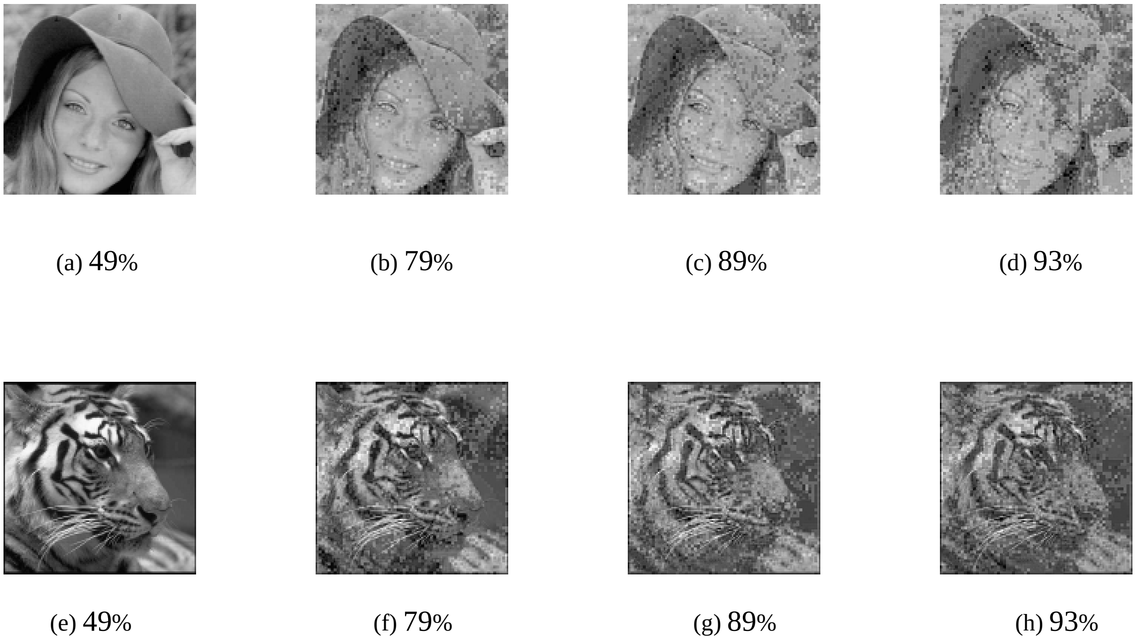
FIGURE 5. JPEG compressed embedded Lena image. The compression factor and the signature image used are indicated below each image. The scale factor used was $\alpha = 7$.

expected, images embedded with larger scale factor result in poor reconstruction for the same compression factor. Figure 8 shows another example wherein a different host image is used to embed the signatures.

In checking for the presence of a signature, the quality of the reconstruction of the signature itself is not an issue. A binary decision for the presence or absence of a signature need to be made. We use a measure similar to the one defined in [3] to compute the cross correlation between the recovered signature $s^*(m, n)$ and the original signature $s(m, n)$ in the wavelet transform domain. This similarity is defined as:

$$S = \frac{\sum_{m, n} s^*(m, n) s(m, n)}{\sum_{m, n} (s^*(m, n))^2} \tag{2}$$

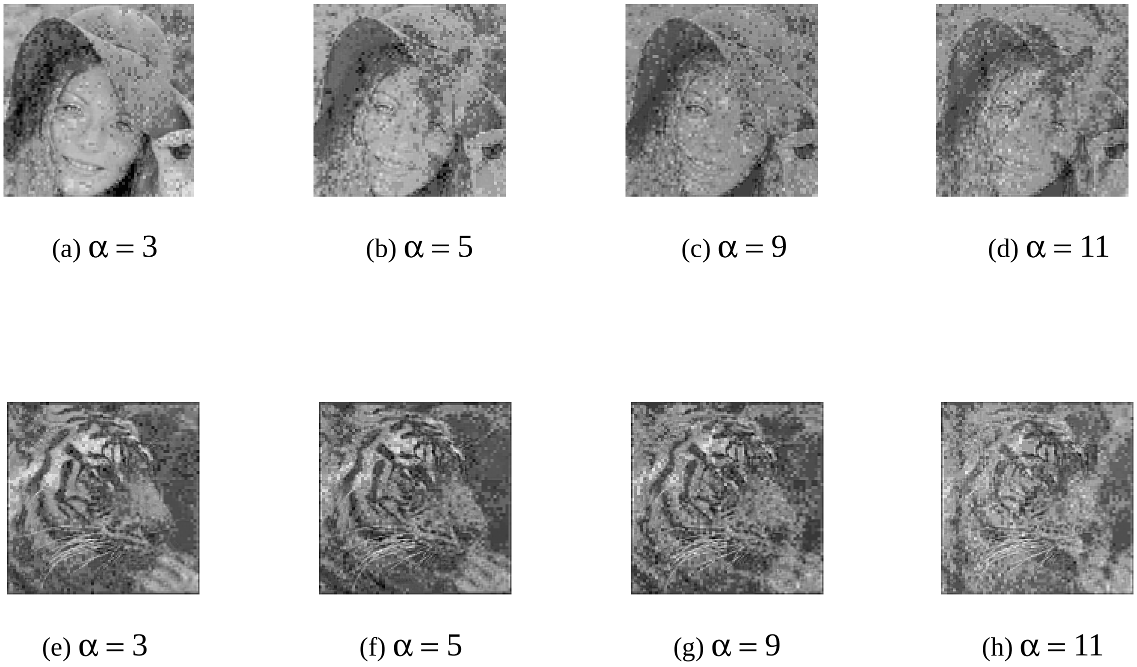
Note that the similarity computed as above does not guarantee that the maximum value is 1.0. A graph of this similarity for varying JPEG compression and for different scale factors α for two different examples are shown in Figure 9. As can be seen from this graph, it is easy to find a threshold for signature detection between unwatermarked and watermarked images.



(a) 49% (b) 79% (c) 89% (d) 93%

(e) 49% (f) 79% (g) 89% (h) 93%

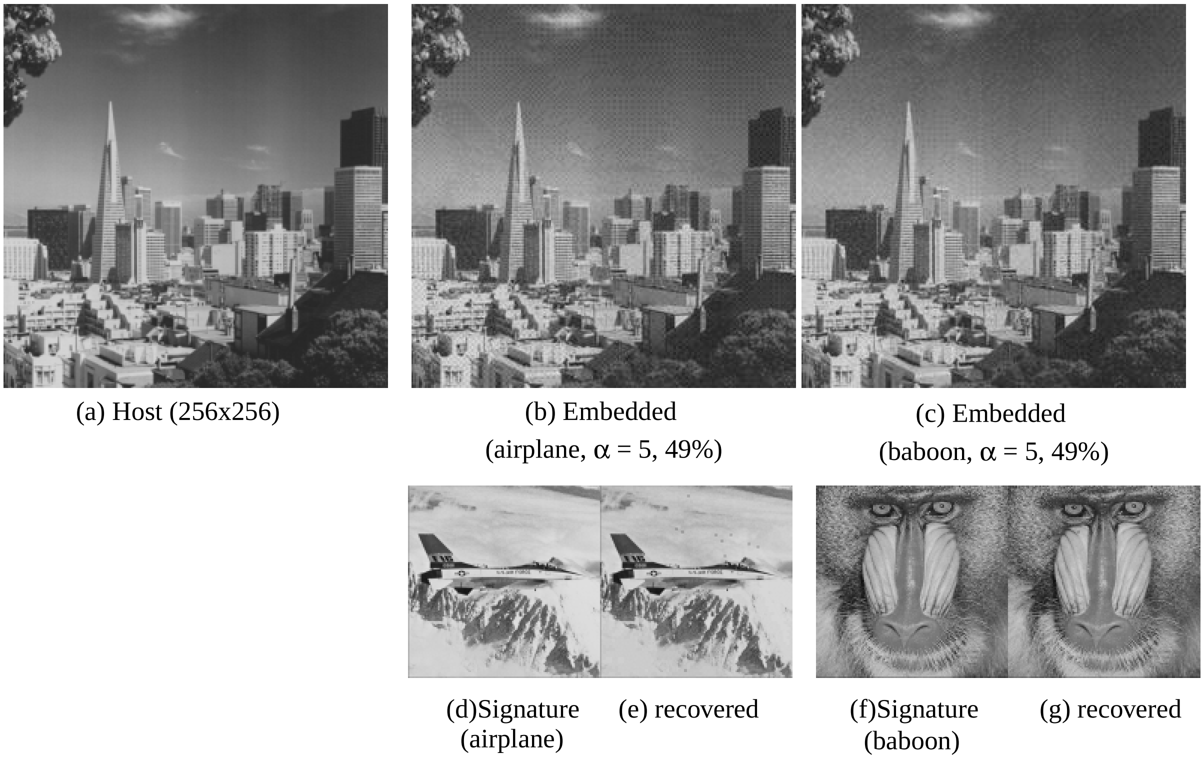
FIGURE 6. Recovered signature images for scale factor α = 5. The JPEG compression factor of the embedded image is indicated below each image.



(a) $\alpha = 3$ (b) $\alpha = 5$ (c) $\alpha = 9$ (d) $\alpha = 11$

(e) $\alpha = 3$ (f) $\alpha = 5$ (g) $\alpha = 9$ (h) $\alpha = 11$

FIGURE 7. Recovered hat-girl and tiger signature image from 93% JPEG (lossy) compressed embedded images for different scale factors.



(a) Host (256x256)

(b) Embedded (airplane, $\alpha = 5$, 49%)

(c) Embedded (baboon, $\alpha = 5$, 49%)

(d)Signature (airplane)

(e) recovered

(f)Signature (baboon)

(g) recovered

FIGURE 8. Another example of data embedding. (a) host image, (b) and (c) are embedded images using the signature images (d) and (f), respectively. (e) is the recovered image from b) and (g) is the recovered image from (c).

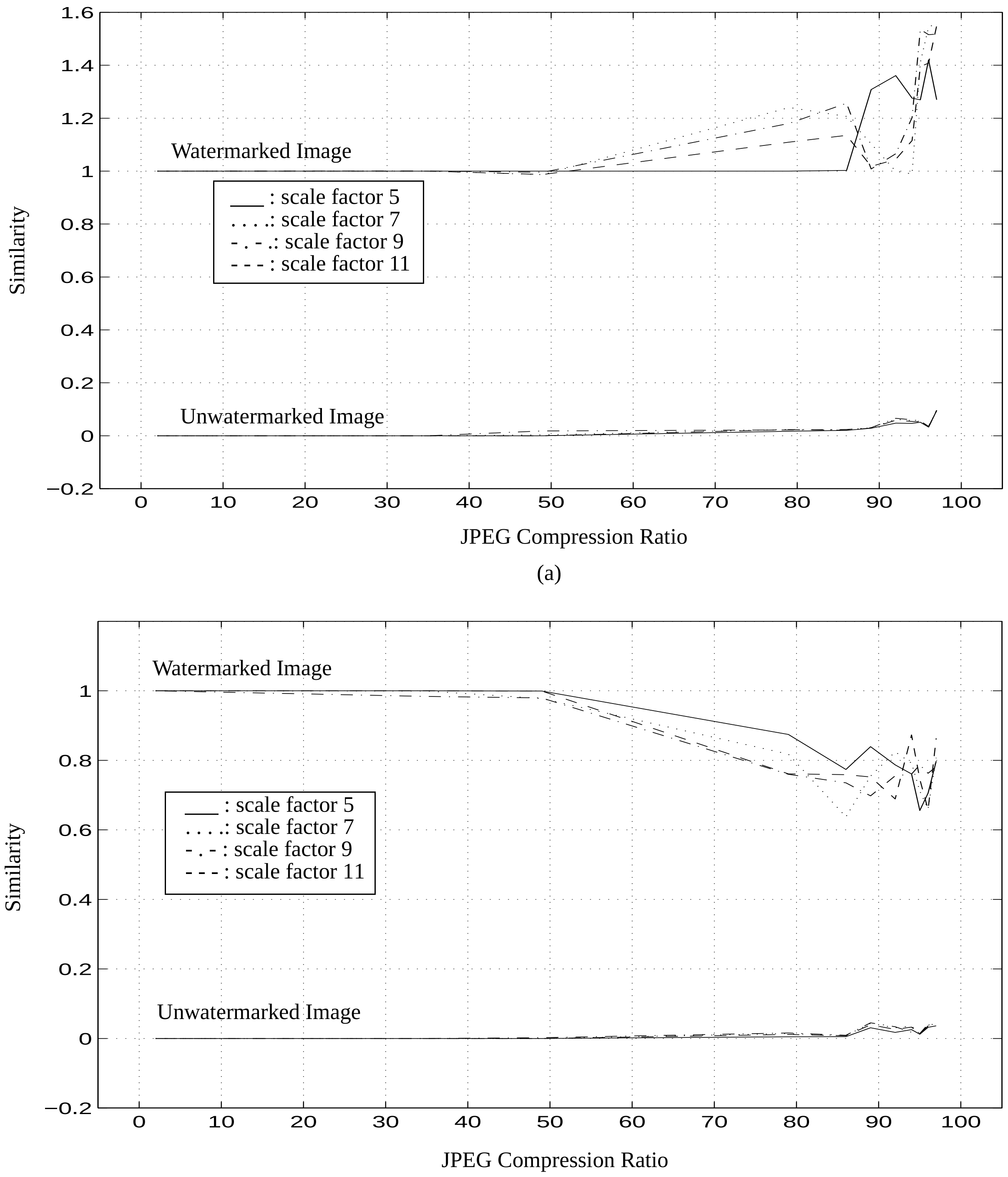
4 DISCUSSIONS

A scheme for image embedding is presented. This approach could be used for both digital watermarking related applications as well as for data hiding purposes. The scale factor in (1) controls the relative amount of host and signature image data in the embedded image. A larger scale factor can be used for data hiding where it is desirable to maintain the perceptual quality of the embedded image. A lower scale factor is better suited for watermarking where robustness to typical image processing operations is needed. Experimental results demonstrate that good quality signature recovery and authentication is possible when the images are quantized and JPEG compressed by as much as 90%.

Even though the Haar wavelet basis was used in the experiments, the method can be easily adopted to other wavelet transforms and for more than one level of decomposition. It might be worth exploring the use of other basis functions depending on the characteristics of the host and signature images. In some cases, particularly when the host image background lacks texture whereas the signature image has lot of texture, one can see a *noisy* background in the embedded image.

In digital watermarking, the signatures are usually of much smaller dimensions (in terms of number of bytes needed) compared to the host image. Since the proposed method can manage a significantly larger number of signature data, it is possible to distribute the signature spatially as well, thus making watermarking robust to operations such as image cropping.

ACKNOWLEDGMENTS: This work was supported in part by grants from NSF (award #94-1130) and NASA (#NAGW 3951). The authors would like to thank Jay Winkeler for his comments.



(a)

(b)

FIGURE 9. Checking for the presence of a signature in lossy compressed images. (a) the host image is Lena and the signature is the tiger image, (b) host image is from Figure 8(a) and the signature is the airplane image (Figure 8(d)). Note that it is easy to identify a threshold for watermark detection in both cases.

REFERENCES

[1] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for Data Hiding," *Proceeding of the SPIE, Storage and Retrieval for Image and Video Database III,* Vol. 2420, pp.164-173, San Jose, Feb., 1995.

[2] J. J. O Rauanaaidh, W. J. Dowling, and F. M. Boland, "Watermarking Digital Images for Copyright Protection," *IEE Proceeding of Vision, Image, Signal Processing*, Vol. 143, no. 4, pp.250-256, Aug., 1996.

[3] I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, "A secure Robust watermark for Multimedia," *Information Hiding, Lecture Notes in Computer Science*, Vol. 1174, pp.183-206, 1996.

[4] S. Craver, N. Memon, B. Yeo, and M. Yeoung, "Can Invisible Watermarks Resolve Rightful Ownership?," *Proceeding of the SPIE, Storage and Retrieval for Image and Video Database V,* Vol. 3022, pp.310-321, San Jose, Feb., 1997.

[5] R. G. van Schyndel, A. Z. Tirkel and C. F. Osborne, "A Digital Watermark," *Proceeding of IEEE International Conference of Image Processing,* Vol. 2, pp. 86-90, Austin, Nov., 1994

[6] M. D. Swanson, B. Zhu and A. H. Tewfik, "Robust Data Hiding for Images," *In IEEE Digital Signal Processing Workshop (DSP 96),* pp. 37-40, Norway, Sep., 1996.

[7] G. Voyatzis and I. Pitas, "Embedding Robust Watermarks by the Chaotic Mixing," *In IEEE Digital Signal Processing Workshop (DSP 97),* Vol. 1, pp. 213-216, Greece, July 1997.

[8] J. Ohnishi and K. Matsui, "Embedding a Seal into a Picture under Orthogonal Wavelet Transform," *International conference on Multimedia and Computing and Systems,* pp.514-512, Japan, June, 1996.

[9] C. Hsu and J Wu, "Hidden signatures in Images," *International Conference on image Processing '96,* Vol. 3, pp.223-226, Sep., Switzer, 1996.

[10] W. Zeng, *Resilient video transmission and multimedia database applications,* Ph.D Dissertation, princeton Univ., June, 1997.

[11] M. M. Yeung, and F. C. Mintzer, "Digital Watermarking for High-quality Imaging," *IEEE first workshop on the Multimedia Signal Processing,* pp. 357-362, 1997

[12] F. Goffin, J.F. Delaigle, C. D. Vleeschouwer, B. Marq and J. -J. Quisquater, "A Low Cost Perceptive Digital Picture Watermarking Method," P*roceeding of the SPIE, Storage and Retrieval for Image and Video Database V,* Vol.3022, pp. 264-276, San Jose, Feb. 1997.

[13] B. Tao and B. Dickison, "Adaptive Watermarking in the DCT Domain," *1997 IEEE International Conference Acoustics, Speech, and Signal Processing*, Vol. 4, pp. 2985-2988, Munich, Germany, April, 1997

[14] G. Strang and T. Nguyen, *Wavelets and Filer Banks*, Wellesley-Cambridge Press, 1996.