An Embedded Data Using Slantlet Transform

*Iman Mohammed Ga'fer Alwan** *Enas Muzaffer Al-Ta'ee***

Received 1 , March, 2010
Accepted 14, January, 2011

Abstract:

Data hiding is the process of encoding extra information in an image by making small modification to its pixels. To be practical, the hidden data must be perceptually invisible yet robust to common signal processing operations. This paper introduces a scheme for hiding a signature image 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. The proposed algorithm uses orthogonal discrete wavelet transforms with two zero moments and with improved time localization called discrete slantlet transform for both host and signature image. A scaling factor α in frequency domain control the quality of the watermarked images. Experimental results of signature image recovery after applying JPEG coding to the watermarking image are included.

Key words: slantlet transform (ST), digital watermarking, data hiding, copyright protection, authentication.

Introduction:

Recently, more and more people communicate with each other by surfing on the Internet. However, it is not very secure when we transmit information through Internet. Everyone can peek, copy even alter our information easily in this wide open environment. Thus, we don't want to transmit the important information without any protection in the public network unless a secure channel is provided for the transmission [1]. 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 [2]. 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, 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

---

*Baghdad University, College of Education for Woman,
**Department of Computer Science

unauthorized person to detect or decode the hidden content.

Generally, digital watermarking /data hiding can be classified into two classes according to the watermark embedding domain, i.e., the spatial and the transform domain. The spatial domain watermarking exploits adding watermark to the pixels of image directly, but its disadvantage is that a common image processing may eliminate the watermark. Other than the spatial-domain watermarking, the transform domain scheme is typically more robust to filtering, compression, etc [3]. The methods using transform domain include DCT domain technique [4] and wavelet transform form [5].

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. In recovering the signature image, it is assumed that the original host image is available.

The proposed schemes distribute the signature information in the discrete slantlet transform domain of the host image. Spatial distribution of the discrete slantlet transform coefficients helps to recover the signature even when the images are compressed using JPEG lossy compression.

The proposed scheme focuses on hiding the signature mostly in the mid slantlet transform bands, stable reconstruction can be obtained even when the images are transformed, quantized (as in JPEG compression algorithm), or otherwise modified by enhancement or low pass filtering operations.

Slantlet Transform:

The Slantlet uses a special case of a class of bases described by [6], the construction of which relies on Gram-Schmidt orthogonalization. It is useful to consider first the usual two-scale iterated DWT filter bank and an equivalent form, which is shown in (Figure1). The “slantlet” filter bank described here is based on the second structure, but it will be occupied by different filters that are not products. With the extra degrees of freedom obtained by giving up the product form, it is possible to design filters of shorter length while satisfying orthogonality and zero moment conditions [7]. For the two-channel case, the shortest filters for which the filter bank is orthogonal and has K zero moments are the well known filters described by Daubechies [8]. For K = 2 zero moments the iterated filters of (Figure 1-b) are of lengths 10 and 4 but the slantlet filter bank with K = 2 zero moments shown in (Figure 2) has filter lengths of 8 and 4. Thus the two-scale slantlet filter bank has a filter length which is two samples less than that of a two-scale iterated Daubechies-2 filter bank. This difference grows with the number of stages.

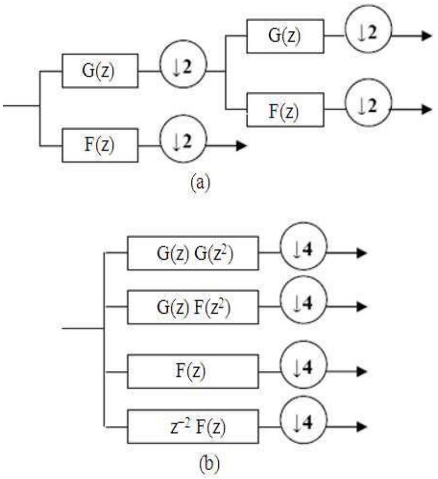


Fig. (1) Two-scale iterated filter bank and an equivalent structure

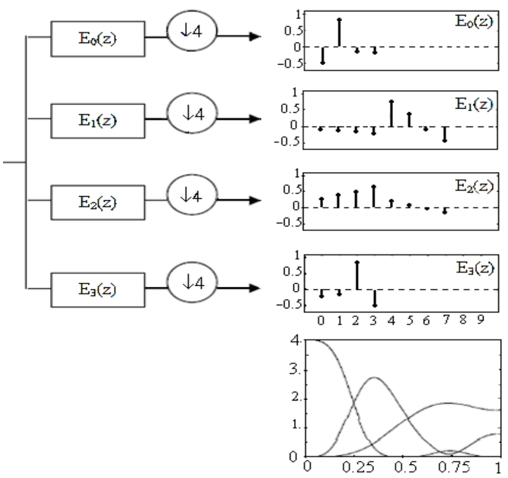


Fig. (2) Two-scale filter bank structure using the slantlet

Some characteristic features of the Slantlet filter bank are orthogonal, having two zero moments and has octave-band characteristic. Each filter bank has a scale dilation factor of two and provides a multi-resolution decomposition. The slantlet filters are piecewise linear. Even though there is no tree structure for Slantlet, it can be efficiently implemented like an iterated DWT filter bank [9]. Therefore, computational complexities of the Slantlet are of the same order as that of the DWT. The filter coefficients used in the slantlet filter bank as derived in by Selesnick [9] are:

$$G_1(z)=\left(-\frac{\sqrt{10}}{20}-\frac{\sqrt{2}}{4}\right)+\left(\frac{3\sqrt{10}}{20}+\frac{\sqrt{2}}{4}\right)z^{-1}+\left(-\frac{3\sqrt{10}}{20}+\frac{\sqrt{2}}{4}\right)z^{-2}+\left(\frac{\sqrt{10}}{20}-\frac{\sqrt{2}}{4}\right)z^{-3} \quad \ldots(1)$$

$$F_2(z)=\left(\frac{7\sqrt{5}}{80}-\frac{2\sqrt{55}}{80}\right)+\left(-\frac{\sqrt{5}}{80}-\frac{\sqrt{55}}{80}\right)z^{-1}+\left(-\frac{9\sqrt{5}}{80}+\frac{\sqrt{55}}{80}\right)z^{-2}+\left(-\frac{17\sqrt{5}}{80}+\frac{3\sqrt{55}}{80}\right)z^{-3}$$
$$+\left(\frac{17\sqrt{5}}{80}+\frac{3\sqrt{55}}{80}\right)z^{-4}+\left(\frac{9\sqrt{5}}{80}+\frac{\sqrt{55}}{80}\right)z^{-5}+\left(\frac{\sqrt{5}}{80}-\frac{\sqrt{55}}{80}\right)z^{-6}+\left(-\frac{7\sqrt{5}}{80}-\frac{3\sqrt{55}}{80}\right)z^{-7} \quad \ldots(2)$$

$$H_2(z)=\left(\frac{1}{16}+\frac{\sqrt{11}}{16}\right)+\left(\frac{3}{16}+\frac{\sqrt{11}}{16}\right)z^{-1}+\left(\frac{5}{16}+\frac{\sqrt{11}}{16}\right)z^{-2}+\left(\frac{7}{16}+\frac{\sqrt{11}}{16}\right)z^{-3}$$
$$+\left(\frac{7}{16}-\frac{\sqrt{11}}{16}\right)z^{-4}+\left(\frac{5}{16}-\frac{\sqrt{11}}{16}\right)z^{-5}+\left(\frac{3}{16}-\frac{\sqrt{11}}{16}\right)z^{-6}+\left(\frac{1}{16}-\frac{\sqrt{11}}{16}\right)z^{-7} \quad \ldots(3)$$

Data Embedding:

As mentioned earlier, watermark should be robust to typical image processing operations, including lossy compression. Compression technique typically affects 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 creates problems if one is interested in visible watermarks. This is particularly true in data hiding applications where the data to be hidden could be a significant percentage of the original data.

This work proposes the use of a slantlet transform to embed signature information in different frequency bands. Both the signature data, which in this case is another image, and the host image data, are decomposed using the discrete slantlet transform (DST).

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 images used in the experiments are shown in (Figure 3).


(a)Host (256 x 256) (b)signature images (128 x 128)

Fig. (3) (a) A host image and (b) signature images, radar image and a butterfly image

Embedding occurs in the slantlet transform domain as the slantlet 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 4).

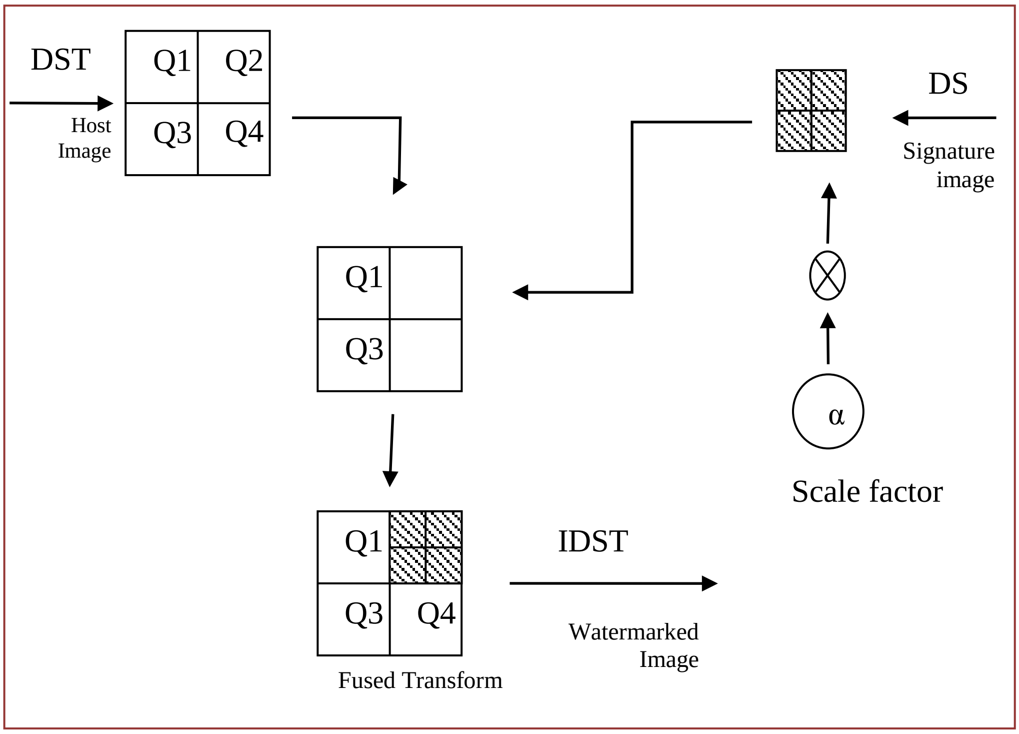


Fig. (4) A schematic of the data embedding approach

The basic steps for embedding the signature coefficients into the host image coefficients are:

1- Decompose the host (NxN) and the signature (N/2 x N/2) images using the DST. This results in different bands (Figure5).
2- Replace the coefficients of the host image in the second quarter Q2 where midband frequencies reside there (Figure 4) with the

coefficients of the signature image multiplied by α, where α is the strength of the watermark controlling the level of the watermark.

$h(m,n)= \alpha s(k,j)$; where m=1 to N/2, n= N/2 +1 to N, k, j= 1 to N/2. (4)

3- Take the inverse slantlet transform for the fused transform coefficients to give the watermarked image.

(a) DST of host image

(b) DST of signature image

Fig. (5) The slantlet transformed image for (a) host image, (b) signature image.

Results:

The results of embedding 128x128 gray scale (one byte per pixel) signature images in a 256x256 Lena image. Two images, one a radar image and the other an image of butterfly, are used as signature images are presented in the following experiments. (Figure1) shows the host and signature images.
The quality of the image is obtained by computing the peak signal- to- noise ratio (PSNR), of the reconstructed image is obtained using (5).

$$PSNR= 20 \log 10 (N/RMSE) \text{ dB} \quad (5)$$

where N is the largest possible value of the signal in the image and RMSE is the root mean square error. Typical PSNR values range between 20 and 40 for good quality [10].
(Figure 6) and (Figure 7) show the PSNR of the embedded Lena images using different scale factors with respect to the original one and the reconstructed signature images. Note that the lowest the scale factor (less than 1), 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 butterfly image, the embedded image cannot be visually distinguished from the original host image. From experimental results the best value of α lies between (0.05-0.1) in which better signature image reconstruction can be obtained.

(a)α =1.0, PSNR= 11.66dB (b)α =0.3, PSNR=21.77dB (c)α =0.08, PSNR= 30.01dB

The reconstructed image for α =1.0 α =0.3 α =0.08

(d) α =0.05, PSNR=31.34dB The reconstructed image for α =0.05

Fig. (6) Embedded images using the radar image as signature at varying scale factors and the reconstructed image.

(a) α =1.0 (b) α =0.3 (c) α =0.08

The reconstructed images for α =1.0 α =0.3 α =0.08

(d) α =0.05 The reconstructed image for α =0.05

Fig. (7) Embedded images using the butterfly image as signature at varying scale factors and the reconstructed butterfly image.

The embedded image was compressed by using JPEG compression system to study the effect of compression on the proposed system. (Figure8) shows the embedded Lena image at various levels of JPEG compression for a scale of α=0.05.

The compression ratio used is [10]:

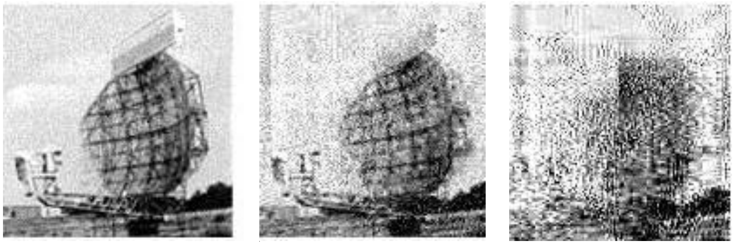
CR= (size of compressed file/size of uncompressed file)*100% (6)

(Figure 9) shows the result of the signature image reconstruction from JPEG lossy compressed images for varying compression ratio. The reconstructed signature images are of good perceptual characteristics especially for low compression ratios.

(a) 75%, butterfly (b) 88%, butterfly (c) 93.75%, butterfly

(a) 75%, radar (b) 88%, radar (c) 93.75%, radar

Fig. (8) JPEG compressed embedded Lena image. The compression ratio and the signature image used are indicated below each image. The scale factor used was α=0.05



(a) 50% (b) 75% (b) 88%

(a) 50% (b) 75% (b) 88%

Fig. (9) Recovered signature images for scale factor α=0.07. The compression ratio of the embedded image is defined below each image.

Conclusion:

From the results of the proposed system, one can deduce the following:

i. The proposed algorithm can produce imperceptible change to the host image when the scaling factor α lies between (0.05-0.1).

ii. Using slantlet transform which provides multi-resolution decomposition offered good characteristics of both host and signature images decomposition, making the hiding algorithm effective. Also if one wants to attack the watermarked image, he must know the restriction of the embedding algorithm (type of transform, region of hiding and value of scaling factor).

iii. Experimental results demonstrate the good quality signature recovery is possible when the images are quantized and JPEG compressed by as 80% .

References:

[1] Kao, C.H. and Hwang, R.J. 2005. Scale Image Information Hiding in Loss Compression Gray. Tamkang J.Sci & Eng., 8(2):99-108.

[2] Voyatzis, M. and Pitas, I. 1997. Embedded Robust Watermarking by the Chaotic Mixing, IEEE DSP Workshop (DSP 97). 1: 213-216.

[3] Huo, F. and Gao, X. 2006. A Wavelet Based Image Watermarking Scheme, IEEE, ICIP. 1:2573-2576.

[4] Rauanaaidh, J.J., Dowling, W.J. and Boland, F.M. 1996. Watermarking Digital Images for Copyright Protection, IEEE Proc. VISP.143(4):250-256.

[5] Hameed, K., Mumtaz, A. and Gilani, S.A.M. 2006. Digital Image Watermarking in The Wavelet Transform Domain, World Academy J.Sci., & Tech.13:86-89.

[6] Alpert, B., Coifman, G.R., and Rokhlin, V., 1993. Wavelet-like bases for the fast solution of second kind integral equations, SIAM J.Sci. Comput., 14:159-184.

[7] Panda, G., Dash, P.K., Pradhan, A.K. and Meher, S.K., 2002. Data compression of power quality events using the slantlet transforms, IEEE Trans. Power Delivery, 17:662-667.

[8] Daubechies, I., 1992. Ten Lectures on Wavelet, Society for Industrial and Applied Mathematics, Philadelphia, PA., ISBN:0-89871-274-2 :354.

[9] Selesnick, I.W., 1999. The Slantlet Transform, IEEE Trans. Signal Process. 47(5):1304-1312.

[10] Poobal, S., and Ravindran, G., 2006. Arriving at an Optimum Value of Tolerance Factor for Compressing Medical Images, World Academy J.Sci. Eng. Tech 24:169-173.

إخفاء البيانات باستخدام تحويلة المويّل

إيمان محمد جعفر علوان* ***إيناس مظفر الطائي*****

*جامعة بغداد- كلية التربية للبنات
**قسم علوم الحاسبات

الخلاصة:

إخفاء البيانات هي عملية ترميز معلومات إضافية في الصورة الرقمية بواسطة إحداث تغيير صغير في قيم النقاط الخاصة بها. عمليا عملية إخفاء البيانات يجب أن تكون غير مرئية كذلك متينة لعمليات الضغط و الترشيح للترددات الواطئة. هذا البحث يقدم أسلوب إخفاء صورة رقمية بأبعاد تصل إلى ربع أبعاد الصورة المضيفة. أن النظام المقترح يستعمل تحويلة المويّل التي تعتبر تحويلة مويجة متعامدة مع تحسين في تمركز الوقت لكلا من الصورة المراد إخفائها(signature) والصورة المضيفة (cover) ومن ثم إخفاء الصورة (signature) في مدى ترددي مناسب للصورة المضيفة. المعامل α في مجال تحويلة المويّل يتحكم في جودة الصورة الناتجة. تقنيات الإخفاء والاستخلاص للصورة موضحة في هذا البحث بالإضافة إلى نتائج تأثر النظام بعملية الضغط من نوع JPEG.