An Image Watermarking Scheme using HVS Characteristics and Spread Transform

Santi P. Maity
Bengal Engineering College (DU),
Dept. of Electronics and Telecommunication Engg.
P.O.-Botanic Garden, Howrah 711 103, India
spmaity@telecom.becs.ac.in

Malay K. Kundu
Indian Statistical Institute
Machine Intelligence Unit
203 B. T. Road, Kolkata 700 108, India
malay@isical.ac.in

Abstract

The paper presents a robust digital image watermarking scheme that uses both the characteristics of the human visual system (HVS) and statistical information measure. Spread transform approach is used where data is embedded through transform coeff icients of both the cover and the watermark data. The spread transform watermarking technique yields better results in terms of imperceptibility, resiliency, capacity and cost compared to widely used spread spectrum watermarking schemes. Hadamard transformation is used not only for simpler implementation but also for its higher data hiding capacity [1]. Experimental results show that the visual quality of the extracted watermark is good in spite of several external attacks. The fact is also supported by mutual information values used as objective measure.

1. Introduction

Recently watermarking is used widely for ownership protection, authentication, and content integrity verification of intellectual property in digital form. Several watermarking techniques for digital images have been proposed in the literature where the characteristics of HVS (human visual system) further improves the imperceptibility and robustness performance of traditional spread spectrum watermarking schemes. Cox et.al proposed a global DCT (Discrete Cosine transform) based spread spectrum watermarking [2] and Podilchuck and Zeng proposed perceptual model-based watermarking scheme using DCT and Wavelet transform [3]. The embedded watermark signal in both cases consists of a sequence of real numbers that are normally distributed but does not convey unique signature. Hence, their detection methods depend on similarity measurement that needs the inevitable presence of watermark signal at the receiver. We use spread transform watermarking scheme in order to achieve better imperceptibility and resiliency, although our spread transform scheme is different to that of Chen and Wornell scheme [4]. In our scheme, transform coefficients of the watermark image modulate the corresponding significant transform coefficients of the cover image according to the Watson model of HVS [5]. We use meaningful gray scale image as watermark so that it not only conveys a unique information but also shows a good degree of resiliency after various forms of image distortion. Hadamard transformation used offers low computation cost and higher data hiding capacity at low quality factor compression [6]. Although our decoding method is based on objective measure like mutual information, but subjective quality of the extracted image is also visually acceptable.

2. Watermark embedding and decoding

We use in this work gray scale image for both the cover and the watermark image.

2.1. Watermark embedding

Step I: Spatial dispersion of watermark image
The watermark image is spatially dispersed using a cryptic key (k) generated by linear feedback shift register. The process converts gray scale watermark image into noise-like image and thus increases imperceptibility by spreading watermark information over wide region of the cover image.

Step II: Image transformation
The block (8×8) based Hadamard transformation is applied over both the cover and the spatially dispersed watermark image.

Step III: Image dependent permutation
In order to increase imperceptibility, the transform coefficients of the cover and the watermark image are sorted in ascending order.

Step IV: Generation of modulation function
We construct modulation function based on Watson visual [5] and entropy masking model. Watson relates frequency sensitivity $(F_{u,v,b})$, luminance masking $(L_{u,v,b})$ and contrast masking $(C_{u,v,b})$ with the DCT coefficients according

0-7695-2128-2/04 $20.00 (C) 2004 IEEE

to the following relations :

$$L_{u,v,b} = F_{u,v,b}\frac{(X_{0,0,b}}{X_{0,0})^{\alpha}}$$

$$C_{u,v,b} = max[L_{u,v,b}, \left|X_{u,v,b}\right|^{\beta_{u,v}}(L_{u,v,b)^{1-\beta_{u,v}}}]$$

where $X_{0,0,b}$ is the dc coeffi*c*ient of the block "b", $X_{0,0}$ is the average of all $X_{0,0,b}$'s, which corresponds to the mean luminance of the display, $X_{u,v,b}$ is the (u,v) th DCT coeffi*c*ient of the block "b" and α and $\beta_{u,v}$ are set to 0.649 and 0.7 to control the degree of luminance sensitivity and contrast sensitivity respectively. We assume that these relations also hold good for Hadamard coeffi*c*ients. In our present work, we link contrast masking with the entropy masking according to the following relations [6].

$$V_{u,v,b} = max[C_{u,v,b}, \left|C_{u,v,b}\right|(E_{u,v,b)^{\gamma}}]$$

$$E_{u,v,b} = \sum_{x \in N(x_{u,v,b})} p(x)e^{1-p(x)}$$

where $E_{u,v,b}$ is the entropy of $N(X_{u,v,b})$ which is set of $X_{u,v,b}$'s eight neighbors. In this model we use exponential function for entropy measure rather than Shannonian form. It has been shown in [7] that this form of non- Shannonian entropy function captures local and global pictorial information in a better way compared to that of Shannonian entropy function. We extend the use of this function in transform domain analysis. The γ value is chosen experimentally to make the $E_{u,v,b}$ work only when it is larger than 1.0. In deriving the modulation function, we use the popular JPEG quantization table for frequency sensitivity. It is assumed that a quantization step Q follows $Q/2$ allowable distortion, and each entry of $F_{u,v}$ is set to the half value of the quantization table.

Step V: Watermarked image formation

After the formation of modulation function, the data is embedded according to the following relation.

$$X^{m}_{u,v,b} = X_{u,v,b} + sgn(X_{u,v,b})V_{u,v,b}\frac{\left|Y_{u,v,b}\right|}{max(Y_{u,v})}$$

if $\left|X_{u,v,b}\right| > V_{u,v,b}$, otherwise

$$X^{m}_{u,v,b} = X_{u,v,b}$$

where

$$sgn(X_{u,v,b}) = \begin{cases} -1 & \text{if} \quad X_{u,v,b} \geq 0.0 \\ 1 & \text{if} \quad X_{u,v,b} < 0.0 \end{cases}$$

$X^{m}_{u,v,b}$ is the data embedded (u,v)th coeffi*c*ient of block "b". $X_{u,v,b}$ is the coeffi*c*ient of the cover image in block "b", $V_{u,v,b}$ is the modulation index obtained after frequency, luminance, contrast and entropy masking, $Y_{u,v,b}$ is the coeffi*c*ient of watermark image which is responsible to modulate $X_{u,v,b}$ and max$Y_{u,v,b}$ is the maximum value of the coeffi*c*ients for watermark image.

We def*i*ne a term as "mod" where

$$mod = sgn(X_{u,v,b})\frac{V_{u,v,b}}{maxY_{u,v,s}}$$

It is observed that better result is achieved if we replace mod by $mod/10$ when (i) $mod.\left|Y_{u,v,b}\right| > 10.0$ and mod by $mod.3$ when (ii) $mod.\left|Y_{u,v,b}\right| < 3.0$. The is because the modifi*c*ation (i) reduces the effect of visual distortion for the relatively high transform coeffi*c*ients of the watermark data and the modifi*c*ation (ii) improves the retrieval of the relatively smaller transform coeffi*c*ients of the watermark data from the distorted watermarked image. After watermark embedding with the new modulation function, block based inverse Hadamard transform is applied and watermarked image is formed.

2.2. Watermark decoding

The extraction of watermark information is given by the following relation:

$$Y^{e}_{u,v,b} = (X^{'}_{u,v,b} - X_{u,v,b}).mod$$

where $X^{'}_{u,v,b}$ are the data embedded coeffi*c*ients of the possibly distorted watermarked image, $X_{u,v,b}$ is the coeffi*c*ient of the cover image and $Y^{e}_{u,v,b}$ are the coeffi*c*ients of the extracted watermark image. The transform coeffi*c*ients of the extracted watermark are placed in the respective positions and block based inverse Hadamard transformation is applied to obtain the watermark image.

A quantitative estimation of robustness effi*c*iency of the extracted image $W^{'}(x,y)$ is $I(X;Y)$, the mutual information of X and Y where random variables X and Y represent respectively the original watermark and its decoded version obtained from the distorted watermarked image. $I(X;Y)$ represents the average amount of information received from the signal degradation and is represented by

$$I(X;Y) = \sum_{i}\sum_{j} p(x_i)p(y_j/x_i)\log\frac{p(y_j/x_i)}{\sum_i p(x_i)p(y_j/x_i)}$$

where $p(x_i)$ represents the probability of occurrence of the i-th pixel value in watermark image and $p(y_j/x_i)$ represents the channel matrix.

3. Results

We test resiliency of the scheme against various image degradation over large number of benchmark images [8]. Fishing boat (f*i*gure 3(a)) is a test image of size (256×256),

8 bits/ pixel gray image and watermark image (figure 3(b)) is 4 bits/pixel (64×64) gray image. Attack and embedding distortions are measured by Peak Signal to Noise Ratio (PSNR) while the security of the hidden data is measured using relative entropy distance (Kulback Leibler distance). The high PSNR values of the watermarked images ($\sim 38dB$) with respect to the cover images and low security values (~ 0.005423) indicate better imperceptibility and security of the hidden data. Figures 1 and 2 show the robustness results graphically for various image degradation. We also test the resiliency of the scheme against multiple watermark embedding. Figure 4(l) shows extracted watermark image after collusion attack (figure 4(k)) with five watermark images (figure 4(o) and (p) show two such images) embedded separately in the same cover image and averaged. We also test the resiliency considering embedder as an attacker i.e. embedding multiple watermarks in the same cover image successively and it is always found that the first embedded watermark always possess high mutual information value. This solves the problem of finding out the rightful ownership.

4 Conclusion

The scheme describes a robust hiding of image like information in an image. The use of HVS characteristics and spread transform approach improves resiliency against various unintentional as well as deliberate attacks. In case of multiple watermark embedding, the scheme shows resiliency and also solves the problem of finding out the rightful ownership. The use of Hadamard transformation not only reduces the computation cost due to its simplicity of kernels but also improves data hiding capacity against lossy compression which is further improved by attack adaptive negative modulation scheme. Moreover, for on line implementation using hardware module, Hadamard transformation is a good candidate for designing such module because of its non trigonometric and identical kernels for both forward and inverse transformation [9],[10].

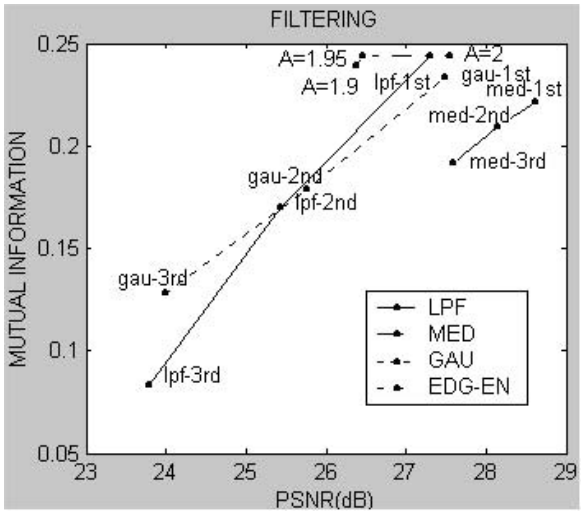

Figure 1. Results of image filtering

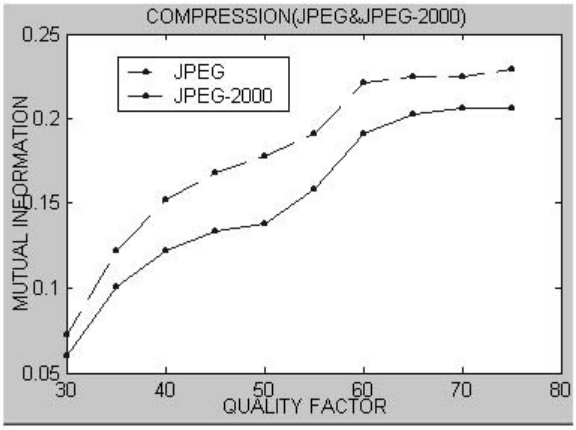

Figure 2. Results of image compression

Reference

[1] M. Ramkumar and A. N. Akansu, Capacity estimates for data hiding in compressed images, *IEEE Transactions on Image Processing*, 10:1252-1263,2001.

[2] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Transaction on Image Processing* 6(12): 1673-1687, 1997.

[3] C. I. Podilchuk and W. Zeng, Image adaptive watermarking using visual models, *IEEE Journal on Selected Areas in Communications* 16:525-539,1998.

[4] B. Chen and G.W. Wornell, Achievable performance of digital watermarking systems, *Proceedings of the IEEE Conf. on Multimedia Computing and Systems*, 1:13-18, June 1999 .

[5] A. B. Watson, DCT quantization matrices visually optimized for individual images, *Proc. SPIE Conf. Human Vision, Visual Processing, and Digital Display IV*, 1913:202-216, 1993.

[6] S. Suthaharan, S. W. Kim, H. K. Lee, and S. Sathananthan, Perceptually tuned robust watermarking scheme for digital images, *Pattern Recognition Letters*, 21:145-149, 2000.

[7] N. R. Pal and S. K. Pal,Object-back ground segmentation using new definitions of entropy, *IEE Proceedings*, 136:284-295, 1989.

[8] http:// www.cl.cam.ac.uk/ fapp2/watermarking.

[9] C. P. Fan and J. F. Yang, Fixed-pipeline two-dimensional Hadamard Transform algorithms, *IEEE Transactions on Signal Processing*, 45(6):1669-1674, June 1997.

[10] Chpdir(www.xs4all.nl/ ganswijk/chipdir).

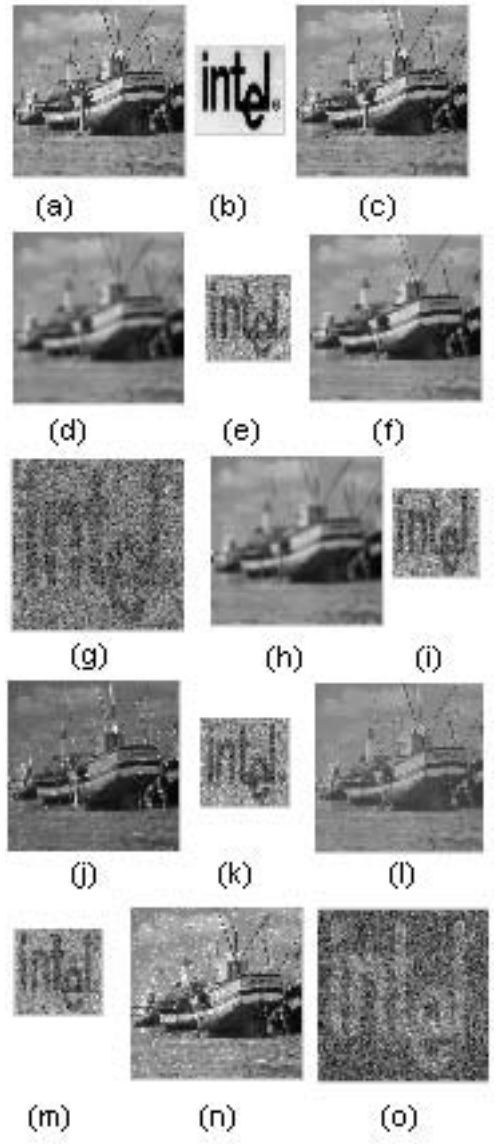

Figure 3. (a): test image, (b): watermark image, (c): watermarked image, (d):watermarked image after mean f*i*ltering with window size (11×11), (e): extracted watermark from (d), (f): watermarked image after median f*i*ltering with window size (9×9), (g): extracted watermark from (f), (h): watermarked image after f*i*ve times gaussian f*i*ltering with variance 1, window size (9×9), (i): extracted watermark from (h), (j): watermarked image after edge enhancement (PSNR 18.23 dB), (k): extracted watermark from (j), (l): watermarked image after dynamic range change from (254-1) to (200-50), (m): extracted watermark from (l), (n): watermarked image after noise addition, (o): extracted watermark from (n).

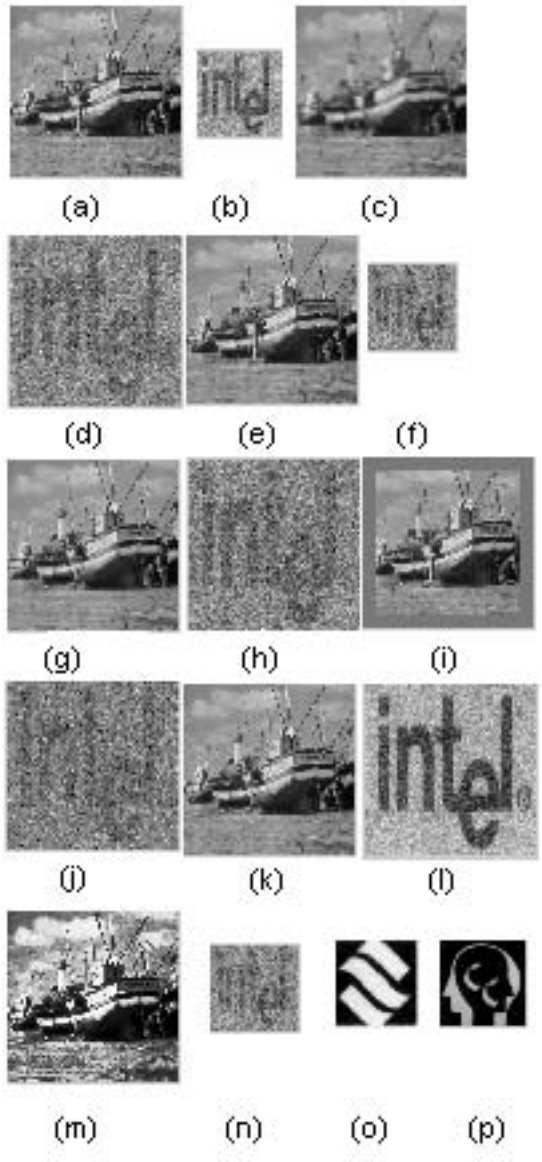

Figure 4. (a): watermarked image after four least signif icant bits f lipping, (b): extracted watermark image from (a), (c): watermarked image after rescaling from its one-fourth size, (d): extracted watermark image from (c), (e): watermarked image after JPEG compression (quality 25), (f): extracted watermark from(e), (g): watermarked image after JPEG 2000 compression (quality 35), (h): extracted watermark from (g), (i): watermarked image after cropping(making the pixel values '0'for 20 rows and columns from both sides of the watermarked image), (j): extracted watermark from (i), (k): watermarked image after collusion attack (the same cover image is embedded by f ive different watermark images separately and averaged), (l): extracted watermark from (k), (m): watermarked image after histogram equalization, (n): extracted watermark from (m), (o): watermark image, (p): watermark image.