Performance Factors Analysis of a Wavelet-based Watermarking Method

Chaw-Seng Woo[1], Jiang Du[1], Binh Pham[2]

[1]Information Security Research Centre (ISRC)
[2]Faculty of Information Technology
Queensland University of Technology
GPO Box 2434, Brisbane, QLD4001, AUSTRALIA

cs.woo@student.qut.edu.au, j.du@isrc.qut.edu.au, b.pham@qut.edu.au

Abstract

The essential performance metrics of a robust watermark include robustness, imperceptibility, watermark capacity and security. In addition, computational cost is important for practicality. Wavelet-based image watermarking methods exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness. Although the Human Visual System (HVS) model offers imperceptibility in wavelet-based watermarking, it suffers high computational cost. In this paper, we examine embedding strength determined by a HVS model, a constant, and a simplified technique. The proposed simplified embedding technique significantly reduces embedding time while preserving the performance of imperceptibility and robustness. The fast embedding technique exploits implicit features of discrete wavelet transform (DWT) sub-bands, i.e. the luminosity information in the low pass band, and the edge information in the high pass bands. It achieves embedding speed comparable to a constant energy embedding process. Robustness is demonstrated with a few conventional attacks, e.g. JPEG compression, Gaussian noise insertion, image cropping, contrast adjustment, median filtering, and global geometrical distortion. Experimental visual quality is measured in Weighted-Peak Signal to Noise Ratio (W-PSNR) for high accuracy. Robustness and imperceptibility of HVS-based embedding could be trade-off with computational simplicity of a fast embedding technique.

Keywords: Robust image watermark, Human Visual System (HVS), Discrete Wavelet Transform (DWT), embedding technique.

1 Introduction

With the widely available tools and broad coverage of network connectivity, digital media such as images, need proper protection against electronic theft. The protection provided by cryptographic methods can be extended using digital watermarking technologies. Robust watermarks which resist different types of attacks are being developed and enhanced to offer copyright protection in digital images. In addition, robust watermarks can be applied in copy protection mechanism. Beside that, it can also assist in tampered image recovery using image registration techniques.

Wavelet-based watermarking methods exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness. Digital watermarks that use wavelet transforms have been experimented by some researchers recently (Fridrich 1998, Kundur and Hatzinakos 1998, Pereira et al. 2000, Fullea and Martinez 2001, Guzmán et al. 2004). However, there is still room for improvement. For example, HVS properties can be exploited to enhance watermark embedding strength. The advantages of wavelet transform compared to discrete cosine transform (DCT) and discrete Fourier transform (DFT) were mentioned in (Pereira et al. 2000). Among the many wavelet domains, discrete wavelet transform (DWT) is widely explored. However, comparative analysis on embedding strength and watermark coefficient values has not yet been addressed so far.

The performance of wavelet-based watermarking methods depends on the overall watermarking method as well as embedding and detection techniques. The essential factors of a good watermarking scheme are robustness, imperceptibility, watermark capacity and security (Cox et al. 1997). A well-balanced watermarking method that offers robustness, imperceptibility, and computational simplicity remains a big challenge (Eyadat 2004). One of the factors that steers the balance point is the embedding strength in an additive embedding technique. Hence, an analysis of DWT-based watermarking method focusing on its embedding strength and watermark coefficient values would provide useful insight in how to improve its performance. The performances measured include robustness, imperceptibility (i.e. fidelity), and computational cost. Embedding strength refers to the magnitude of watermark message inserted into the wavelet domain of a cover image. Watermark coefficient values are the actual values of watermark message, and it can take any real values. Particularly, we are interested in analysing the performance under HVS-based embedding and a simplified adjusted-strength embedding. HVS models enable adaptive strength embedding of a watermark to gain robustness while maintaining its fidelity. It considers sensitivity of the human eye to noise, luminosity and textures. For instance, higher embedding strength can be

applied to complex regions of an image. The proposed simplified method aims at achieving similar results with less computation. The method mimics a HVS model using the implicit features of DWT sub-bands.

We evaluated three of the essential elements of a robust watermarking method, i.e. robustness, imperceptibility, and computational cost under different embedding strengths. Robustness refers to the ability to survive intentional attacks as well as accidental modifications, for instance, lossy compression, noise insertion, region cropping, local and global geometrical transformations. Imperceptibility or fidelity means the perceptual similarity between the watermarked image and its cover image. High robustness often offsets the imperceptibility of a watermark. Furthermore, a computationally simple watermarking system usually cannot attain desirable robustness and imperceptibility. Ideally, a watermarking method should achieve a balance among these mutually exclusive requirements.

While the variance-based mask (Pereira et al. 2000, Kundur and Hatzinakos 1997) uses local sub-band variance to increase watermarking energy, its non-overlapping blocks with fixed block size made it "rigid". Furthermore, the non-blind watermark detection of the method made it less practical. Another wavelet-based watermarking method that exploits HVS is mentioned as image-adaptive wavelet (IA-W) method in (Wolfgang et al. 1999). The major drawback of the method is the requirement of an original test image in watermark detection, thus reduces its practicality in real life scenario.

In the analysis, a recent DWT-based image watermarking method (Barni et al. 2001) was chosen based on its overall performance. The method embeds a watermark in all the high pass bands of the DWT domain. This is due to the good embedding capacity and imperceptibility provided by high pass bands. In addition, a watermark is usually embedded in all the high pass bands to avoid derivation attacks. However, embedding in the low pass band is possible with careful selection of embedding technique because it could easily cause visual artefacts. The embedding technique exploits an adaptive weighting of the HVS model. Although the HVS model offers imperceptibility in wavelet-based watermarking, it suffers high computational cost. We investigated the performance factors of the watermarking method and analysed the results. The analysis and comparisons are presented in graphical and numerical forms. The performance is compared for three cases: embedding with a HVS model, a constant strength (Wolfgang et al. 1999), and adjustable-strength based on a simplified model.

The next section describes briefly the watermark embedding and detection techniques. Experimental results are analysed and presented in the third section followed by a discussion on the limitations of the methods and ways to improve them. Finally, future work is covered in the conclusion.

2 The Watermarking Method

A complete watermarking process consists of embedding and detection parts. This section describes the embedding step using three different techniques, and a blind detection step. The embedding techniques examined are: a HVS model, a constant energy, and a simplified technique.

2.1 Watermark Embedding

Common watermark embedding strategies are additive, multiplicative, and indexed. Additive embedding is simple and fast. It usually takes the form $I' = I + \alpha m$ where I' is the marked content, I is the original content, α is the embedding strength, and m is the watermark message.

The watermark embedding steps for the three techniques studied are similar. It begins with an image decomposition using DWT, followed by embedding strength computation using the respective techniques, and finishes with an inverse DWT (IDWT) that reconstructs the marked image. Figure 1 below depicts the processes involved.

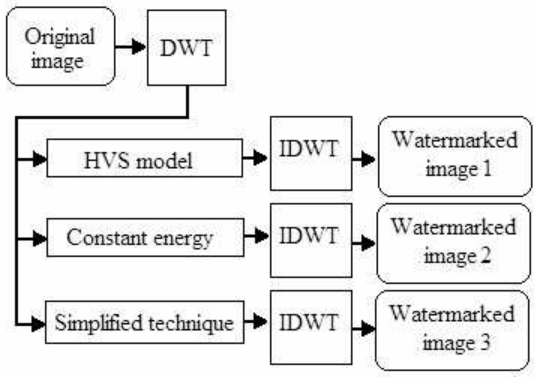

Figure 1 Watermark Embedding Using the Three Examined Techniques

The robust wavelet-based watermarking method (Barni et al. 2001) embeds watermark information in the DWT domain. It also incorporates an embedding weight factor that exploits the HVS characteristics. This adapts embedding strength according to the changes of image texture, edge distance, noise sensitivity and local luminosity. Therefore, the method gained robustness and imperceptibility simultaneously.

Firstly, an image is decomposed into its high pass and low pass bands using DWT with a Daubechies-6 filter. A 4-level decomposition with its sub-bands is sketched in Figure 2.

Each of the *l*-th level of the decomposition consists of three directional high pass bands I_l^0, I_l^1, I_l^2 and a low pass band I_l^3. To avoid analytical attacks, a watermark is usually embedded in all the high pass bands instead of some of the sub-bands.

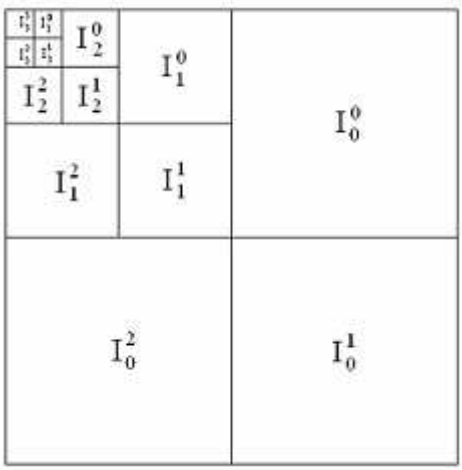

Figure 2 Four-level DWT Decomposition

2.1.1 HVS Embedding Technique

Details of the HVS-based watermarking method are presented in (Barni et al. 2001), and summarized here. The watermark is embedded in the three high pass bands at level 0 using the following equation.

$$I'^{\theta}_{0}(i,j) = I^{\theta}_{0}(i,j) + \alpha w^{\theta}(i,j)x^{\theta}(i,j) \quad (1)$$

where

$\theta \in \{0,1,2\}$ is the high pass sub-band selection.

$I^{\theta}_{0}(i,j)$ is the original sub-band coefficients.

$I'^{\theta}_{0}(i,j)$ is the watermarked sub-band of $I^{\theta}_{0}(i,j)$.

α is a global energy parameter that determines watermark embedding strength.

$w^{\theta}(i,j)$ is a weight function derived from local noise sensitivity which provides masking characteristics of the HVS.

$x^{\theta}(i,j)$ is a pseudorandom binary sequence, $m_h \in \{+1, -1\}$ coded in two-dimensional array using equation (2).

$$x^{\theta}(i,j) = m_{(\theta MN+iN+j)} \quad (2)$$

where

$\theta \in \{0,1,2\}$ is the high pass sub-band selection.

$2M \times 2N$ is the size of the cover image.

The weight function w is an adaptation of DWT coefficient quantization used in image compression (Lewis and Knowles 1992). Considering noise sensitivity of the human eye, (Barni et al. 2001) proposed the weight calculation below:

$$q^{\theta}_{l}(i,j) = \Theta(l,\theta)\Lambda(l,i,j)\Xi(l,i,j)^{0.2} \quad (3)$$

where

$\Theta(l,\theta)$ denotes noise sensitivity as shown in equation (4).

$\Lambda(l,i,j)$ denotes local luminosity for gray levels in I^{3}_{3} with reference to equations (5), (6) and (7).

$\Xi(l,i,j)$ considers edges distance and texture as indicated in the first and second terms of equation (8).

$$\Theta(l,\theta) = \begin{Bmatrix} \sqrt{2} & if \quad \theta = 1 \\ 1 & otherwise \end{Bmatrix} \cdot \begin{Bmatrix} 1.00 & if \quad l = 0 \\ 0.32 & if \quad l = 1 \\ 0.16 & if \quad l = 2 \\ 0.10 & if \quad l = 3 \end{Bmatrix} \quad (4)$$

$$\Lambda(l,i,j) = 1 + L(l,i,j) \quad (5)$$

$$K(l,i,j) = \frac{1}{256} I^{3}_{3}\left(1 + \left[\frac{i}{2^{3-l}}\right], 1 + \left[\frac{j}{2^{3-l}}\right]\right) \quad (6)$$

$$L(l,i,j) = \begin{Bmatrix} 1 - K(l,i,j) & if\ K(l,i,j) < 0.5 \\ K(l,i,j) & otherwise \end{Bmatrix} \quad (7)$$

$$\Xi(l,i,j) = \sum_{k=0}^{3-l} \frac{1}{16^{k}} \sum_{\theta=0}^{2} \sum_{x=0}^{1} \sum_{y=0}^{1} \left[I^{\theta}_{k+l}\left(y + \frac{i}{2^{k}}, x + \frac{j}{2^{k}} \right) \right]^{2} \cdot \mathrm{Var}\left\{ I^{3}_{3}\left(1 + y + \frac{i}{2^{3-l}}, 1 + x + \frac{j}{2^{3-l}} \right) \right\}_{\substack{x=0,1 \\ y=0,1}} \quad (8)$$

Assuming changes smaller than half of the calculated weights are imperceptible, the weight function w gives maximum embedding energy in the quantization of DWT coefficients using

$$w^{\theta}(i,j) = \frac{q^{\theta}_{0}(i,j)}{2} \quad (9)$$

From equation (1), it is apparent that the computed weight function w at each pixel enables HVS-based watermarking to obtain high level of imperceptibility and robustness. However, the computations in equations (3) to (9) consume a large amount of resources (e.g. CPU cycles and memory).

Finally, IDWT is performed after the watermark embedding to produce the marked image.

2.1.2 Constant Energy Embedding Technique

A constant energy embedding technique is realized using a similar method, with the weight function w omitted.

$$I'^{\theta}_{0}(i,j) = I^{\theta}_{0}(i,j) + \alpha x^{\theta}(i,j) \quad (10)$$

Note that the value of α in equation (10) has to be bigger than that of (1) to guarantee high embedding energy and warrant successful watermark detection. Obviously, this embedding technique requires the least computation compared to the HVS and Simplified techniques. The constant energy embedding technique is chosen as a baseline in this comparative study.

2.1.3 Simplified Embedding Technique

To achieve a balance between the two extremes of the HVS and constant energy techniques, we propose a simplified embedding technique. The proposed Simplified embedding technique significantly reduces embedding time while preserving the performance of imperceptibility and robustness. The fast embedding technique exploits implicit features of DWT sub-bands. The DWT coefficients in the low pass band provide a

good approximation of an image's luminosity information. Also, the DWT coefficients in the high pass bands give an estimation of edges information of an image.

Referring to equation (1), the Simplified embedding technique employs a different weight function *s*.

$$I'^{\theta}_{0}(i,j) = I^{\theta}_{0}(i,j) + \alpha s^{\theta}(i,j)x^{\theta}(i,j) \qquad (11)$$

where

$s^{\theta}(i,j)$ denotes the luminosity and edge information in an image; and other terms are the same as mentioned in equation (1).

The weight function *s* is calculated using equations (12) and (13) below.

$$s^{\theta}(i,j) = \frac{q''^{\theta}_{0}(i,j)}{2} \qquad (12)$$

$$q''^{\theta}_{l}(i,j) = \Theta(l,\theta)\Lambda''(i,j)\Xi''^{\theta}_{0}(i,j)^{2} \qquad (13)$$

where

$\Theta(l,\theta)$ considers noise sensitivity as shown in equation (4).

$\Lambda''(i,j)$ considers luminosity for gray levels in I^{3}_{3} with reference to equation (14). It makes sense to take a fraction of approximation values from the low pass band because the values indicate luminosity information. Our experimental outcome shows $\beta = 0.01$ gives good results.

$\Xi''^{\theta}_{0}(i,j)$ considers edges information using equation (15). As opposed to (3), this value is squared in (13) to provide a fast reduction of a value while considering edges information in each of the sub-bands. Our experiments show that $\delta = 0.005$ provides good results.

$$\Lambda''(i,j) = I^{3}_{3}(i,j) \times \beta \qquad (14)$$

$$\Xi''^{\theta}_{0}(i,j) = I^{\theta}_{0}(i,j) \times \delta \qquad (15)$$

We trade-off texture information in (15) for computation speed.

An enhanced version of the Simplified embedding technique omits the edge information totally by taking out $\Xi''^{\theta}_{0}(i,j)$ for faster computation. Our experiments show that the performance is similar to the original version because the small values of edges information in equation (13) have little effect on the weight function *s*.

Note that watermark capacity in all of the embedding techniques mentioned above is the same. This is due to the same size of watermark pattern *x* applied.

2.2 Watermark Detection

Regardless of the embedding technique used, a cross-correlation method is adopted in blind watermark detection. This provides a fair comparison among the three embedding techniques for robustness under various attacks.

To detect the presence of a watermark pattern (watermark message) *x*, we begin with a DWT operation on the marked image similar to the embedding process. Then, a cross-correlation value between the marked sub-band coefficients *I'* and the watermark pattern *x* is calculated using equation (16).

$$\rho = \frac{1}{3MN}\sum_{\theta=0}^{2}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} I'^{\theta}_{0}(i,j)x^{\theta}(i,j) \qquad (16)$$

It is worth mentioning that an adaptive threshold value T_p is computed dynamically, avoiding the requirement of embedding strength factor α. If $\rho > T_p$, then the watermark *x* is present; otherwise it is absent. To ensure that the false detection probability does not exceed 10^{-8}, the threshold T_p is chosen as follows:

$$T_p = 3.97\sqrt{2\sigma^{2}_{\rho B}} \qquad (17)$$

$$\sigma^{2}_{\rho B} \approx \frac{1}{(3MN)^{2}}\sum_{\theta=0}^{2}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(I^{\theta}_{0}(i,j)\right)^{2} \qquad (18)$$

The calculation of this threshold value is adapted from Neyman-Pearson criterion.

3 Analysis of Experiment Results

3.1 Experiment Settings

Using the watermark embedding and detection procedures explained in Section 2, a set of five common images were tested. The images are illustrated in Figure 3. They are all gray scale images with standard dimension 256×256 pixels. The images are identified by name: *Baboon*, *Cameraman*, *Lena*, *Pepper*, and *Fishing boat*. *Baboon* represents images with large areas of complex texture (i.e. the fur) and homogeneous areas (i.e. the face); *Cameraman* is chosen for its flat regions (i.e. the sky) and high contrast regions (i.e. the shirt and its background); *Lena* has a mixture of characteristics (e.g. smooth background, while the hat has complex textures and big curves); *Pepper* provides luminosity changes (i.e. light reflection surfaces); *Fishing boat* contains smooth parts (i.e. the clouds) as well as other feature combinations.

Figure 3 Test Images Used in Experiments (from left to right: *Baboon, Cameraman, Lena, Pepper, Fishing boat*)

The factors evaluated are watermark embedding duration, imperceptibility, and robustness.

Computational costs are compared by measuring the embedding time taken by each of the embedding techniques. Intuitively, the HVS model has the highest amount of computation because the weight function calculation involves many summation/convolution operations. On the contrary, the constant energy

embedding technique should be the fastest because there is no computation of weight function.

To evaluate the imperceptibility quality of watermarked images, W-PSNR of each watermarked image is measured. The collected data are interpreted in graphical form in the next section. W-PSNR is chosen due to its higher accuracy over PSNR metric (Voloshynovskiy et al. 2001, Watson et al. 1997). W-PSNR is calculated using equation (19).

$$\mathrm{WPSNR} = 10\log_{10}\frac{\max(x)^2}{\left\|\mathrm{NVF}(x'-x)\right\|^2} \qquad (19)$$

where *x'* is the watermarked image, and *x* is the original image.

Robustness tests were carried out with six types of conventional attack listed in Table 1.

No	Attack type	Description
1	JPEG compression	Quality factor 85%, 70%, 55%, 40%, and 25%
2	Gaussian noise insertion	Zero mean, variance are 0.0002, 0.0004, 0.0006, 0.0008, and 0.0010
3	Cropping	8×8, 16×16, 32×32, 64×64, and 128×128 squares at image centre cropped out
4	Contrast adjustment	Gamma 0.8
5	Median filtering	2D median filtering using 3×3 neighbourhood
6	Global geometrical distortion	3 degree rotation at image centre, random bending.

Table 1: Attacks Used in Robustness Tests

JPEG compression is one of the common compression attacks on digital images. With JPEG compression, one makes a trade-off between image quality and file size by specifying its compression qualities. Gaussian noise insertion is a type of signal processing operation. The amount of noise is controlled by its mean and variance. Cropping represents data reduction attack. Contrast adjustment is part of signal enhancement manipulation. It can be used to change the appearance of an image to be "brighter" or "darker". Median filtering is a type of non-linear filtering that produces a "smoother" image. Global geometrical distortion such as rotation is a big challenge. A small degree of rotation usually retains visual appearance while damaging watermark information. Normally, correlation-based watermark detection is vulnerable to such attack.

3.2 Experimental Results Analysis

By applying the embedding steps illustrated in Figure 1, a binary watermark pattern shown in Figure 4 below is embedded into the three high pass bands (i.e. the dark quadrants) of *Lena*.

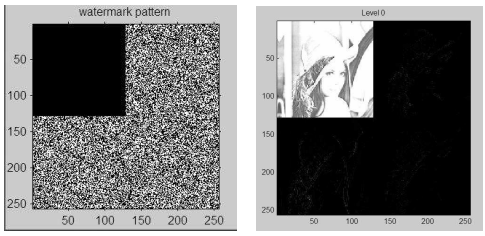

Figure 4 Left: Watermark Pattern *x*; Right: Level 0 sub-bands of DWT for *Lena*

3.2.1 Embedding Time Evaluations

Experiments showed that the Simplified embedding technique takes as little time as the constant energy embedding. On the other hand, the HVS embedding technique requires more than 55 factors of time. Table 2 shows the embedding time for the images processed.

Image	Embedding time (seconds)		
	HVS	Simplified	Constant
Baboon	62.370	1.222	1.111
Cameraman	61.398	1.172	1.071
Lena	61.209	1.182	1.072
Pepper	61.089	1.182	1.072
Fishing boat	61.209	1.182	1.072

Table 2: Embedding Time of the Three Embedding Techniques

The detection of watermark prior to attacks was done on each of the embedded images. In all cases, the watermarks were detected successfully.

3.2.2 Imperceptibility Evaluations

The watermarked images produced by each of the embedding techniques are measured its W-PSNR value. Figures 5 to 9 depict the marked images and its W-PSNR values. For these tests, we used the enhanced version of the Simplified embedding technique because the influence of edge information is very small on the total embedding strength $\alpha s^{\theta}(i,j)$. Note that α values selected for the HVS, constant energy, and Simplified embedding techniques are 4.5, 1.5 and 2.2 respectively. In addition, the Simplified embedding technique uses $\beta = 0.01$. Such arrangements are necessary since the major interest is in performance factors comparison. Although the α values of the embedding techniques are different, the effective embedding strengths after multiplication with its respective weight functions do not differ much.

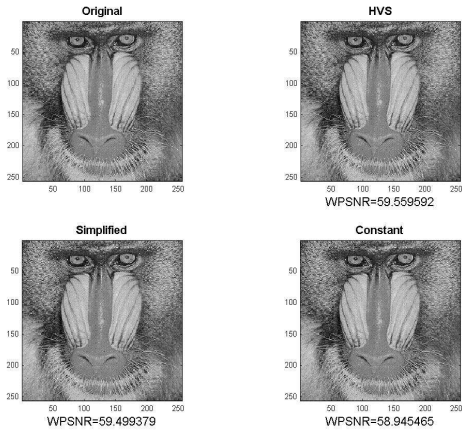

Figure 5 Set of *Baboon* Embedding Results with Their Respective W-PSNR

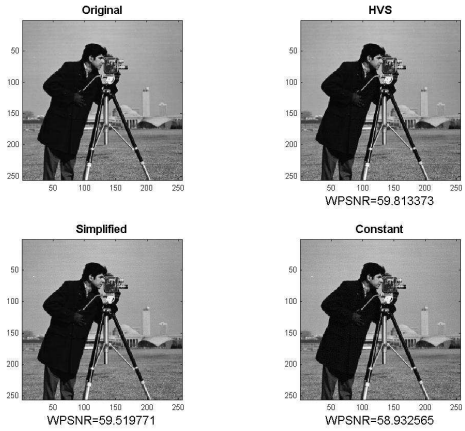

Figure 6 Set of *Cameraman* Embedding Results with Their Respective W-PSNR

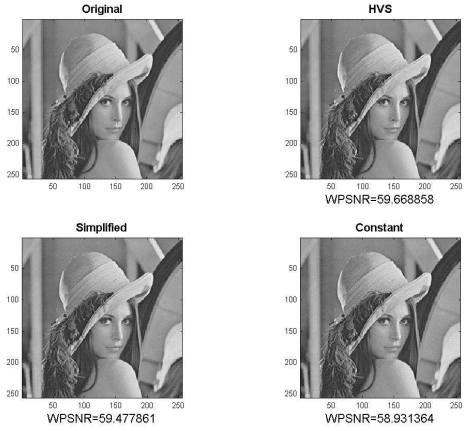

Figure 7 Set of *Lena* Embedding Results with Their Respective W-PSNR

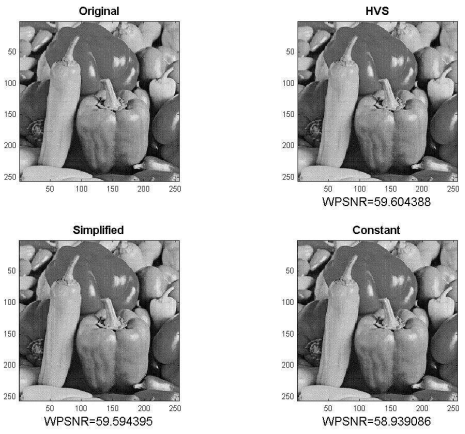

Figure 8 Set of *Pepper* Embedding Results with Their Respective W-PSNR

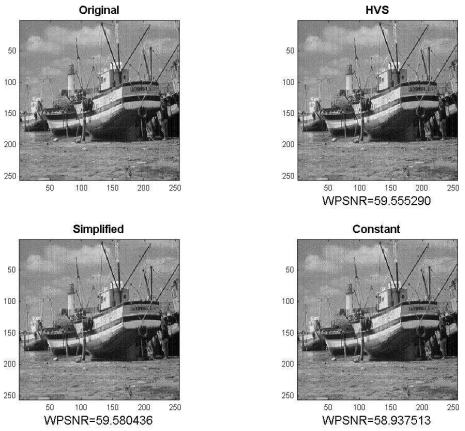

Figure 9 Set of *Fishing boat* Embedding Results with Their Respective W-PSNR

A visual comparison of imperceptibility in graphical form is presented in Figure 10. Constant energy embedding technique has the lowest visual quality overall, and the HVS embedding technique achieves the highest visual quality in general. It is also noticed that the Simplified embedding technique obtained visual qualities slightly lower than the HVS embedding technique.

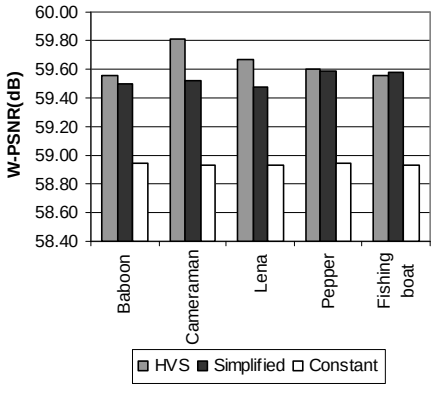

Figure 10 W-PSNR of Watermarked Images Under Different Embedding Techniques

3.2.3 Robustness Evaluations

Subsequently, all the embedded images were attacked with the six operations listed in Table 1. For the first 3 types of attacks, five levels of attack described in the table were performed. Samples of various attacked images are presented in Figure 11. The original *Lena* image is shown in 11(a). A JPEG compression with quality factor 25% on HVS embedded image is depicted in 11(b). Gaussian noise with variance 0.001 is inserted into the Simplified embedded image and illustrated in 11(c), and 11(d) represents a 32×32 pixels region cropping on constant energy embedded image. Contrast adjustment with Gamma set to 0.8 on the HVS embedded image is printed in 11(e). Figure 11(f) is a two-dimensional median filtered image on the constant energy embedded *Lena*, and it uses a 3×3 neighbourhood kernel. Lastly, a global rotation at 3 degree around the image centre in the anti-clockwise direction on the Simplified embedded image is given in 11(g).

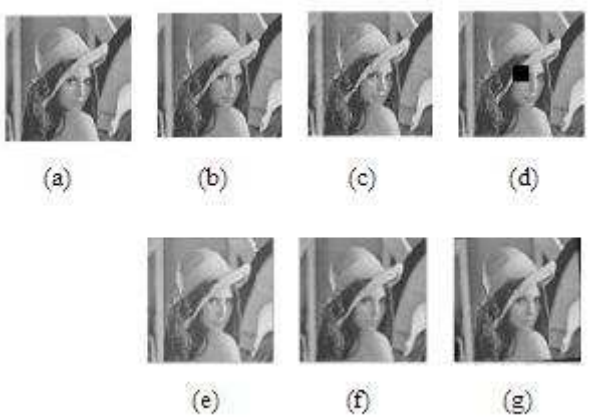

Figure 11 Samples of Various Attacked Images

Experimental results for all of the five images under all attack conditions listed in Table 1 are compiled. The robustness tests results are summarized in Table 3. For each of the JPEG compression, Gaussian noise insertion, and cropping attacks, every detection method is tested with 25 watermarked images. For each of the three remaining attacks listed in the table, every detection method is tested with five watermarked images.

For JPEG compression attacks, constant energy embedding performed excellently since the energy chosen is strong enough in a trade-off for visual quality. However, HVS and Simplified embedding techniques cannot resist high level of lossy compression.

We use the value $C = (\rho - T_p)$ to measure the "Competency" of watermark detection. Following the definition in Section 2.2, a positive C value indicates a watermark is detected and a negative C value otherwise. A higher C value means a higher "strength" of successful watermark detection.

No	Attack type	Number of watermarks detected		
		HVS	Constant	Simplified
1	JPEG compression	21	25	21
2	Gaussian noise insertion	25	25	25
3	Cropping	25	25	25
4	Contrast adjustment	5	5	5
5	Median filtering	1	1	1
6	Global geometrical distortion	0	0	0

Table 3: Summary of Watermark Detection Result for All Levels of Attacks

From Table 4, it is noted that HVS embedding technique does not produce detectable watermark in *Cameraman* under JPEG compression attack with quality factor 55% (also for lower quality factors 40% and 25%). In the experiments, watermarks were not detected for *Cameraman* images produced by Simplified embedding technique when JPEG compression attack quality factor is set to 40% or 25%.

Image	Competency value		
	HVS	**Simplified**	**Constant**
Baboon	1.1961	1.3458	2.2954
Cameraman	– 0.0016	0.1142	0.4805
Lena	0.1740	0.1830	0.4464
Pepper	0.6264	0.6225	1.1627
Fishing boat	0.4942	0.5867	1.2233

Table 4: Competency Comparisons of the Three Embedding Techniques under JPEG Compression Attack with Quality Factor 55%

All of the embedding techniques were able to give positive results under three subsequent attack types: Gaussian noise insertion, regional cropping, and contrast adjustment.

Some positive Competency values, C were obtained under median filtering for all the embedding techniques. In fact, all detections in *Lena* were successful under the attacks for HVS, constant energy, and Simplified embedding techniques. However, none of the embedding techniques supplied detectable watermarked images under median filtering for *Baboon*, *Cameraman*, *Pepper*, and *Fishing boat*.

It is evident that global geometrical distortion remains a big challenge because none of the embedding techniques is able to warrant a successful detection for all the test images.

4 Discussion

The Simplified embedding technique offers efficient computation with similar performance as the HVS embedding technique. It offers a moderate option between two extremes of HVS and constant energy embedding techniques.

4.1 Embedding Time

Obviously, the HVS embedding technique is very slow compared to constant energy embedding and the Simplified embedding technique. This can be referred to the fact that weight function computation in the HVS embedding technique involves many complex convolution operations. Such calculation definitely increases with an increase in image size. The constant energy embedding technique requires the least amount of computation compared to the HVS and Simplified techniques. The proposed Simplified embedding technique significantly reduces embedding time while preserving the performance of imperceptibility and robustness. Its embedding speed is comparable to those of the constant energy embedding technique.

4.2 Imperceptibility

Comparing the W-PSNR values in the watermarked images of each embedding techniques, it is clear that constant energy embedding gives lowest visual quality. This is due to the rigid energy level used. HVS embedding has highest visual quality since it has adaptive advantage in visual masking with its weight function calculations. The Simplified embedding technique achieves HVS-comparable levels of imperceptibility, especially for *Pepper* and *Fishing boat* images.

4.3 Robustness

Table 3 shows the constant energy embedding technique is the most robust technique. Thanks to the high level of embedding energy, it survives all levels of JPEG compression attacks. Remember that it traded-off imperceptibility for robustness.

Gaussian noise insertion, cropping, and contrast adjustment do not pose a treat to all embedding techniques. Therefore, partial information retained in the attacked images helped with successful watermark detection.

Severe level of median filtering caused the embedding techniques to fail in watermark detection for most images. The major changes in filtered images caused its threshold values T_p goes lower than its correlation value ρ.

Although the HVS embedding technique can resist partial geometrical manipulations such as *implode* and *pinch* operations (Barni et al. 2001), it cannot survive global geometrical distortions. The reason behind this is that the watermark detection step only requires a small piece of unchanged image area in order to succeed. However, such requirement is not met in a global geometrical distortion.

Despite the simplicity in correlation-based watermark detection, its major drawback is its weakness under global geometrical transformations. Beside this, Random Bending Attack (RBA) and JPEG compression remain a big challenge for robust watermarking.

One way to overcome the weakness in robustness is to insert a watermark recovery step before the watermark detection. For this, re-synchronization can be done using many techniques published in the literature.

5 Conclusions

An efficient embedding technique for wavelet-based watermarking is demonstrated. The Simplified embedding technique promises fast embedding speed with its computational simplicity. It attained competitive performance in terms of imperceptibility and robustness in par with the HVS-based model. In addition, the practical advantages also lie in its fast embedding speed and blind watermark detection.

The wavelet-based watermarking scheme is vulnerable to severe levels of JPEG compression and median filtering attacks. Furthermore, it is particularly weak under global geometrical attacks. This is due to the correlation nature of the detection method. To overcome the weakness, an additional step of re-synchronization is required prior to watermark detection. The re-synchronization can be accomplished in many ways. A simple yet effective method is to break up the image into small blocks and recover the original image properties using existing techniques in the literature (Hartung et al. 1999). Extended work in this direction is underway.

In summary, the Simplified technique significantly reduces embedding time compared to the HVS technique. It also maintains visual quality of the HVS technique while achieving comparable robustness. Hence, robustness and imperceptibility of a HVS-based embedding could be trade-off with computational simplicity of the fast embedding technique.

6 Acknowledgement

This work is supported by the Strategic Collaborative Grant on Digital Rights Management (DRM) awarded by Queensland University of Technology (QUT), Australia.

7 References

Barni, M., Bartolini, F. and Piva, A. (2001):Improved Wavelet-Based Watermarking Through Pixel-Wise Masking. *IEEE Transactions on Image Processing*, **10**(5): 783-791.

Cox, I. J., Kiliany, J., Leightonz, T. and Shamoony, T. (1997):Secure Spread Spectrum Watermarking for Multimedia. *IEEE Trans. on Image Processing*, **6**(12): 1673-1687.

Eyadat, M. (2004): Factors that Affect the Perfomance of the DCT-Block Based Image Watermarking Algorithms. *International Conference on Information Technology: Coding and Computing*IEEE.

Fridrich, J.,*Secure Encryption and Hiding of Intelligence Data, Final Technical Report*, Air Force Research Laboratory, Mission Research Corporation, (September 1998) New York

Fullea, E. and Martinez, J. M. (2001): Robust digital image watermarking using DWT, DFT and quality based average. *The 9th ACM international conference on Multimedia*, Ottawa, Canada, 489-491 ACM.

Guzmán, V. V. H., Miyatake, M. N. and Meana, H. M. P. (2004): Analysis of a Wavelet-based Watermarking Algorithm. *14th International Conference on Electronics, Communications and Computers*IEEE.

Hartung, F., Su, J. K. and Girod, B. (1999): Spread Spectrum Watermarking: malicious attacks and counter-attacks. *Security and Watermarking of Multimedia Contents*, San Jose, California, USA., **3657:** 147-158 SPIE.

Kundur, D. and Hatzinakos, D. (1997): A robust digital image watermarking method using wavelet-based fusion. *4th IEEE Int. Conf. Image Processing '97*, Santa Barbara, California, USA, 544-547 IEEE.

Kundur, D. and Hatzinakos, D. (1998): Digital watermarking using multiresolution wavelet decomposition. *International Conference on Acoustic, Speech and Signal Processing (ICASP)*, Seattle, Washington, USA., **5:** 2969-2972 IEEE.

Lewis, A. S. and Knowles, G. (1992):Image compression using the 2-D wavelet transform. *IEEE Trans. Image Processing*, **1**244–250.

Pereira, S., Voloshynovskiy, S. and Pun, T. (2000): Optimized wavelet domain watermark embedding strategy using linear programming. *SPIE AeroSense 2000*, Orlando, Florida USA, (Ed, Vetterli, H. H. S. a. M.), SPIE.

Voloshynovskiy, S., Pereira, S., Iquise, V. and Pun, T. (2001):Attack modelling: Towards a second generation watermarking benchmark. *Signal Processing - Special Issue on Information Theoretic Issues in Digital Watermarking*, 1177-1214.

Watson, A., Yang, G., Solomon, J. and Villasenor, J. (1997):Visibility of wavelet quantization noise. *IEEE Trans. on Image Processing*, **6**(8): 1164-1175.

Wolfgang, R. B., Podilchuk, C. I. and Delp, E. J. (1999): Perceptual watermarks for digital images and video. **87:** 1108-1126 IEEE.