Proceedings of the 6th WSEAS International Conference on Multimedia Systems & Signal Processing, Hangzhou, China, April 16-18, 2006 (pp88-96)

Multiple Image Watermarking using the SILE Approach

VIDYASAGAR POTDAR, CHRISTOPHER JONES, ELIZABETH CHANG
School of Information Systems, Curtin Business School
Curtin University of Technology
Hayman Road, Bentley, Perth, Western Australia
AUSTRALIA
Vidyasagar.Potdar@cbs.curtin.edu.au http://www.fit.cbs.curtin.edu.au/~potdarv

Abstract: - Digital copyright protection has attracted a great spectrum of studies. One of the optimistic techniques is digital watermarking. Many digital watermarking algorithms were proposed in recent literature. One of the highly addressed issues within the watermarking literature is robustness against attacks. Considering this major issue, we propose a new robust image watermarking scheme. The proposed watermarking scheme achieves robustness by watermarking several images simultaneously. It firstly splits the watermark (which is a binary logo) into multiple pieces and then embeds each piece in a separate image, hence, this technique is termed '*Multiple Images Watermarking*'. The binary logo is generated by extracting unique features from all the images which have to be watermarked. This watermark is first permuted and then embedded using SILE algorithm [7]. Permutation is important step to uniformly distribute the unique characteristics acquired from multiple logos. The proposed watermarking scheme is robust against a variety of attacks including Gamma Correction, JPEG, JPEG2000, Blur, Median, Histogram Equalization, Contrast, Salt and Pepper, Resize, Crop, Rotation 90, Rotation 180, Projective, Row Column Blanking and Row Column Copying and Counterfeit attack.

Key-Words: - Watermarking, DWT, Robustness, HVS, Haar Wavelet Transform, Perceptual Transparency.

1 Introduction

With the adoption of Internet in day to day life new threats to information security are coming into the lime-light. For example, exchange or illegal distribution of copyrighted material over peer-to-peer (P2P) networks results in copyright infringement and ownership verification issues. Although some threats can be protected against or prevented by employing cryptographic measures; copyright protection is difficult because cryptographic tools can only protect digital assets during transmission but once the encrypted content is decrypted it does not stop its illegal distribution. Thus, the person who infringes the copyright cannot be prosecuted because there is no evidence to prove who distributed the digital content illegally. This has caused major concerns for content providers who produce digital content.

In an attempt to address copyright protection, digital watermarking techniques have received considerable attention recently. Digital watermarking is a technique of hiding proprietary information in digital content like photographs, digital music, digital video or any digital media. Some digital watermarking algorithms were proposed in recent literature [1-14]. However, most of these watermarking schemes cannot simultaneously address issues like offering robustness against an optimistic number of attacks, watermarking multiple images simultaneously, maintaining perceptual transparency of the watermarked image and offering security against protocol attack

In this paper, we will propose a new robust watermarking scheme which can simultaneously address all the issues listed above. The paper is organized in the following manner:

In § 2, we discuss some preliminary concepts like the Human Visual System (HVS) model and Haar Wavelet Transform.

In § 3, we discuss existing wavelet based watermarking schemes which embed binary logo watermarks.

In § 4, we describe the proposed watermarking scheme;

In § 5, we discuss the experimental setting where we specify the attacks and their intensity which would be used to test the robustness of the proposed watermarking scheme.

In § 6, we describe the results obtained after each attack and a conclusion is drawn as to how our algorithm resists these attacks.

Finally, in §7, we conclude the paper with some future directions.

2 Preliminary Concepts

Following, we discuss some preliminary concepts that would be useful in understanding the proposed watermarking algorithm.

2.1 Haar Wavelet Transform

There are a number of wavelet algorithms like Daubechies wavelets, Mexican Hat wavelets and Morlet wavelets. These wavelet algorithms provide better resolution for smoothly changing time series. However, the main drawback of these algorithms is that they are computationally more expensive than the Haar wavelets. The Haar wavelet transform has a number of advantages namely; it is conceptually simple and fast. It is memory efficient because it does not require a temporary array to store intermediate results and it is exactly reversible without the edge effect which is an issue with other wavelet transforms. We use Haar Wavelet Transform in our algorithm

2.2 Human Visual System

In order to design a robust and transparent watermark, HVS characteristics can be explored to analyze the DWT coefficients so that during the process of embedding the modifications introduced to the DWT coefficients are within the limits of perceptual transparency. In Lewis and Knowles [1], the authors describe three psychophysics functions to analyse DWT coefficients where they analyze frequency, luminance and texture to decide the quantization factor Q_l^θ that would be used to modify the DWT coefficients. The formula for HVS calculation is given as:

$$Q_l^\theta(x,y) = frequency(l,\theta) * lumiance(l,x,y) * texture(l,x,y)^{0.2} \quad (1)$$

3 Existing Research

One of the earliest and most cited works in watermarking is the one presented by Cox, Killian, Leighton and Shamoon [2]. In their approach the watermark was PRGS. The algorithm selected the first highest magnitude DCT coefficients to embed the watermark. It follows linear additive embedding as shown in Eq. 2 where is the scaling factor which is used to control the strength of the embedded watermark, is the host coefficient and is the watermarked coefficients. This formula is presented by Cox et al. [2].

$$I_{ij}^w = I_{ij}^o + \alpha W_i^o \quad (2)$$

$$W_i^e = I_{ij}^e - I_{ij}^o / \alpha \quad (3)$$

$$SF(W^o, W^e) = W^o.W^e / \sqrt{W^o.W^o} \quad (4)$$

The watermark is extracted using Eq. 3. The extracted watermark is then compared with the original watermark to detect the similarity using Eq. 4. Since the watermark is embedded in the highest magnitude DCT coefficients it is robust against common image processing attacks and some geometric distortions. All other PRGS based watermarking schemes are based and evolved from this concept.

Hsu and Wu [3] present a wavelet based watermarking scheme which embeds a binary logo as a watermark. The watermark is embedded in the mid frequency components of the wavelet sub-bands. This scheme is resistant to common image processing attacks only. Its robustness against geometric distortions is not discussed. The main drawback of this algorithm is its non-blind nature i.e. the original image is required for detecting the presence of watermark.

Raval and Rege [9] present a non-blind watermarking scheme where two binary watermarks are embedded in LL_2 and HH_2 subband. All the coefficients in the LL_2 and HH_2 subband are used. After performing a two level decomposition of the host image (I), the binary watermark is embedded in the LL_2 and HH_2 subband by additive embedding. It has been shown that watermarks embedded in LL_2 subbands are robust to one set of attacks (filtering, lossy compression, geometric distortions) while those embedded in HH_2 sub-band are robust to another set of attacks (histogram equalization, gamma correction, contrast and brightness adjustment and cropping). However the use of uniform scaling parameter results in some visible artefacts. It should have been a good idea to consider variable scaling factors for different subbands.

Ganic and Eskicioglu [10] inspired by [9] propose another watermarking scheme based on DWT and Singular Value Decomposition (SVD). They argue that the watermark embedded by using [9] scheme is visible in some parts of the image especially in the low frequency areas, which reduces the commercial value of the image. Hence they generalize their technique by using all the four sub-bands and embedding the watermark in SVD domain. However even this algorithm is non-blind which is its main drawback.

All the algorithms discussed so far require the original image for detecting the presence of

watermark which is a major drawback and is not feasible in all scenarios. Hence we now discuss some blind water-marking algorithms which embed an image logo as a watermark.

In Tsai, Yu and Chen [5] improve the scheme proposed in [3] by presenting a scalar quantization based blind watermarking scheme which embeds a binary logo as a watermark and the offer blind detection. They embed the watermark in all sub-bands except LL subband. All the selected coefficients are quantized by a constant factor which is a main issue with this algorithm. This algorithm shows robustness against JPEG compression only. It's robustness against geometric attacks and other image processing attacks is not discussed.

Barni Bartolini and Piva [6] present wavelet based watermarking scheme which incorporates HVS to modulate the strength of the watermark according to the local characteristics. The watermark is not a binary logo but it is a binary PRGS. The watermark is embedded in HH_l, HL_l and LH_l subbands. This scheme is robust against JPEG compression, cropping and morphing.

Chen, Horng and Wang [8] present another quantization based watermarking scheme which improves on the algorithm proposed in Tsai et al. by incorporating variable quantization based on HVS similar to Barni et al. [6]. They embed the watermark in the approximate subband of the fourth level wavelet decomposition i.e. the LL_4. This scheme is robust against blurring, noising, sharpening, scaling, cropping and compression. The scheme is also robust against counterfeit attacks because it employs the concept of digital signature and time stamps. However robustness against other image processing attacks like gamma correction, rotation, salt and pepper, resizing, median filtering, histogram equalization, contrast enhancement is not shown.

All the algorithms discussed so far embed the watermark in single image. No one so far has discussed an approach to watermark multiple images simultaneously using a single watermark. In this paper we present one such scheme which watermarks multiple images simultaneously using a single watermark. The proposed scheme is robustness against attacks as well as results in perceptually acceptable watermarked image.

4 Multiple Image Watermarking using SILE Approach

In this paper we propose a new robust image watermarking algorithm based on SILE initially proposed by Potdar et al. (2005). The proposed algorithm watermarks multiple images simultaneously using portions of a single permuted binary watermark. This watermark is generated by extracting some unique features from multiple host images. Most of the previously proposed schemes [6, 8] do not use a binary logo watermark which is related or derived from the host image. In contrast to the schemes proposed earlier [6, 8], our scheme generates the watermark (from the host) by extracting unique features from the host images. The unique features from each host image are combined together to generate a binary watermark logo. This watermark is then permuted to uniformly distribute all these features (from multiple images) across the entire watermark logo. After permuting; the watermark it is sub-divided into multiple pieces (equal to the number of hosts), and these pieces are then embedded in the individual host image. The process of permuting the watermark results in uniform distribution of features from multiple images and these mixed features are then embedded in individual host image.

The novelty of this approach lies in the fact that when the watermark is to be detected multiple images are used simultaneously to extract the watermark. This has three fold advantages *firstly* we can detect watermark in multiple images simultaneously, *secondly* this approach can act as a reliable proof when watermark from one of the image cannot be detected, however because the feature of the originally watermarked image can be partially extracted, it can be concluded that the attacked image was originally watermarked and *finally* the probability of watermark detection is much higher because watermark is extracted and detected from multiple images. The possibility that all the images would be severely attacked is much lower compared to an individual image being attacked.

Since the features from multiple images are filtered in the watermark and the watermarks are then permuted, the features from all the images are embedded in each host image and this helps in detection. Our water-marking scheme is divided into three steps, firstly watermark generation step followed by watermark embedding step and finally extraction step.

4.1 Watermark Generation

Inputs: Original Host Image I_i $0<i<n+1$ where n is the number total number of images to be watermarked.

Output: Permuted Binary Logo Watermark W_i

Suppose the original host image to be watermarked is $I_i \mid 0<i<n+1$ (Fig. 1a), and the image dimension are $S \times S$. We generate binary watermark W from Ii. A copy of I_i is scaled down to $1/16^{th}$ of its size to generate the grey-scale watermark Wg (as shown in Fig. 1b) hence the dimensions of the watermarks would be $S/16 \times S/16$. This grey scale watermarks W_g are then converted to binary watermark (as shown in Fig. 1c) either by accessing the most significant bit plane from W_g or using any photo editing tool to convert W_g to binary format. Thus the watermark logo is a scaled down binary version of I_i. The binary watermark logos from multiple images are combined together to form one big watermark logo. This watermark W_i is then permuted by using seed S and a pseudo random permutation (PRP) function $f(.)$. The seed is a shared secret.

Fig. 1a Scaled down version of Original Image

Fig. 1b Grey Scale Watermarks

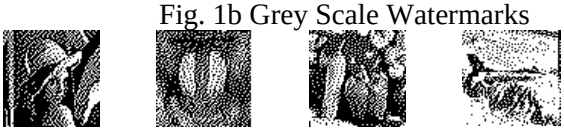


Fig. 1c Binary Watermarks

The combined grey scale watermarks and binary watermarks are shown in Fig. 2a and Fig. 2b respectively. This combined binary logo watermark is then permuted (Fig. 2c) and later split into four separate logos to watermark the four images separately as shown in Fig. 2d.

4.2 Watermark Embedding

The algorithm for embedding a binary logo watermark in images was presented by the authors earlier (Potdar, Han & Chang 2005). This embedding algorithm should be simultaneously used to watermark multiple images.

Inputs: Original Host Image I and Permuted Binary Logo Watermark W_i
Output: Watermarked Image I_w

Suppose the original image is an 8 bit grey scale image with dimensions $S \times S$ and watermark is a binary logo image of dimensions $S/16 \times S/16$. The process of watermark embedding is then completed in six steps. These steps are discussed next.

Fig. 2a Combined grey scale logo watermarks

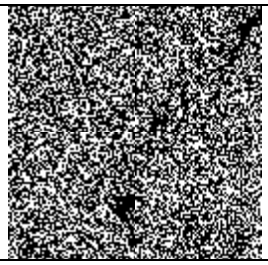


Fig. 2c Combined permuted logo watermark

Fig. 2b Combined binary watermark logo

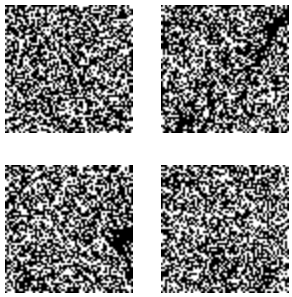


Fig. 2d Separate permuted watermark logo

4.2.1 Wavelet Transform

The original image I is decomposed by one level wavelet transform to obtain LL_1, LH_l, HL_l and HH_l subbands. As discussed in section 2.3 an image can be transformed to wavelet domain by using any wavelet filter. In the proposed scheme we use Haar Wavelet Filter because of its simplicity and computational efficiency.

4.2.2 Block Mean Intensity Calculation

For each sub-band except the LL_1 sub-band, starting at the top left corner divide the wavelet coefficients into non-overlapping blocks of $8x8$ $B_{I,J} \mid 0<I,J<S/16$ and calculate their mean intensity values. Mean intensity $M_{B_{I,J}}$ is the average of the magnitude of 64 wavelet coefficient. This is given as:

$$M_{B_{I,J}} = \frac{1}{64} \sum_{i=1,j=1}^{8} C_{i,j}^{I,J}$$

Where $C_{i,j}^{I,J}$ represent the magnitude of the wavelet coefficients in the block $B_{I,J}$. From the set of n blocks find the blocks which have the highest

($M_{\max}$) and the lowest ($M_{\min}$) mean intensity values.

4.2.3 Construct Quantization Table

The construction of quantization table *T* is divided into two steps, firstly defining the quantization interval Q_I and secondly assigning binary values to the quantization intervals. To decide the quantization interval we first identity M_{min} and M_{max} because it will provide the range of mean values for a block within a selected sub-band. Since a watermarked image can undergo malicious attacks this might change the M_{min} and M_{max} so the quantization table should provide enough room to accommodate-date all possible mean values after attacks. Hence the range of *T* is decided as [M_{min} - *C*, M_{max} + *C*] such that $M_{min} - C \geq 0$. *C* is a positive constant. Once the range of *T* is fixed Q_I has to be identified. To decide the Q_I we select a positive constant *N* and divide the range into *N* equal sections which represents the quantization interval. *N* can be chosen by the user to control the trade-off between robustness and transparency. If *N* is very low then the watermarked image would be perceptually degraded as visible distortions would be evident. However if *N* is low the robustness of the water-mark extraction increases because the mean intensity of the block would not cross the set quantization interval. Q_I can be generated by the following formula.

$$Q_I = \left\lceil \frac{[(\mathrm{M}_{\max} + \mathrm{C}) - (\mathrm{M}_{\min} - \mathrm{C})]}{\mathrm{N}} \right\rceil$$

Once the quantization interval is fixed we can construct the quantization table as shown in Table 1.

Table 1 Quantization Table

x_1 to $x_1 + Q_I$	.....	x_n to $x_1 + N \cdot Q_I$
y_1	.....	y_N

Where $\{x_1, x_2, \mathrm{K}\ x_n\}$ (n is a positive integer and $x_{i+1} > x_i + i \cdot Q_I$) represent the range of magnitude of wavelet coefficient in one sub-band. In the quantization table *T* each quantization interval is termed as a 'bracket' and is represented as $Br_i = [x_i, x_1 + i \cdot Q_I] (1 \leq i \leq N)$. Then $y_i = i \bmod 2$ or $y_{i+1} = (i+1) \bmod 2$ where $(1 \leq i \leq N)$. Equivalently we set $y_i(Br_i) = i \bmod 2$ or . $y_{i+1}(Br_{i+1}) = (i+1) \bmod 2$

Where $y_i(Br_i)$ means we assign the value y_i to the i[th] bracket Br_i .

4.2.4 Quantifying a block of DWT Coefficients using HVS threshold

After obtaining the quantization table *T*, we can quantify all the DWT coefficients in one block by the following method. We use one block of *8x8* to embed one watermark bit. Hence we can embed *S/16 x S/16* bits in an image of size *S x S*. The embedding process begins by identifying the mean intensity of a selected block

Case 1: If the mean of the current block (M) represents the watermark bit that we want to embed then the final mean M' should be as follows, where '<' represents scaling-down and '>' represents scaling-up.

$$M' < M \quad if \quad M < \frac{1}{2}R$$

$$M' > M \quad if \quad M \geq \frac{1}{2}R$$

To identify the desired scaling parameter (< or >) we use the following formula $P_S = M'/M$ where $M' = \frac{1}{2}Br$. However before actually scaling the coefficients by P_S, calculate the maximum allowable scaling parameter (Q_l^θ) for each coefficient using the HVS model discussed in Section 2. After calculating Q_l^θ scale each coefficient using Eq. 5 where *Q* is the final scaling parameter.

$$\begin{aligned} Q &= Q_l^\theta \quad If \quad Q_l^\theta < P_S \\ Q &= P_S \quad If \quad Q_l^\theta > P_S \end{aligned} \qquad (5)$$

Case 2: If the current mean M does not represents the watermark bit (that we want to embed) then scale the mean of the current block B so that the final mean M' is in the adjacent quantization interval.

Case 2a: If the current mean is less than ½ Bi then scale-down the entire mean so that the final mean M' is in adjacent interval ½ Bi-1 i.e.

$$M' = \frac{1}{2}Br_{i-1} \quad \text{if} \quad M < \frac{1}{2}Br_i$$

(where Br_i = *current bracket*)

Case 2b: If the current mean is greater than ½ Bi then scale-up the entire mean so that the final mean M' is in adjacent interval ½ Bi+1 i.e.

$$M' = \frac{1}{2}Br_{i+1} \quad \text{if} \quad M > \frac{1}{2}Br_i$$

4.2.5 Inverse Quantization

We apply inverse wavelet transform to generate the watermarked image. The secret keys used in this algorithm are the seed *S* and the quantization table *T*. These are termed as verification keys.

4.2.6 Digital Signature and Time Stamping

The verification keys are digitally signed. Suppose $D_S = Sign_{Key}(S,Q)$ where $Sign_{Key}(S,Q)$ is the digital signature signed by the owner's private key. This digital signature is now time stamped by a trusted third party like a certifying authority (*CA*) e.g. Verisign. The *CA* then computes $TS = TS_{Key}(D_s)$ where TS_{Key} denotes the time stamp by the *CA's* private key. The time stamped digital signature is then stored together with the verification keys and is used for proving the ownership of the content.

4.3 Watermark Extraction

The extraction algorithm begins by verifying the digital signature and the time stamp. If the timestamp and the signature cannot be verified the algorithm does not proceed to the next step. If the verification is positive the extraction algorithm begins and uses the quantization table T and the secret seed S to recover the watermark. The original image in not required during extraction.

4.3.1 Wavelet Transform

The watermarked image I_w is decomposed by one level wavelet transform to obtain LL_1, LH_1, HL_1 and HH_1 subbands.

4.3.2 Watermark Recovery

For each sub-band except the LL_1 sub-band, starting at the top left corner we divide the sub-band into non-overlapping blocks of *8x8* and calculate the mean intensity values of the wavelet coefficients. These values are then compared with the quantization table *T* to generate the watermark bit. All the watermark bits are thus generated and the permuted watermark is recovered. Using the secret seed S and the inverse permutation function *f(.)* we can recover the watermark.

5 Experimental Setting

In the experiments that we conducted we used the original host images I_i as shown in Fig. 1a. The watermark logo W_b that is used in the experiments is shown in Fig. 2b, the permuted watermark W^*_b is shown in Fig. 2c. The size of the original images is 1024 x 1024 pixel grey scale image whereas the size of the watermark logo is 128 x 128 pixels. We used Haar Wavelet filter to decompose the image in the wavelet domain.

(a) H (b) V

Fig. 3 Extracted watermarks without applying any attacks

We first decomposed each image into four subbands by one level DWT transform and embedded individual permuted watermark in the HL_1 (or H) and LH_1 (or V) sub-bands. We then extracted the watermark without applying any attacks. The recovered watermarks without attacks are shown in Fig 3.

The proposed approach to watermarking is shown to be robust against sixteen major attacks i.e. Gamma Correction, JPEG, JPEG2000, Blur, Median, Histogram Equalization, Contrast, Salt and Pepper, Resize, Crop, Rotation 90, Rotation 180, Projective, Row Column Blanking and Row Column Copying and Counterfeit attack.

Although distortions exist the watermark is still visually recognizable (subjective detection) and statistically detected (PSNR values).

Apart from these individual attacks listed above we also applied combined attacks to identify the robustness of the proposed watermarking approach. The basic assumption is that multiple host images may experience different set of attacks. Hence an attack strategy is devised and used for the experiments; this is shown in Table 2.

Suppose the host images are numbered as follows Pepper - 1, Lena – 2, F16 – 3, Baboon – 4. These numbers are used to represent the combination attacks in Table 7.

Table 2 Combined attacks applied to multiple host images	
Experiment One	
A	Blank 1
B	Blank 1 + Blank 2
C	Blank 1 + Blank 2 + Blank 3
D	Blank 50% of 1 + 50% of 2 + 50% of 3 + 50% of 4
Experiment 2	
E	Blank 1 + Attack 2 with 16 attacks

6 Experimental Results and Observation

In this section we discuss the experiments that we conducted and the results that we observed by running our prototype. We conducted three different experiments as listed in Table 2. We now discuss the results and observations from these experiments.

6.1 Robustness against Cropping Attack

In this section we discuss the robustness of our algorithm against cropping attack. For the proposed approach cropping could be considered as a special case where one of the images is not available for watermark detection.

From a set on 4 images which were used for multiple images watermarking, firstly we tried to extract watermark with using only three images, and later we blanked additional images successively and tried to detect the watermark. The results are shown in the Table 3.

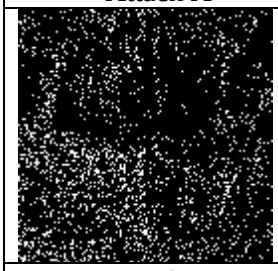
In the first attack (i.e. Attack A) we removed the Pepper image and recovered the watermark (25% loss). The extracted watermark is easily detected by visual inspection. The main features from the extracted watermarks include the Leena face, the pepper, the F-16 plane and the baboon face.

In the second attack (i.e. Attack B) we removed the Pepper and Leena from the combination and recovered the watermark (50% loss). The extracted watermark is still easily detected by visual inspection. Specifically the features like the vertical pepper, the Lena's hat, and the tail of F-16 are easily distinguishable.

Table 3 Watermarks after Attack A,B,C,D

Attack A

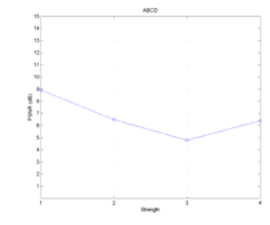
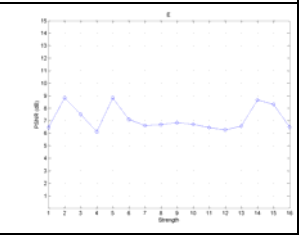
Attack B



Attack C

Attack D

In the third attack (i.e. Attack C) we removed the Pepper, Leena and F-16 from the combination and recovered the watermark (75% loss). This attack was the most severe attack because we lost 75% of the information; however some distinct features from the watermark are still visible like the outline of Lena's hat and the vertical pepper.

Table 4a PSNR of the extracted watermark after Attacks ABCD	Table 4a PSNR of the extracted watermark after Attacks E
	

In the fourth attack (i.e. Attack D) we cropped 50% of all the images and recovered the watermark. The results were similar to Attack B because the overall effect was like blanking two images.

For objective watermark detection we calculated the PSNR values using the embedded watermark and the extracted watermark.

The results are show in the graph in Table 4a. It is evident from the graph that the quality of the extracted watermark deteriorates as the attack strength increases which is theoretically supported because with increase the strength of attack a lot of embedded information is lost.

6.2 Robustness against blanking one image and attacking one image

In this section we discuss the robustness of our algorithm against cropping attack combined with the 16 attacks listed earlier. In this experiment we blanked one image completely (i.e. Pepper) and attacked one image (i.e. Lena) with the 16 attacks.

Table 5 Watermarks after Attack E

	
Attack E + Contrast	Attack E + Equalize
	
Attack E + Gamma	Attack E + JPEG
	
Attack E + Projective	Attack E + Resize
	
Attack E + Salt n Pepper	Attack E + Row Column Blanking

The results are shown in the Table 5 and the PSNR values are represented in the graph in Table 4b. The best results were achieved after contrast and gamma correction attacks (both PSNR 9dB); however the worst results were achieved for histogram equalization operation (PSNR 6dB). Row-Column Copy (PSNR 8.8dB) attack as well as Salt n pepper (PSNR 8.4dB) gave extremely good results as well. Attacks like blur, JPEG2000, median, projective, resize, rotate 90 and 180, row-column blank, and blur gave mediocre results, where the PSNR values ranged in between 6dB to 7dB. Even if the PSNR values are not considered all the extracted watermarks are still easily visually recognizable. All the prominent features like the pepper, Lena's hat and her facial features, and the tail of F-16 and baboons face can be easily distinguished. Due to space limitation we only show a few results for these set of attacks.

7 Discussion and Conclusion

In this paper we proposed a multiple image watermarking scheme. We embedded the watermark in the detailed sub-bands of the wavelet domain. The embedding process is based on scalar quantization. The wavelet coefficients are quantized under the constraint of HVS. The proposed scheme is shown to be robust against 16 different attacks. Some of the main features of our algorithm are as follows

1. We use a binary watermark which is a smaller version of the host image which is to be watermarked. The process to generate this watermark is very convenient.
2. We embed the watermark in the detailed sub-bands of the wavelet decomposition which offers implicit masking. At the same time we also incorporate HVS model during embedding to achieve higher perceptual transparency
3. As the magnitudes of the detailed sub-bands are low compared to the approximate (LL_1) sub-band we use a block of *8x8* wavelet coefficients to represent one bit of watermark. This technique increases the robustness of our scheme.
4. The quantization table can be easily generated if the values of C, N, M_{min}, M_{max} and the first bit of the binary string are available.
5. The watermark is permuted to achieve robustness against any attacks that result in loss of information e.g. cropping. A secret seed is used in the permutation function to improve the security of our scheme.
6. The secret verification keys used in the embedding algorithm are digitally signed by the owner's private key. This digital signature is then time stamped by a trusted third party to achieve robustness against counterfeit attacks.

From the experiments that we conducted we made the following observations

1. For 7 out of the 16 attacks, the V sub-band gave the best results. The seven attacks include

gamma correction, jpeg, jpeg2000, median filtering, contrast, salt and pepper, row-column copy.

2. For most of synchronization removal attacks (resizing, projective) and removal attacks (blur-ring, row-column blanking) the D sub-band gave the best results while the V sub-band gave the worst results (resizing, projective).
3. For the 7 attacks listed above, the H sub-band closely followed the results from the V sub-band. For example in gamma correction attack the PSNR of the extracted watermark from the V sub-band was in the range of 45 – 33dB while the H sub-band was 42 - 28dB. Similar results were observed for JPEG (30 – 7dB vs. 29 – 5dB) and JPEG 2000 (20 – 5 dB vs. 23 – 5dB). Similar trend was also observed after median filtering, salt-n-pepper, and contrast attacks. For synchronization removal attacks the PSNR for the watermarks extracted from both the V and H sub-band were low e.g. resize attack (5.5 – 5 dB), warping (4.7 – 4.6 dB), projective (5.5 – 4.3 dB).
4. The extracted watermarks after blurring and median filtering didn't give as good results as compared to all other attacks however the watermark could still be recognized using the hair and hat features of Lena image.
5. Histogram equalization gave the worse results of all if we look at the PSNR values. However the watermark is still visually perceivable.

In future we would like to test this algorithm for embedding grey scale watermark. We would consider grey-scale image as a set of multiple binary images. The most significant bits planes of the grey scale image could be embedded using this algorithm. We understand that a grey scale watermark has a greater probability of survival because it preserves the contextual relationship. In future we would gather some results after conducting such experiments.

References:

[1] A. S. Lewis and G. Knowles, 'Image Compression using 2-D Wavelet Transform,' in *IEEE Transactions on Image Processing*, vol. 1, pp. 244-250, 1992.

[2] I. J. Cox, J. Killian, F. T. Leighton, and T. Shamoon, 'Secure spread spectrum watermarking for multimedia,' *IEEE Transactions on Image Processing*, vol. 6, pp. 1673-1687, 1997.

[3] C. T. Hsu and J. L. Wu, 'Multiresolution Watermarking for Digital Images,' in *IEEE Transactions on Circuits and System—II Analog and Digital Signal Processing*, vol. 45, pp. 1097-1101, 1998.

[4] C. T. Hsu and J. L. Wu, 'Hidden Digital Watermarks in Images,' *IEEE Transactions on Image Processing*, vol. 8, pp. 58-68, 1999.

[5] M. J. Tsai, K. Y. Yu, and Y. Z. Chen, 'Joint Wavelet and spatial transformation for digital watermarking,' in *IEEE Transactions on Consumer Electronics*, vol. 46, pp. 241-245, 2000.

[6] M. Barni, F. Bartolini, and A. Piva, 'Improved Wavelet-based Watermarking Through Pixel-Wise Masking,' in *IEEE Transactions on Image Processing*, vol. 10, pp. 783-791, 2001.

[7] V. Potdar, & E. Chang, 2005, '*Scalar quantization based robust image watermarking algorithm in the wavelet domain*', in Proceedings of the ICT WA 2005 Conference, Perth, Western Australia, 18 November 2005. Accessed on Jan 24, 2006 Available online at http://www.ceebi.curtin.edu.au/~potdarv

[8] T. Z. Chen, G. Horng, and S. H. Wang, 'A Robust Wavelet Based Watermarking Scheme using Quantization and Human Visual System Model,' in *Pakistan Journal of Information and Technology*, vol. 2, pp. 212-230, 2003.

[9] M. S. Raval and P. P. Rege, '*Discrete wavelet transform based multiple watermarking scheme*,' in Convergent Technologies for the Asia-Pacific Region, Bangalore, India, 2003.

[10] E. Ganic and A. M. Eskicioglu, '*Robust digital watermarking: Robust DWT-SVD domain image watermarking: embedding data in all frequencies*,' presented at Proceedings of the 2004 Multimedia and Security Workshop on Multimedia and Security, 2004.

[11] V. Potdar, S. Han, E. Chang, '*Fingerprinted Secret Sharing Steganography for Robustness against Image Cropping Attacks*', in Proceedings of the 3rd International IEEE Conference on Industrial Informatics, Perth, Western Australia, 10-12 Aug 2005. Accessed on Jan 24, 2006 Available online at http://www.ceebi.curtin.edu.au/~potdarv

[12] V. Potdar, S. Han, E. Chang, '*A Survey of Digital Image Watermarking Techniques*', in Proceedings of the 3rd International IEEE Conference on Industrial Informatics, Perth, Western Australia, 10-12 Aug 2005. Accessed on Jan 24, 2006 Available online at http://www.ceebi.curtin.edu.au/~potdarv

[13] V. Potdar, E. Chang, '*Tamper Detection for Ubiquitous RFID-enabled Supply Chain*', in International Conference on Computational Intelligence and Security, Xi'an, China, 15-19 Dec 2005 Accessed on Jan 24, 2006 Available at http://www.ceebi.curtin.edu.au/~potdarv

[14] V. Potdar, M. Khan, E. Chang, P. Worthington and M. Ulieru, '*e-Forensics Steganography System for Terrorist Information Retrieval*', International Journal of Advanced Engineering Informatics, vol. 19, 235-241.