11

Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Domain

Clara Cruz Ramos, Rogelio Reyes Reyes, Mariko Nakano Miyatake and Héctor Manuel Pérez Meana
SEPI ESIME Culhuacan, National Polytechnic Institute of México, México City, México

1. Introduction

Nowadays, digital images and video are gradually replacing their conventional analog counterparts. This is quite understandable because digital format is easy to edit, modify, and exploit. Digital images and videos can be readily shared via computer networks and conveniently processed for queries in databases. Also, digital storage does not age or degrade with usage. On the other hand, thanks to powerful editing programs, it is very easy even for an amateur to maliciously modify digital media and create "perfect" forgeries. It is usually much more complicated to tamper with analog tapes and images. Tools as digital watermarks help us establish the authenticity and integrity of digital media and can prove vital whenever questions are raised about the origin of an image and its content.

A digital watermarking technique embeds an invisible signal with an imperceptible form for human audio/visual systems, which is statistically undetectable and resistant to lossy compression and common signal processing operations. So far there some content authentication of digital image methods, which can be classified in two groups: watermarking based technique (Hsu & Wu, 1999) and digital signature based technique (Friedman, 1993). Some authors had written about digital image authentication systems (Wong, 1998; Holiman & Memos, 2000; Wong & Memon 2001; Celik, et al, 2002; Monzoy, et al, 2007; Cruz, et al, 2008; Cruz, et al, 2009; Hernandez, et al, 2000; Lin & Chang 2001; Maeno, 2006; Hu & Chen, 2007; Zhou, et al, 2004; Lu & Liao 2003) and are classified in three categories: complete authentication, robust authentication and content authentication (Liu & Steinebach, 2006). Complete authentication refers to techniques that consider the whole piece of multimedia data and do not allow any manipulation (Yeung & Mintzer, 1997; Wu & Liu, 1998). Because the non-manipulable data are like generic messages, many existing message authentication techniques can be directly applied. For instance, digital signatures can be placed in the LSB of uncompressed data, or the header of compressed data. Then, manipulations will be detected because the hash values of the altered content bits may not match the information in the altered digital signature.

We define robust authentication as a technique that treats altered multimedia data as authentic if manipulation is imperceptible. For example, authentication techniques, that

tolerate lossy compression up to an allowable level of quality loss and reject other manipulations, such as tampering, belong to this category.

Content authentication techniques are designed to authenticate multimedia content in a semantic level even though manipulations may be perceptible. Such manipulations may include filtering, color manipulation, geometric distortion, etc. We distinguish these manipulations from lossy compression because these perceptible changes may be considered as acceptable to some observers but may be unacceptable to others.

A common objective for authentication is to reject the crop-and-replacement process that may change the meaning of data. Many robust watermarking techniques in literature are designed to be robust to all manipulations for copyright protection purpose. They usually fail to reject the crop-and–replacement process so that they are not suitable for robust authentication and content authentication.

An authentication system can be considered as effective if it satisfies the following requirements:

1. Sensibility: The authenticator is sensitive to malicious manipulations such as crop-and-replacement.
2. Robustness: The authenticator is robust to acceptable manipulations such as lossy compression, or other content-preserving manipulations.
3. Security: The embedded information bits cannot be forged or manipulated. For instance, if the embedded watermarks are independent of the content, then an attacker can copy watermarks from one multimedia data to another.
4. Portability: Watermarks have better portability than digital signatures because the authentication can be conducted directly from only received content.
5. Identification of manipulated area: Users may need partial information. The authenticators should be able to detect location of altered areas, and verify other areas as authentic.

Regardless of security issues, watermarking capacity is determined by invisibility and robustness requirements. There are three dimensions shown in Figure 1. If one parameter is determined, the other two parameters are inversely proportional. For instance, a specific application may determinate how many bits of message are needed. After the embedded amount is decided, it always exists a trade-off between visual quality and robustness which must be considered. Robustness refers to the extraction of embedded bits with an error probability equal to or approaching zero. Watermark imperceptibility (invisibility) represents the quality of watermarked image respect to the original one. In general, if we want to make our watermark more robust against attacks then a longer codeword or larger codeword amplitudes will be necessary to provide better error-resistence. However, visual quality degradation cannot be avoided. Another scenario may be that with a default visual quality, there exists a trade-off between the information quantity of embedded message and robustness. For instance, the fewer the message bits are embedded, the more redundant the code word can be. Therefore, the code word has better error correction capability against noise.

It is difficult for an authenticator to know the purpose of manipulation. A practical approach is to design an authenticator based on the manipulation method. In this work, we design an authenticator which accepts format transformation and lossless compression (JPEG). The authenticator rejects replacement manipulations because they are frequently used for attacks. Our authenticator does not aim to reject or accept, in absolute terms, other manipulation methods because the problem of whether they are acceptable or not depends on applications.

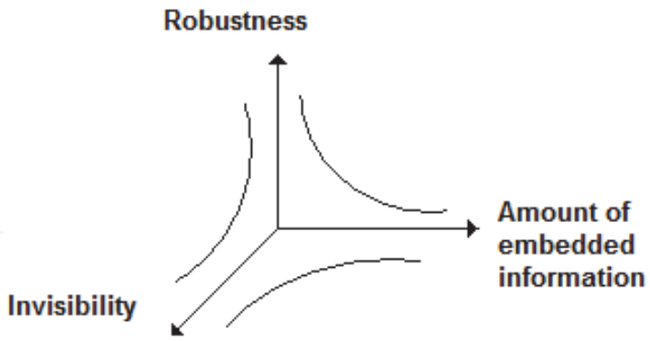


Fig. 1. Parameters of watermarking: Robustness, information quantity of embedded message and invisibility.

2. Previous techniques for robust authentication and content authentication

In Paquet, Ward & Pitas, 2003, a novel watermarking scheme to ensure the authenticity of digital images is presented. Their authentication technique is able to detect malicious tampering of images even if they have been incidentally distorted by common image processing operations. The image protection is achieved by the insertion of a secret author's identification key in the wavelet coefficients by their selective quantization. Their system uses characteristics of the human visual system to maximize the embedding energy while keeping good perceptual transparency and develop an image-dependent method to evaluate, in the wavelet domain, the optimal quantization step allowing the tamper proofing of the image. The nature of multiresolution discrete wavelet decomposition allows the spatial and frequency localization of image tampering. Experimental results show that system can detect unauthorized modification of images.

Kundur & Hatzinakos (Kundur & Hatzinakos, 1999), presented a fragile watermarking technique for the tamper proofing of still images. A watermark is embedded in the discrete wavelet domain by the quantization of the corresponding wavelet coefficients. The Haar wavelet is used for the image decomposition and a pseudo-random binary sequence is generated by a secret identification key. The rounding of the DWT coefficients to even or odd quantization steps embeds the zeros or ones of the watermark. The embedding locations are stored in the coefficient selection key, *ckey*. In addition, an image-dependent quantization key, *qkey*, is introduced to improve security against forgery and monitor specific changes to the image.

In the same line a digital image authentication procedure that allows the detection of malicious modifications, while staying robust to incidental distortion introduced by compression is presented in Yu, et al., 2000. A binary watermark is embedded in the wavelet transform domain. The insertion is again done by the even or odd quantization of selected wavelet coefficients. To increase the robustness of the scheme to image processing operations, the authors proposed to make the embedded watermark more robust by rounding the mean value of weighted magnitudes of wavelet coefficients to quantization levels specified by the predetermined function Q(x,q). The same function is also used in the blind detection process to retrieve the watermark privately by reversed quantization. In order to distinguish malicious tampering from incidental distortion, the amount of modification on wavelet coefficients introduced by incidental versus malicious tampering is modeled as Gaussian distributions with small vs. large variance. The probability of

watermark detection error due to incidental alterations is shown to be smaller than the probability of watermark detection error due to malicious tampering because they produce comparatively smaller variance difference with the embedded marks. The authors argue that this grants a certain degree of robustness to the system and show that their method is able to authenticate JPEG compressed images without any access to the original unmarked image. However, the degree of image compression allowed by the detection procedure is not stated and the selection procedure of quantization parameters is not explained either.

In this work we develop a content authentication technique using imperceptible digital watermarking which is robust to malicious and incidental attacks for image authentication, embedding a digital signature as watermark. A digital signature is a set of features extracted from an image, and these features are stored as a file, which will be used later for authentication. To avoid the extra bandwidth needed for transmission of the signature in a conventional way; having extracted the digital signature we applied the discrete wavelet transform (DWT) to the image to embed the watermark in the sub band of lowest frequency, because we want the watermark insertion to be imperceptible to the Human Visual System and robust to common image processing such as JPEG compression and noise contamination. The proposed system is able to extract the watermark in full blind detection mode, which does not have access to the original host signal, and the watermark extracted has to be re-derived from the watermarked signal, this process increases the system security.

In the security community, an integrity service is unambiguously defined as one which insures that the sent and received data are identical. Of course, this binary definition is also applicable to image, however it is too strict and not well adapted to this type of digital document. Indeed, in real life situations images will be transformed, their pixel values will therefore be modified but not the actual semantic meaning. In other words, the problem of image authentication is released on the image content, for example: when modifications of the document may change its meaning or visually degrade it. In order to provide an authentication service for still images, it is important to distinguish between malicious manipulations, which consist of changing the content of the original image (captions, faces, etc.) and manipulations related to the usage of an image such as format conversion, compression, noise, etc.

Unfortunately this distinction is not always clear; it partly depends on the type of image and its usage. Indeed the integrity criteria of an artistic master piece and a medical image will not be the same. In the first case, a JPEG compression will not affect the perception of the image, whereas in the second case it may discard some of the fine details which would render the image totally useless. In the latter case, the strict definition of integrity is required. We applied the proposed algorithms in to grayscale and color no medical images.

3. Proposed watermarking algorithm

The figure 2(a) shows a general block diagram to the watermark insertion where we can see that original image is divided in non-overlapping blocks, we extracted a digital signature from each block then we insert a signature as watermark in the same block, finally all the watermarked blocks form the watermarked image. Figure 2(b) shows a general block diagram to the watermark extraction process from the watermarked block where we can see that is not necessary to now the original image to extract the digital signature. Finally in the verification process we compare the extracted watermark and the digital signature to determine if the image has been modified, or not.

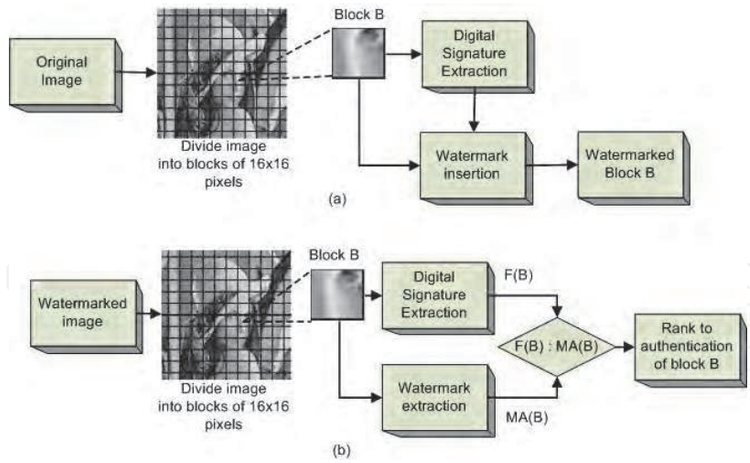


Fig. 2. (a) Watermark insertion system; (b) Watermark extraction system.

3.1 Digital signature generation

The algorithm used to extract the digital signature was proposed in Fridrich, 1999, and used by Chen, et al., 2001. The goal of this algorithm is to make a method for extracting bits from image blocks so that all similarly looking blocks, whether they are watermarked or attacked, will produce almost the same bit sequence of length N. Method is based on the observation that if a low-frequency DCT coefficient of an image is small in absolute value, it cannot be made large without causing visible changes to the image. Similarly, if the absolute value of a low-frequency coefficient is large, we cannot change it to a small value without influencing the image significantly. To make the procedure key-dependent, we replace DCT modes with low-frequency DC-free (i.e., having zero mean) random smooth patterns generated from a secret key (with DCT coefficients equivalent to projections onto the patterns). For each image, we calculate a threshold Th so that on average 50% of projections have absolute value larger than Th and 50% are in absolute value less than Th. This will maximize the information content of the extracted N bits.

Given an image I, we divide it into blocks of 16x16 pixels (for large images, larger block sizes could be used) as showed in Figure 3. Using a secret key K (a number uniquely associated with an author, movie distributor, or a digital camera) we generate N random matrices with entries uniformly distributed in the interval [0, 1]. Then, a low-pass filter is repeatedly applied to each random matrix to obtain N random smooth patterns. All patterns are then made DC-free by subtracting the mean value from each pattern. Considering the block and the pattern as vectors, the image block B is projected on each pattern P_i, $1 \leq i \leq N$ and its absolute value is compared with a threshold *Th* to obtain N bits b_i:

$$if|B.Pi| < Th \quad bi = 0$$

$$if|B.Pi| \geq Th \quad bi = 1 \tag{1}$$

Since the patterns P_i have zero mean, the projections do not depend on the mean gray value of the block and only depend on the variations in the block itself. The distribution of the projections is image dependent and should be adjusted accordingly so that approximately half the bits b_i are zeros and half are ones. This will guarantee the highest information content of the extracted N-tuple. This adaptive choice of the threshold becomes important

for those image operations that significantly change the distribution of projections, such as contrast adjustment.

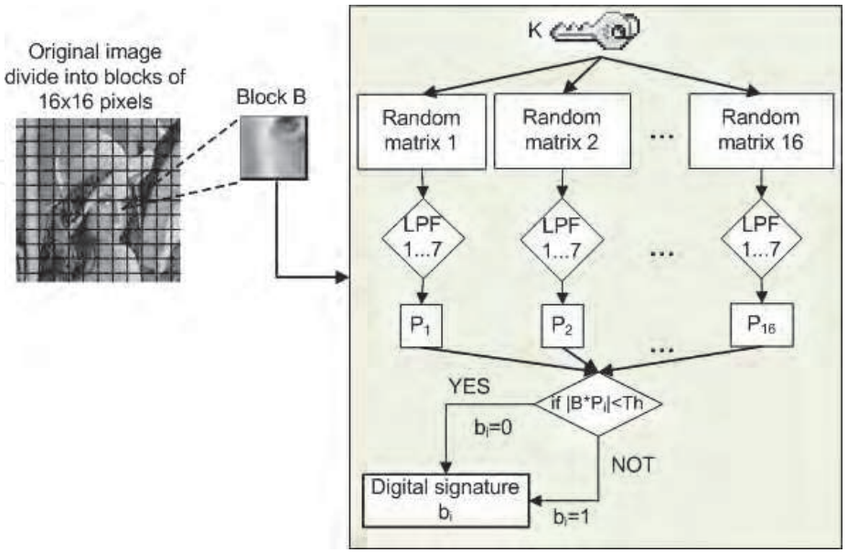


Fig. 3. Digital signature extraction process.

3.2 Wavelet transform for image signals

Two-dimensional DWT leads to a decomposition of approximation coefficients at level j in four components: the approximation at level j + 1, and the details in three orientations (horizontal, vertical, and diagonal).

Figure 4 describes the basic decomposition steps for images.

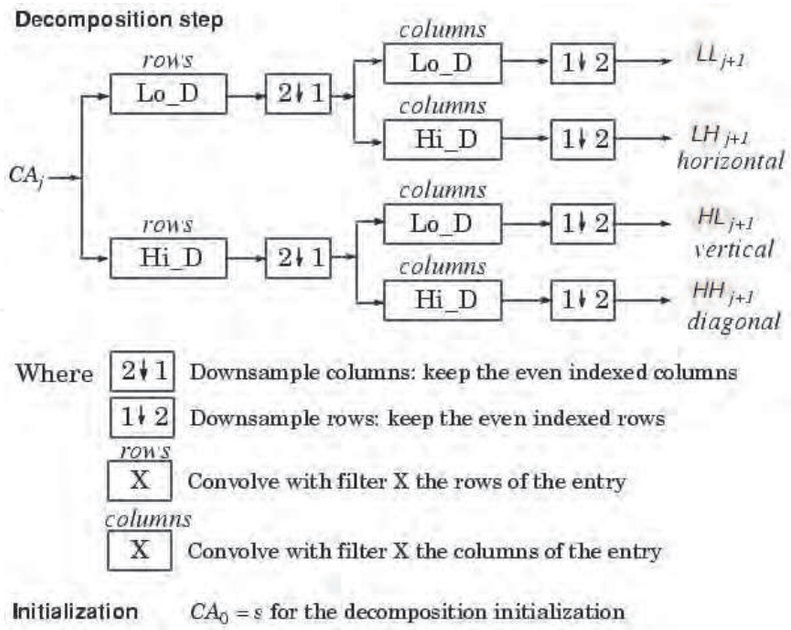


Fig. 4. Subband decomposition using 2D-DWT.

The subbands labeled LH_1, HL_1, and HH_1 represent the finest scale wavelet coefficients. In the present work, the wavelet transform is realized with Daubechies Wavelets of order 2. Using this wavelets, the image is decomposed into four subbands: LL_1, LH_1, HL_1 and HH_1.

3.3 Watermark embedding algorithm

Because we want the embedded watermark to be imperceptible to the Human Visual System (HVS) and robust to common image processing such as JPEG compression and contamination, we implement the algorithm proposed by Inoue, et al. 2000. In this method information data can be embedded in the lowest frequency components of image signals by using controlled quantization process. The data is then extracted by using both the quantization step-size and the mean amplitude of the lowest frequency components without access to the original image.

Once the digital signature is extracted, we applied the discrete wavelet transform (DWT) to embed the watermark, the subband $LL_1(i,j)$ is divided into small subblocks B_k with the size of $b_x \times b_y$ and calculate the mean M_k of the wavelet coefficients of B_k. A quantization step-size which is called the embedded intensity Q=5 is used, then we calculate the mean of the wavelet coefficients of B_k. The watermark information is embedded into the subblock B_k modifying the quantization value q and adds δM_k to the wavelet coefficients of B_k, as described in detail (Inoue, et al. 2000). Finally we construct the watermarked image using the inverse wavelet transform.

Figure 5 illustrates the embedding process; the data w_k =0 or 1 into a subblock B_k when $b_x=b_y$ =2 and Q =5.

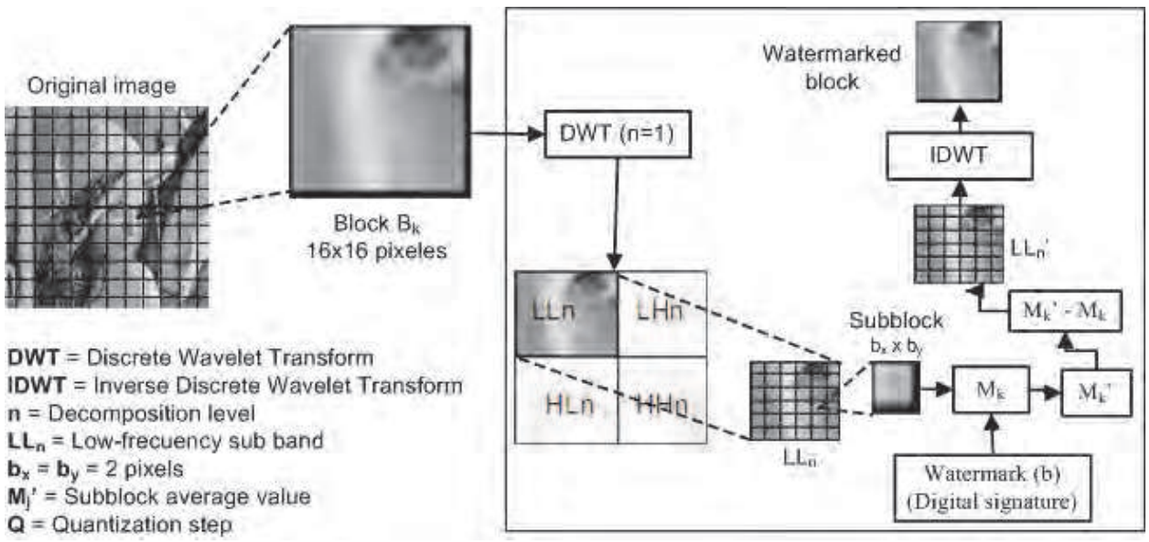


Fig. 5. Watermark insertion process.

3.4 Watermark extracting algorithm

We can extract the embedded data w by using the parameters n (decompose level), b_x, b_y, Q and LM′. Let I′ be the watermarked image, we decompose I′ for the scale 1 and obtain the lowest frequency components $LL_1'(i,j)$. Then we divide $LL_1'(i,j)$ into subblocks B_k with the size of $b_x x b_y$ and compute the mean M_k' of B_k and find the quantization value S from

$$S = int[(M_k') / Q] \tag{2}$$

Then, we extract the embedded binary data w_k as follows: if S is an even number, then w_k =0, otherwise w_k =1.

3.5 Authentication process

After the watermark w_k and the digital signature sequences are extracted from the watermarked image I′, we determines a threshold (Th_v) to decide using an XOR operation if the block is tampered or not, which is expressed in equation (3).

$$if \begin{cases} \sum \widetilde{w_k} \otimes \widetilde{b_k} \leq Th_v \ authentic\ block \\ \sum \widetilde{w_k} \otimes \widetilde{b_k} \geq Th_v \ modified\ block \end{cases} \tag{3}$$

Threshold Th_v was determined through trial and error; resulting value of Th_v was 4, it means that if bits number of digital signature extracted of the block authenticated has at least 12 of 16 bits equal, the block is consider as authentic else it is consider as modified. Although the block is considered modified, sometimes you do not get the same 16-bit digital signature extracted with respect to the original signature can be caused by any intentional modification, which is why we proposed the following process check.

3.6 Verification process

After the watermark w_k from the watermarked image I′ is extracted, we compare it with the digital signature extracted from I′. If they have some different blocks we make an "difference image"(I_{dif}).

According to evaluation carried out using 200 images, in authentication process, the following conclusion was reached: when error blocks are present in regions non intentional modified, these blocks are presented in isolation, as shown in figures 6(a,b), however in the case of images modified intentionally error blocks are detected in concentrated form as shown in figures 6(c,d), so when error blocks are detected isolated, means that region is authentic otherwise it is non-authentic. Therefore to establish a criterion to determine whether the change at a block is intentional or unintentional, we define the following rule:

If there are more than three consecutive error blocks in the region of I_{dif} the image was intentionally modified, otherwise the change was made by common signal processing as JPEG compression or noise. Applying the concept of connectivity between the 8 neighbors of error blocks, it can help us to identify intentionally modified regions of which are not. This criterion is represented mathematically by the equation (4).

$$region \begin{cases} Authentic\ \ if\ \tilde{B} \leq 3 \\ Tampered\ \ if\ \tilde{B} > 3 \end{cases} \tag{4}$$

were $\tilde{B}$ represents an error block, so if there are more than three consecutive error blocks in the region, it has been intentionally modified.

(a) Isolated error blocks

(b) Isolated error blocks

(c) Concentrated error blocks

(d) Concentrated error blocks

Fig. 6. (a,b) Non intentional modified image; (c,d) Intentionally modified image.

4. Experimental results

4.1 Digital signature robustness

To evaluate the robustness of the bit extraction procedure, we subjected the test image "Barbara" with 512x512 pixels and 256 gray levels to various image processing operations available in specialized commercial image manipulation software (we used Photoshop). The test image "Barbara" had 1024 blocks of 16x16 pixels. We extracted N=16 bits from each block for the original image and the manipulated image and calculated the average number of error over all 1024 blocks. The results are shown in Table 1.

Image name	Shine (%)	Average number of error bits
Barb_100	10	0
Barb_200	20	0
Barb_300	30	0
Barb_400	40	0
Barb_500	50	0
	Contrast (%)	
Barb_10	10	0
Barb_20	20	0
Barb_30	30	0
Barb_40	40	0
Barb_50	50	0
Ecualization		0.015
JPEG compression		
Quality factor		Average number of error bits
20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 95 and 100		2.15, 1.98, 1.78, 1.69, 1.51, 1.35, 1.30, 1.22, 1.11, 1.08, 0.98, 0.91, 0.75, 0.67, 0.5, 0.36 and 0.07
Impulsive noise		
Intensity	PSNR	Average number of error bits
0.0010	35.8258	0.58
0.0020	32.3782	0.98
0.0030	30.8060	1.16
0.0040	29.6593	1.23
0.0050	28.6105	1.87
0.0060	27.8483	2.01
0.0070	27.1725	2.22
0.0080	26.5314	2.53
0.0090	26.0121	2.85
0.0100	25.6005	2.92

Table 1. Average number of error recovered bits out of 16 bits after some image processing operations.

4.2 Semi-fragile watermark system performance

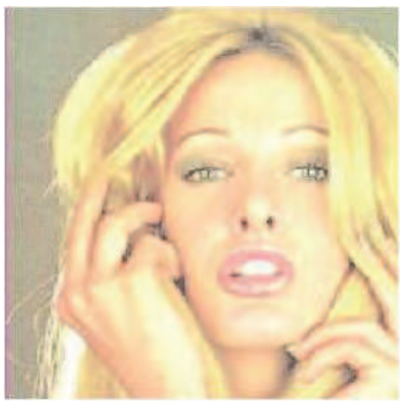
In order to confirm that the proposed digital watermark system is effective, we implemented some numerical experiments with attacks such as JPEG compression, impulsive and Gaussian noise and photomontage. Experimental results show that the algorithm is capable to determine whether the image has been altered. The algorithm was evaluated using 200 standard images. These images are 8 and 24 bits per pixel (bpp) grayscale and color images, which were 512x512 and 128x128 pixels in size showed in figure 7.

Another advantage of this algorithm is that the size and texture of the image doesn´t affect on the correct operation of the system.

(a) 8 bits per pixel (bpp) grayscale image

(b) 8 bits per pixel (bpp) grayscale image

(c) 24 bits per pixel (bpp) color image



(d) 24 bits per pixel (bpp) color image

Fig. 7. Some images used in the experimental process.

4.2.1 Watermarked image quality

In our system we use the peak signal to noise ratio (PSNR) to mesure the degradation of the image quality caused by watermarking, this value is given by (5),

$$PSNR_{dB} = 10\ log_{10} \frac{255^2}{\delta_q^2} \tag{5}$$

where δ_q^2 is the mean square of the difference between the original image and the watermarked one.

Figure 8 shows some examples of original images (in grayscale and color) together with their respective watermarked images and PSNR values, where we can see that watermarked images are to perceptually very similar to the original version. In table 2 PSNR values of some grayscale and color images are shown, where we can observe that the average PSNR value in the grayscale image is 45 dB's and in the color image is 50 dB's, so we can conclude that degradation in the watermarked image is not perceptible.


Original grayscale image


Watermarked grayscale image PSNR=45 dB


Original color image


Watermarked color image PSNR=49.80 dB

Fig. 8. Watermarked image quality.

Grayscale watermarked image	PSNR (dB´s)	Color watermarked image	PSNR (dB´s)
Barbara	45.059944	Plane	49.806491
Boat	44.966452	Mountain	49.848597
Bridge	45.007931	Lake	49.810409
Camera	45.056509	Chiles	49.853756
Chiles	45.003896	People	49.848703
Goldhill	44.959921	Lena	49.815038
Lena	44.958274	Home	50.342928
Baboon	45.041577	Girl	49.568472
Bird	44.962013		

Table 2. PSNR values of some grayscale and color watermarked tested images.

4.2.2 Robustness against JPEG compression

The authenticator is sometimes expected to pass only those images that are compressed by JPEG up to a certain compression ratio or quality factor (fc). For example, if the image is JPEG compressed below to image quality 75 (The Mathworks, 2008), the image is acceptable, otherwise, if it is more compressed, it will fail the test. The argument for failing highly compress images is that such images usually have poor quality and should not be

considered as authentic. To satisfy this need, we calculate the increase of the number of the "different" signature bits after compression (error blocks). The number of the error blocks increases if the image is more compressed. We can set a threshold on this change to reject those images that have too many error blocks.

If the error blocks are isolated, we apply equation (4) to determinate if those blocks are result of a JPEG compression, however, if they are concentrated we are talking about an intentional attack. We called to this process "verification" and it helps us to differentiate between an intentional or non intentional attack.

Figure 9 shows the extracted results from the authentication JPEG compressed watermarked images with quality factors higher than 75 and their corresponding verified image; we can see that compressed images with quality factors higher than 75 have their error blocks (white blocks) isolated; consequently, before the verification process they are considered as not attacked.

Error blocks of "chiles", with fc=75
Authenticated image

Verified image
(not attacked)

Error blocks of "boat", with fc=80
Authenticated image

Verified image
(not attacked)

Fig. 9. Tampered regions detection of the JPEG compressed images.

Table 3 shows some compression ratio where the JPEG compressed watermarked image is considered as authentic by the system. In this table we can see that in grayscale watermarked images were considered as authentic when their quality factor of JPEG compression was higher than 75 and in the color compressed images with a quality factor higher than 70.

4.2.3 Robustness against additive and Gaussian noise

We contaminate watermarked image with different levels of additive and Gaussian noise to simulate the communication channel noise. Tables 4 and 5 show the highest density and variance value of additive and Gaussian noise in grayscale and color images before the system considers the error blocks detected as intentionally tampered, these results indicate that the system is efficient in front of impulsive noise attacks because it supports a density= 0.002 which produces a PSNR average value equal to 32 dB between watermarked image and contaminated watermarked image; a similar case occurs whit the Gaussian noise; the highest variance that the system accepts is 0.00011 before it considered watermarked contaminated image as intentionally modified.

	Quality factor	Error blocks	Original size/ compresion	Bits/ pixel
Grayscale watermarked images				
Boat	80	5	257k/38.7k	1.20
Bridge	75	18	65k/14.6k	1.79
Camera	80	14	65k/10.3k	1.26
Chiles	75	18	257k/31.4k	0.97
Lena	75	4	65k/10.5k	1.29
Baboon	80	24	257k/72.1k	2.24
Bird	80	11	65k/7.56k	0.93
Color watermarked images				
Plane	70	13	193k/11k	0.45
Home	70	5	193k/9k	0.37
Girl	75	17	193k/10k	0.41
Chiles	65	17	193k/14k	0.58
Lake	70	14	193k/14k	0.58
Lena	65	2	193k/11k	0.45
Mountain	75	12	193k/12k	0.49
People	70	11	193k/9k	0.37

Table 3. Compression ratio of some JPEG compressed images considered as authentics.

Grayscale watermarked image	Density	Error blocks	PSNR (dB´s)	Color Watermarked image	Density	Error Blocks	PSNR (dB´s)
Barbara	0.002	27	32.6765	Plane	0.0016	9	33.0454
Boat	0.002	30	32.9256	Home	0.0016	15	33.5461
Bridge	0.002	17	32.1300	Girl	0.0015	18	32.4259
Camera	0.002	36	32.4250	Chiles	0.0024	8	31.4738
Chiles	0.002	26	32.0939	Lake	0.0018	7	32.0180
Goldhill	0.002	11	32.3100	Lena	0.0025	12	31.1327
Lena	0.002	14	32.0448	Mountain	0.0015	18	33.0446
Baboon	0.002	24	32.7793	People	0.0015	26	32.2085
Bird	0.0009	18	35.7967				

Table 4. Test to resistance to impulsive noise from grayscale and color watermarked images.

Grayscale watermarked image	Variance	Error blocks	PSNR (dB´s)	Color Watermarked image	Variance	Error blocks	PSNR (dB´s)
Barbara	0.00011	48	39.5594	Plane	0.00031	14	35.2396
Boat	0.0001	36	40.0032	Home	0.00027	15	35.5625
Bridge	0.00014	22	38.8350	Girl	0.00027	20	35.9495
Camera	0.00011	29	39.5884	Chiles	0.00033	21	35.1859
Chiles	0.00011	37	39.5761	Lake	0.00027	10	35.5499
				Lena	0.00031	16	35.2449
				Mountain	0.00027	24	35.5431
				People	0.00027	23	35.8596

Table 5. Test to resistance to gaussian noise from grayscale and color watermarked images.

4.2.4 Robustness against photomontage

Of course, an important aspect of our system is its ability to localize tampered regions into the image. For that reason, we have tampered the previously watermarked Bird and lake images and evaluated the ability of our system to detect. We found that the ability of our system to detect tampering is excellent (Figure 10) because our system detected correctly which group of blocks were modified intentionally and which were not into the watermarked image, based on the assumption explained in section 2.5. To tamper the images we used Photoshop. Figures 10(a) to 10(d) show the results of this evaluation in grayscale images and figures 10(e) to 10(g) the results of color images. Figures 10(c) and 10(g) show by white blocks the tampered detected by our system where we can see that its location is correct comparing 10(a) vs. 10(b) and 10(e) vs. 10(f) where the first are the watermarked images and the others are the tampered watermarked images. Finally in figure 10(d) we see that the verification is working well because it eliminates the isolated error blocks which were caused by the processing image.

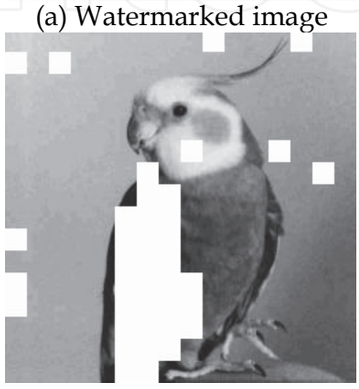
5. Conclusion

The transition from analog to digital technologies is widely used, with the higher capacity of storage devices and data communication channels, multimedia content has become a part of our daily lives. Difital data is now commonly used in many areas such as education, entertainment, journalism, law enforcement, finance, health services, and national defense. The low cost of reproduction, storage, and distribution has added an additional dimension to the complexity of the problem. In a number of applications, multimedia needs to be protected for several reasons. Watermarking is a group of complementary technology that has been identified by content provider to protect multimedia data.

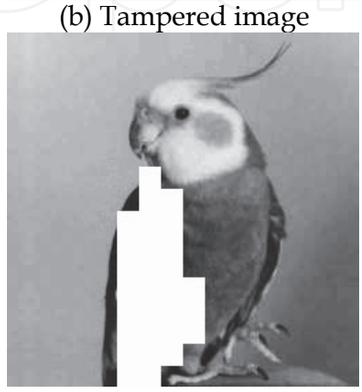
In this paper we have successfully developed a robust digital signature algorithm which is used as a semi-fragile watermarking algorithm for image authentication. The highest advantage of this combination besides the digital signature robustness and the watermark image imperceptibility, is that is not necessary an additional band width to transmit the digital signature, since this is embedded in the host image as a watermark. Besides to the extraction and authentication process, we propose a verification process, which helps us to differentiate between an intentional or non intentional modification applying the concept of connectivity between the 8 neighbors of error blocks.

(a) Watermarked image

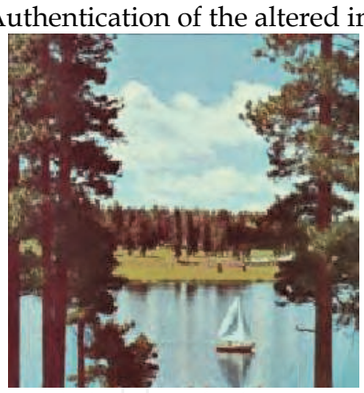
(b) Tampered image



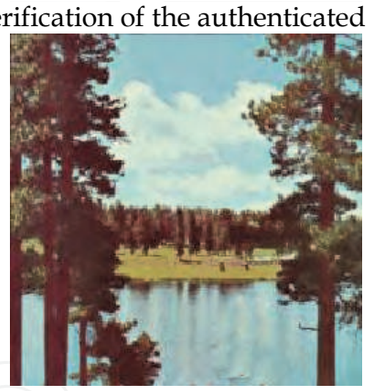
(c) Authentication of the altered image



(d) Verification of the authenticated image



(e) Watermarked image



(f) Tampered image

(g) Authentication of the altered image

Fig. 10. Authentication and verification process of a tamper watermarking grayscale and color image.

Numerical experiments show that this algorithm is robust to JPEG lossy compression, the lowest acceptable JPEG quality factor is 75 for grayscale images and 70 for color images. In the case of impulsive noise, verification system determines that a watermarked image has no-intentional modification if its density value is less than 0.002 which produce a PSNR average value equal to 32 dB between watermarked image and contaminated watermarked image; a similar case occurs with the Gaussian noise; the highest variance that the system accept is 0.00011 before it consider watermarked contaminated image as intentionally modified.
An important characteristic of this system besides its robustness against common signal processing is its capacity to detect the exact tampered locations, which are intentionally modified. Several watermarking systems using digital signature had been reported but they aren't robust to JPEG compression neither to modifications caused by common signal processing.
Finally it is important to mention that the watermarked images generated by the proposed algorithm are secure because the embedded watermarks are dependent on their own content.

6. Acknowledgment

This work is supported by the National Polytechnic Institute of México.

7. References

Celik, M.; Sharma, G.; Saber, E. & Tekalp, A. (2002), Hierarchical Watermarking for Secure Image Authentication with Localization, *IEEE Transactions on Image Processing*, Vol. 11, No. 6, pp. 585–595.

Chen, T.; Wang, J. & Zhou, Y. (2001), Combined Digital Signature and Digital Watermark Scheme for Image Authentication, *Info-tech and Info-net, 2001. Proceedings. ICII 2001 - International Conferences on*, Vol. 5, pp. 78-82, Print ISBN: 0-7803-7010-4.

Cruz, C. ; Reyes, R.; Nakano M. and Pérez, H. (2009), Image Authentication Scheme Based on Self-embedding Watermarking, *CIARP '09 Proceedings of the 14th Iberoamerican Conference on Pattern Recognition: Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications*, ISBN: 978-3-642-10267-7.

Cruz, C.; Reyes, R.; Mendoza, J.; Nakano, M. and Pérez, H. (2008), A Novel Verification Scheme for watermarking based Image Content Authentication Systems, *Telecommunications and Radio Engineering*, vol. 67, no. 19, pp. 1777-1790, 2008, ISSN:0040-2508, http://begelhouse.com

Fridrich, J. (1999), Robust Bit Extraction from Images, Proceedings of IEEE International Conference on Multimedia Computing and Systems (ICMCS'99), Vol. 2, pp. 536-540, ISBN:0-7695-0253-9.

Friedman, G.L. (1993), The Trustworthy Digital Camera: Restoring Credibility to the Photographic Image, *IEEE Transactions on Consum. Elec.*, Vol. 39, pp. 905–910.

Hernández, V. ; Cruz, C. ; Nakano M. and Pérez, H. (2000), Algoritmo de Marca de Agua Basado en la DWT para Patrones Visualmente Reconocibles, *IEEE Latin America Transactions*, Vol. 4, No. 4, June 2006.

Holiman, M. & Memos N. (2006), Counterfeiting Attacks on Oblivious Block-Wise Independent Invisible Watermarking Scheme, *IEEE Transactions on Image Processing*, Vol. 9, No. 3, pp. 432-441.

Hsu, C. T. & Wu, J.I. (1999). Hidden Digital Watermarks in Images, IEEE *Transactions on Image Processing*, Vol. 8, pp. 58–68.

Hu, Y. & Chen, Z. (2007), An SVD-Based Watermarking Method for Image Authentication, *Proceedings of the Sixth International Conference on Machine Learning and Cybernetics*, pp. 1723-1728, Hong Kong, 19-22 August (2007).

Inoue, H.; Miyazaki, A. & Katsura, T. (2000), A Digital Watermark for Images Using the Wavelet Transform, *Journal Integrated Computer-Aided Engineering*, Vol. 7, No. 2, pp. 105-115.

Kundur, D. & Hatzinakos, D. (1999). Digital watermarking for telltale tamper proofing and authentication, *Proceedings of the IEEE*, Vol. 87, No.7, pp. 1167–1180.

Lin, C. & Chang S. (2001), A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation, *IEEE Transactions on Circuits and systems of Video Technology*, Vol. 11 No. 2, pp. 153-168.

Liu, H. & Steinebach, M. (2006), Semi-Fragile Watermarking for Image Authentication with High Tampering Localization Capability, Proc. of Int. Conf. Automated Production of Cross Media Content for Multi-Channel Distribution, ISBN:0-7695-2625-X.

Lu, C. & Liao, H. M. (2003), Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme, *IEEE Transactions on Multimedia*, Vol. 5, No. 2, pp. 161-173.

Maeno, K.; Sun, Q.; Chang, S. & Suto, M. (2006), New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Nonuniform Quantization, *IEEE Trans. on Multimedia*, Vol. 8, No. 1, pp. 32-45.

Monzoy, M.; Salinas, M.; Nakano, M. & Pérez, H. (2007), Fragile Watermarking for Color Image Authentication, *4th Int. Conf. Electrical and Electronic Engineering (ICEEE 2007)*, pp. 157-160.

Paquet, H. A.; Ward, R. K. & Pitas, I. (2003). Wavelet packets-based Digital Watermarking for Image Verification and Authentication, *Journal Signal Processing - Special section: Security of data hiding technologies archive*, Vol. 83 Issue 10, Amsterdam, The Netherlands.

The Mathworks. Inc. (2008), Imwrite: Functions (Matlab functions references), Matlab help, Ver. 7.6.0.324.

Wong, W. P. (1998), A Public Key Watermark for Image Verification and Authentication, *Proceedings of the IEEE Int. Conf. Image Processing*, pp. 425-429.

Wong, W. P. & Memon, N. (2001), Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership Verification, *IEEE Transactions on Image Processing*, Vol. 10, No. 10, pp. 1593-1601.

Wu, M. & Liu, B. (1998), Watermarking for image authentication, *Image Processing, 1998. ICIP 98. Proceedings. International Conference on*. Vol. 2, pp. 437–441, Print ISBN: 0-8186-8821-1

Yeung, M. & Mintzer, F., (1997), An Invisible Watermarking Technique for Image Verification, *Image Processing, International Conference on*, Vol. 2, pp. 680, ISBN: 0-8186-8183-7.

Yu, G.J. ; Lu, C.-S. ; Liao, H.-Y. M. & Sheu, J.-P. (2000). Mean quantization blind watermarking for image authentication, *IEEE International Conference on Image Processing (ICIP'2000)*, Vol. III, pp. 706–709, Vancouver, BC, Canada.

Zhou, X.; Duan, X. & Wang, D. (2004), A Semi-Fragile Watermark Scheme for Image Authentication, Proc. of Int. Conf. Multimedia Modeling Conference, pp. 374 – 377, Print ISBN: 0-7695-2084-7.

Discrete Wavelet Transforms - Algorithms and Applications

Edited by Prof. Hannu Olkkonen

ISBN 978-953-307-482-5
Hard cover, 296 pages
Publisher InTech
Published online 29, August, 2011
Published in print edition August, 2011

The discrete wavelet transform (DWT) algorithms have a firm position in processing of signals in several areas of research and industry. As DWT provides both octave-scale frequency and spatial timing of the analyzed signal, it is constantly used to solve and treat more and more advanced problems. The present book: Discrete Wavelet Transforms: Algorithms and Applications reviews the recent progress in discrete wavelet transform algorithms and applications. The book covers a wide range of methods (e.g. lifting, shift invariance, multi-scale analysis) for constructing DWTs. The book chapters are organized into four major parts. Part I describes the progress in hardware implementations of the DWT algorithms. Applications include multitone modulation for ADSL and equalization techniques, a scalable architecture for FPGA-implementation, lifting based algorithm for VLSI implementation, comparison between DWT and FFT based OFDM and modified SPIHT codec. Part II addresses image processing algorithms such as multiresolution approach for edge detection, low bit rate image compression, low complexity implementation of CQF wavelets and compression of multi-component images. Part III focuses watermaking DWT algorithms. Finally, Part IV describes shift invariant DWTs, DC lossless property, DWT based analysis and estimation of colored noise and an application of the wavelet Galerkin method. The chapters of the present book consist of both tutorial and highly advanced material. Therefore, the book is intended to be a reference text for graduate students and researchers to obtain state-of-the-art knowledge on specific applications.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元

Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen

IntechOpen