

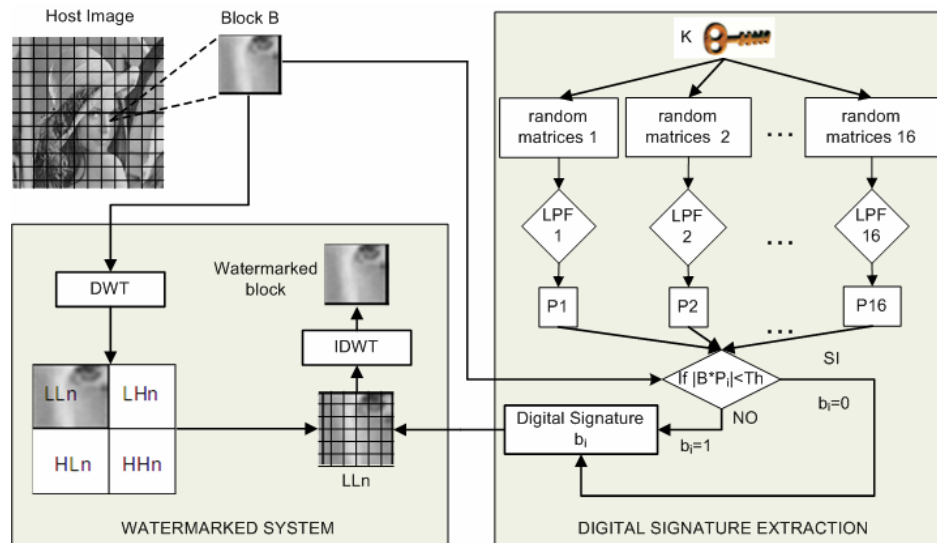
# Robust Image Watermarking System Based in Digital Signature

Clara Cruz, Rogelio Reyes, Mariko Nakano, Héctor Pérez

SEPI ESIME Culhuacan, National Polytechnic Institute of México  
 Av. Santa Ana 1000 Col. San Francisco Culhuacan, CP 04430, México, City. MÉXICO  
 ccruzra@ipn.mx, mariko@calmecac.esimecu.ipn.mx

**Abstract.** The digital watermark technology is now drawing the attention as a new method of protecting copyrights, it is realized by embedding 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, on the other hand, digital signature is another conventional scheme for image authentication, it is a set of features extracted from a media, 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 digital signature scheme, we present in this paper a combined digital signature and digital watermark scheme for image authentication method. The image provider extracts the content-dependent signature from the original image and then embeds it back into the images as a semi-fragile watermark.

## Watermark Embedding Method



**Figure 1.** Block diagram of the digital signature extraction and watermark embedding method

The figure 1 shows a block diagram of the watermark embedding method, where first we divide a host image into blocks of 16x16 pixels. From each image's block a digital signature is extracted by the method proposed by Fridrich [1], having extracted the digital signature we applied the discrete wavelet transform (DWT) to embed the watermark in the subband of lowest frequency into small subblocks  $B_k$  with the size of  $b_x \times b_y$  and

calculate the mean of the wavelet coefficients of  $Bk$ . The watermark information is embedded into the subblock  $Bk$  modifying the quantization value  $q$  and adds  $\delta Mk$  to the wavelet coefficients of  $Bk$  how is detailed in [2]. Finally we construct the watermarked image using the inverse wavelet transform. The data are then extracted by using both the quantization step-size and the mean amplitude of the lowest frequency components without access to the original image. After to extract the watermark from the watermarked image we define the following rule to judge whether a modification is malicious or incidental; first we compare the watermarked and the digital signature both extracted from the watermarked image, if they have some different blocks we make an “difference image”, if we located more than 3 blocks together in the “difference image” that modification is malicious else the modification is caused by common signal processing.

## Experimental Results

The watermark algorithm has been evaluated using gray scale images and color images with different characteristics and sizes, in the case of color images the watermark was inserted in the Y (luminance) channel. Table 1 and 2 shows the values to JPEG compression and adding impulsive and Gaussian noise when the out system say that the modification in the watermarked image is incidental, however such high compression or more noise leads to obvious image degradation, which is rarely used in applications.

Image	PSNR (dB's)	COMPRESSION			IMPSULSIVE NOISE		GAUSSIAN NOISE	
		Quality JPEG	Original size/ compression	Bits/ pixel	Density	PSNR (dB's)	Variance	PSNR (dB's)
Barbara	45	70	257kb/35.6kb	1.10	0.002	32.6	0.00011	39.5
Barco	44.9	80	257kb/38.7kb	1.20	0.002	32.9	0.0001	40
Bridge	45	75	65kb/14.6kb	1.79	0.002	32.1	0.00014	38.8
Camera	45	80	65kb/10.3kb	1.26	0.002	32.4	0.00011	39.5
Chiles	45	75	257kb/31.4kb	0.97	0.002	32	0.00011	39.5
Goldhill	44.9	70	257kb/35.8kb	1.11	0.002	32.3	0.0001	38.8
Lena	44.9	75	65kb/10.5kb	1.29	0.002	32	0.00011	40.1
Mandrill	45	80	257kb/72.1kb	2.24	0.002	32.7	0.0001	39.5
Pájaro	44.9	80	65kb/7.56kb	0.93	0.0009	35.7	0.00011	38.6

**Table 1.** Results of JPEG compression, impulsive and Gaussian noise attacks to gray scale images.

Image	PSNR (dB's)	COMPRESSION			IMPSULSIVE NOISE		GAUSSIAN NOISE	
		Quality JPEG	Original size/ compression	Bits/ pixel	Density	PSNR (dB's)	Variance	PSNR (dB's)
Avión	49.8	70	193kb/11kb	0.45	0.0016	33	0.00011	39.5
Montaña	49.8	70	193kb/9kb	0.37	0.0016	33.5	0.00031	35.2
Lago	49.8	75	193kb/10kb	0.41	0.0015	32.4	0.00027	35.5
Chiles	49.8	65	193kb/14kb	0.58	0.0024	31.4	0.00027	35.9
Personas	49.8	70	193kb/14kb	0.58	0.0018	32	0.00033	35.1
Lena	49.8	65	193kb/11kb	0.45	0.0025	31.1	0.00027	35.5
Casa	50.3	75	193kb/12kb	0.49	0.0015	33	0.00031	35.2
Chica	49.5	70	193kb/9kb	0.37	0.0015	32.2	0.00027	35.5

**Table 2.** Results of JPEG compression, impulsive and Gaussian noise attacks to color images.

Figure 2 shows some gray scale and color images which were modified intentionally, here we demonstrate the system capacity to detect the exact locations, which are intentionally modified.



**Figure 2.** Photomontage test. (a) watermarked image, (b) tamper image, (c) error blocks detected (d) “difference image” to verification process; (e)-(h) photomontage test to color image.

## Conclusions

The numerical experiments show that the proposed method provides a high-quality watermarked image. This algorithm is robust to JPEG compression with compression ratio 17:1. In the case of additive noise or Gaussian noise, if its density is less than 0.0002 for the first or its variance is less than 0.00026 for the second, the system detect that the modification is incidental. An important characteristic of this system besides its robustness against common signal processing is its capacity to detect the exact locations, which are intentionally modified, therefore we can say that these results make sure the information authenticity and protect the copyright. Several watermarking systems used digital signature had been reported but they aren't robust to JPEG compression neither to modifications caused by common signal processing.

**Acknowledgments.** This work is supported by the National Polytechnic Institute of México and National Council for Science and Technology of Mexico.

## References

1. J. Fridrich, “Extracción de Bits Robustos en Imágenes”, in Proceedings of IEEE Internacional Conference on Multimedia Computing and Systems (ICMCS'99), Vol. 2, 1999, pp. 536-540.
2. H. Inoue, A. Miyazaki y T. Katsura, “Marca de Agua Digital en Imágenes Usando la Transformada Wavelet”, Integrated Computer – Aided Engineering, Vol. 7, No. 2, 2000, pp. 105-115.