A Blind Video Watermarking Scheme Robust To Frame Attacks Combined With MPEG2 Compression

C. Cruz-Ramos, R. Reyes-Reyes, M. Nakano-Miyatake*, H. Perez-Meana

D Mechanical and Engineering School, Culhuacan Campus,
National Polytechnic Institute,
Av. Santa Ana no. 1000, Col. San Francisco Culhuacan, 04430
Mexico City, Mexico
*mnakano@ipn.mx

ABSTRACT
In this paper, we propose a robust digital video watermarking scheme with completely blind extraction process where the original video data, original watermark or any other information derivative of them are not required in order to retrieve the embedded watermark. The proposed algorithm embeds 2D binary visually recognizable patterns such as company trademarks and owner's logotype, etc., in the DWT domain of the video frames for copyright protection. Before the embedding process, only two numerical keys are required to transform the watermark data into a noise-like pattern using the chaotic mixing method which helps to increase the security. The main advantages of the proposed scheme are its completely blind detection scheme, robustness against common video attacks, combined attacks and its low complexity implementation. The combined attacks consist of MPEG-2 compression and common video attacks such as noise contamination, collusion attacks, frame dropping and swapping. Extensive simulation results also show that the watermark imperceptibility and robustness outperform other previously reported methods. The extracted watermark data from the watermarked video sequences is clear enough even after the watermarked video had suffered from several attacks.

Keywords: Video watermarking, blind detection method, copyright protection, combination attacks, visually recognizable patterns.

RESUMEN
En este artículo se propone un sistema de marca de agua robusto para la protección de derechos de autor en video digital donde el proceso de extracción de la marca de agua es completamente a ciegas, ya que no requiere ninguna información directa o derivada del video original ni de la marca de agua original. El algoritmo inserta patrones binarios bidimensionales reconocibles visualmente, los cuales pueden ser logotipos de compañías o cualquier otra imagen en el dominio de la DWT de algunos cuadros de video seleccionados aleatoriamente. Antes del proceso de inserción, son necesarias únicamente dos llaves para desordenar los datos de la marca de agua mediante el método de mezclas caóticas, con la finalidad de incrementar la seguridad. Las ventajas principales del sistema propuesto son la extracción de la marca de agua es completamente a ciegas, su bajo costo computacional y su desempeño en contra de ataques combinados al video es mejor que otros métodos propuestos por diferentes autores. Resultados obtenidos demuestran la imperceptibilidad de la marca de agua y que la marca de agua extraída es suficientemente distinguible aún después de que la secuencia de video ha sido sometida a diversos ataques combinados.

1. Introduction

Nowadays, digital video contents are propagated rapidly and widely via the World Wide Web or a Peer-to-Peer Network. These contents can be copied and modified easily by unauthorized people and this situation causes serious copyright violation problems. The development of technical solutions based on watermarking technique for copyright protection has been a topic of active research during the last decade. In the video watermarking, copyright information is embedded into the video data so that the rightful owner may prove his ownership in the case of a dispute, determining if some user is making unauthorized copies of watermarked video or using it in an illegal manner, etc. [1].

A video watermarking scheme involves determining a tradeoff among three conflicting

requirements: imperceptibility, robustness and payload. To obtain watermark imperceptibility, some algorithms employ the perceptual models based on the human visual system (HVS) [2-4]; some of them are applied also in image watermarking schemes [5, 6]. In [2], the visual masking composed by frequency and spatial masking is introduced in the watermark embedding stage. The principal disadvantage of this algorithm is its non-blind detection scheme, which means that the original video sequence is required for watermark retrieval and obviously it impedes the practical use of this algorithm. In [3, 5], the Just Noticeable Distortion (JND) is introduced to generate a visual model allowing the transparency of embedded watermark; however, the watermark detection stage requires the original un-watermarked data (the original video sequence [3] and the original image [5]). In [4], the authors used spatial and temporal perceptual factors to adapt watermark embedding energy, in which the watermark can be detected in a blind manner. It is well worth noting that in all of above algorithms, including image watermarking schemes [5, 6], the watermark signal is a pseudorandom sequence generated by a secret key and the correlation function is used to detect the presence of the watermark sequence. The real payload of this type of watermark is 1 bit, while a watermark sequence that represents a visually recognizable pattern such as logotype, contains multiple bits and in the watermark extraction stage, all bits data must be extracted as correctly as possible. The visually recognizable watermark offers more convincing proof of the ownership than a correlation value, and also it improves the trustworthiness of owner's identification for non-technical arbitrators. Thus the watermarking algorithms that use the visually recognizable watermark must be more ingenious than those that use the pseudorandom watermark, especially in the situations where a blind detection is required.

Watermark robustness is another important requirement for video watermarking schemes. The embedded watermark signal must be robust against intentional or unintentional attacks such as common signal processing, video compression, collusion attacks, frame dropping, frame swapping, etc. Many researchers proposed video watermarking schemes in frequency domains due to the better resilience against several attacks [2], [7-12].

Basically, video watermarking strategies have been classified in three categories: watermarking in the uncompressed video stream, watermarking during the video compression process and watermarking in the compressed video stream. The latter two categories are efficient in a specific video coding such as MPEG2, MPEG4 or H264; however, they show a fatal vulnerability against code conversion such as conversion from MPEG2 to H264, etc. Since recently, coded video streams can be converted easily, using public domain video converters [13-15], into a video stream coded by any other coding system. Taking into account this situation, the watermarking strategy in the uncompressed video stream offers better global robustness compared with the other two categories. Also, for this strategy some efficient image watermarking algorithms can be adapted considering each frame as a still image.

In the watermarking techniques for uncompressed video stream, recently an important number of algorithms have been reported in the literature. Zhuang [8] proposed an algorithm based on video scene segmentation and 3D discrete wavelet transform (DWT), where the watermark is a binary logotype which is disordered converting it into a noise-like pattern. The disordered watermark is then embedded into the 3D wavelet coefficients of a selected video scene. In the detection process, however, this scheme is not completely blind because it requires the disordered watermark generated during the embedding process to extract the embedded watermark. Li [10] proposed a scheme based on 3D-DWT and artificial neural network (ANN) in which the watermark is adaptively embedded in the wavelet coefficients using their statistical features and the relationship among their neighbors. The relationship is constructed by the ANN in the embedding stage and it is saved as the ANN connection weights. In the extraction stage, statistical features of coefficients and their relationship are used. Therefore, this scheme is not completely blind, on the contrary, a large amount of data is required to extract watermark sequence. Fan [11] proposed a completely blind DWT-based video watermarking algorithm applying Direct Sequence Code Division

Multiple Access (DS-CDMA), where the encoded watermark is embedded into the lowest frequency subband LL4 of the DWT transformed video frames. Khalilian [12] proposed a scheme where a binary watermark is embedded into the transformed frames using the 3D Modified Ridgelet Transform (MRT), based on the 3D Discrete Analytical Ridgelet Transform (DART). To extract the watermark sequence, they used a non-blind procedure in which the MRT is applied to both the original and the watermarked video files.

Numerous watermarking algorithms for still images are proposed in the literature, which may be used to develop video watermarking algorithm, some of them employ visually recognizable patters such as logotype, as the watermark sequence [16-19]. In [16], a grayscale image is used as the watermark sequence which is embedded in DWT domain using tree structure of wavelet sub-bands that is the perceptual model used in the EZW compression algorithm proposed by [20]. This algorithm shows the watermark transparency, however, in the watermark extraction stage, the original un-watermarked image is required [16]. In [17] the authors used the JND concept to embed the binary logotype in an imperceptible manner, but this algorithm also uses a non-blind watermark extraction method. Authors of [18] proposed a watermarking scheme using Barni's pixel-wise masking HVS model [6] to embed grayscale logotype images in an imperceptible manner; however, the watermark extraction process also requires the original image. In [19], the grayscale logotype is embedded into a perceptual significant wavelet sub-band (LL) and it can be extracted in a blind manner.

In this paper, a robust video watermarking scheme is proposed, where watermark sequence is a visually recognizable binary pattern; and its embedding and extraction process were performed in the DWT domain of uncompressed video sequence. In the watermark extraction stage, the watermark sequence can be extracted completely in a blind manner. This means that none information derived from the original data is required, neither the original image nor the original watermark. To get watermark imperceptibility and robustness in the completely blind scheme, the embedding strength is adaptively controlled by modifying the statistical characteristics of each block of wavelet coefficients. The statistical characteristics are based on the relationship between a center coefficient of the block and its neighbors, and then in the embedding stage, the center coefficient of the selected block is modified according to its neighbor's value and a corresponded watermark bit. To increase the security of the embedded watermark, the watermark pattern is transformed into a noise-like pattern by using the chaotic mixing method before its embedding. This technique has two advantages: the first one is that the embedded watermark is distributed in the entire frame instead of concentrating on a part of them, while in the second one, the original watermark is not able to be restored without the secret keys, even though that the noise-like watermark can be extracted correctly from the video sequence. Also, the computer complexity required for the watermark extraction process of the proposed scheme may allow it to be used in some real-time applications with a dedicated hardware.

2. Proposed video watermarking scheme

2.1. Watermark embedding

To embed the watermark into the video signal, firstly, the binary watermark image *W* (with values -1 or 1) is transformed into a noise-like two dimensional binary sequence using the chaotic mixing method [21]. In the chaotic mixing method, a mapping matrix $A_N(k)$, with $L_N \to L_N$, is generated, where L_N is a two-dimensional indexes set, and it is applied iteratively to the watermark pattern *W*, as shown by

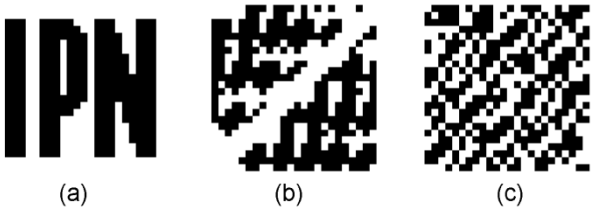
$$W^d = W^{(i)} = A_N^i(k)W^{(0)}, \quad i = 1,2,\ldots,P-1$$

$$A_N(k) = L_N \to L_N, \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (\text{mod } N)$$

(1)

where, $W^{(0)}$ is the original watermark pattern, $W^{(i)}$ is a noise-like watermark pattern after the *i-th* application of $A_N(k), (x_n, y_n) \in L_N, k \in [1, N] \subset Z$, P-*1* is the total number of possible watermarks that can be generated using (1) and N is the size of

$W^{(0)}$. Two keys are required to reconstruct the watermark pattern: the first key is *k* and the iteration number i is the second one. Fig.1 shows the watermark patterns generated by (1) with different iteration i.



(a) (b) (c)

Figure 1. (a) Original watermark, (b) Watermark processed with the Chaotic Mixing using a key *k=5* and iteration *i=5* and (c) Watermark processed with the Chaotic Mixing using a key *k=5* and iteration *i=10*.

The whole host video sequence is used for watermark embedding. Firstly the first level decomposition of each frame of the luminance channel F_r*(r=1,2,..,R)* is computed using a two dimensional Daubechies wavelet function, where R is the total number of frames. Then the noise-like watermark generated by (1) is embedded into the information subband, LL_1. Here the wavelet coefficients of frame F_r are denoted by $X_r\ (r=1,2,\ldots,R)$. Next this noise-like watermark is embedded into the magnitudes of the wavelet coefficients X_r, which are segmented into non overlapping blocks of size 3x3. Then the mean of each block is computed and denoted by M. Subsequently, a bit of watermark is embedded by changing the value of center coefficient V_c of each block to get a modified value $\tilde{V}_c$. Based on two thresholds (Th_1, Th_2) and an intensity factor α, the computation of $\tilde{V}_c$ is carried out as follows:

I. Calculate the magnitude of the difference δ between V_c and M.

$$\delta = \left| V_c - M \right| \tag{2}$$

II. Depending on the value of δ with respect to Th_1, Th_2 and the corresponding bit of $W^d(i,j)$, V_c is modified according with

1) If $\delta > Th_1$, then watermark is not embedded.

2) If $\delta < Th_1$, then watermark is embedded according to the following four cases:

a) If $V_c > M$, $W^d(i,j) = 1$ and $\delta < Th_2$, then the value of V_c of the block under analysis is modified using (3).

$$\tilde{V}_c = V_c + \frac{9}{8}(Th_2 - \delta) + \alpha \tag{3}$$

b) If $V_c < M$, $W^d(i,j) = 1$ and $\delta < Th_2$, then the center coefficient value V_c is modified using (4).

$$\tilde{V}_c = V_c - \frac{9}{8}(Th_2 - \delta) - \alpha \tag{4}$$

c) If $V_c > M$, $W^d(i,j) = -1$ and $\delta > Th_2$, then the center coefficient value V_c is modified using (5).

$$\tilde{V}_c = V_c - \frac{9}{8}(\delta - Th_2) - \alpha \tag{5}$$

d) If $V_c < M$, $W^d(i,j) = -1$ and $\delta > Th_2$, then the center coefficient value V_c is modified using (6).

$$\tilde{V}_c = V_c + \frac{9}{8}(\delta - Th_2) + \alpha \tag{6}$$

Finally, the watermarked video is obtained computing the inverse DWT of the modified wavelet coefficient frames in the luminance channel $\tilde{X}_r$. Figure 2 shows the embedding process.

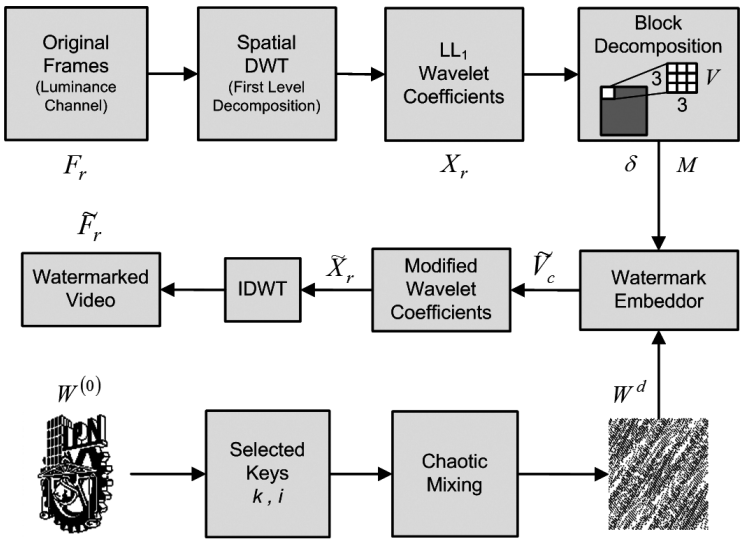


Figure 2. Flowchart of the video watermark embedding scheme.

2.2. Blind watermark detection

The watermark pattern is extracted using a blind manner, in which neither the original un-watermarked video nor the original watermark pattern is required. Based principally on the necessity that the watermark detection process should not be computationally intensive, we propose a simple detection method that extracts a watermark bit from a watermarked video frame depending only on the difference value $\tilde{\delta}$ with respect to the known thresholds Th_1 and Th_2. The watermark detection process is as follows: firstly the first level decomposition of a two dimensional DWT of the luminance channel frames $\tilde{F}_r(r=1,2,\ldots,R)$ of the watermarked video is computed, where R is the total number of frames of the video. Applying the DWT to the *r-th* frame $\tilde{F}_r$, the information subband coefficients *LL1* is got and denoted by $\tilde{X}_r\ (r=1,2,\ldots,R)$. Next, the wavelet coefficients $\tilde{X}_r$ are divided into non-overlapping blocks of 3x3; subsequently the mean value of each block is computed and denoted by $\tilde{M}$. Next, the watermark value $\tilde{W}_r^d(i,j)$ of each block is extracted using the center coefficient $\tilde{V}_c$ of the block; the following operations are carried out:

I. Calculate the magnitude of the difference $\tilde{\delta}$ between $\tilde{V}_c$ and $\tilde{M}$.

$$\tilde{\delta} = \left|\tilde{V}_c - \tilde{M}\right| \qquad (7)$$

II.Depending of the $\tilde{\delta}$ value with respect to Th_1 and Th_2, the corresponding bit of $\tilde{W}_k^d(i,j)$ is obtained according with:

1) If $\tilde{\delta} > Th_1$, then a watermark bit was not embedded and then assigned $\tilde{W}_r^d(i,j) = 0$

2) else if $\tilde{\delta} < Th_1$, then a watermark bit is extracted as follows:

a) If, $\tilde{\delta} \geq Th_2$, then the extracted watermark bit is $\tilde{W}_r^d(i,j) = 1$.

b) Otherwise, $\tilde{W}_r^d(i,j) = -1$

The mean value of the extracted noise-like watermark is computed by (8)

$$\bar{W}^d(i,j) = \frac{1}{R}\sum_{r=1}^{R} \tilde{W}_r^d(i,j) \quad (8)$$

where *R* is the total number of frames used in the embedding process, $\tilde{W}_r^d(i,j)$ is the watermark bit in the *r-th* video frame. Finally the noise-like watermark pattern can be estimated using (9).

$$\hat{W}^d(i,j) = \begin{cases} 1 & \bar{W}^d(i,j) > 0 \\ -1 & \bar{W}^d(i,j) < 0 \end{cases} \quad (9)$$

The reconstructed watermark pattern $\hat{W}^{(0)}$ is estimated from extracted pattern $\hat{W}^d$ by (9), applying the inverse matrix of $A_N(k)$ to $\hat{W}^d$, iteratively until the number of iterations are equal to i as given by (10). Here, two secret keys, k and i, employed in the watermark embedding stage are used.

$$\hat{W}^{(0)} = A_N^{-i}(k)\hat{W}^d \quad (10)$$

Figure 3 shows the proposed watermark extraction scheme.

3. Experimental results

To evaluate the proposed watermarking method, some well-known video sequences such as "Foreman", "carphone" and "bus" are employed.

These sequences are coded in the YUV color space, with a size of 288x352 pixels (CIF format) [22]. The embedded watermark is a binary pattern of size 48x48 pixels. The performance of the proposed video watermarking scheme is evaluated in terms of the normalized correlation (NC) between the original watermark and the extracted one given by (11).

$$NC\left(\hat{W}^{(0)}, W^{(0)}\right) = \sum_i \sum_j \left(\hat{W}^{(0)}(i,j) \cdot W^{(0)}(i,j)\right) \Big/ \sum_i \sum_j W^{(0)}(i,j)^2 \quad (11)$$

Threshold value Th_1 indicates the watermark strength, which controls the compromise between watermark invisibility and robustness. Figure 4 provides evaluation curves to determine the optimum value of Th_1, in which varying the Th_1 value, average values of Peak Signal to Noise Ratio (PSNR) and NC are plotted. The values of other factors such as threshold Th_2 and the intensity factor α formulated in terms of Th_1 are given by (12):

$$Th_2 = \frac{Th_1}{2} \text{ and } \alpha = \frac{9}{16}Th_2 \quad (12)$$

The mathematical reasoning for (12) is provided in the appendix.

Taking into account the watermark imperceptibility (PSNR) and robustness (NC), from Fig. 4, it follows that an optimum value of Th_1 may be considered as 40.

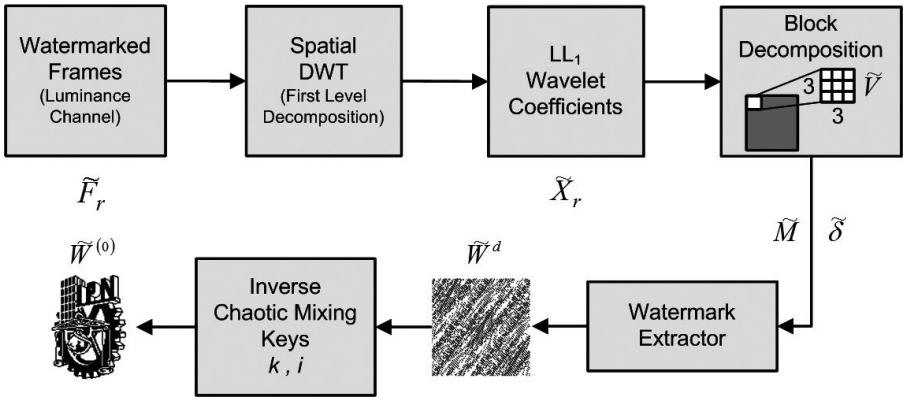


Figure 3. Flowchart of the video watermark detection scheme.

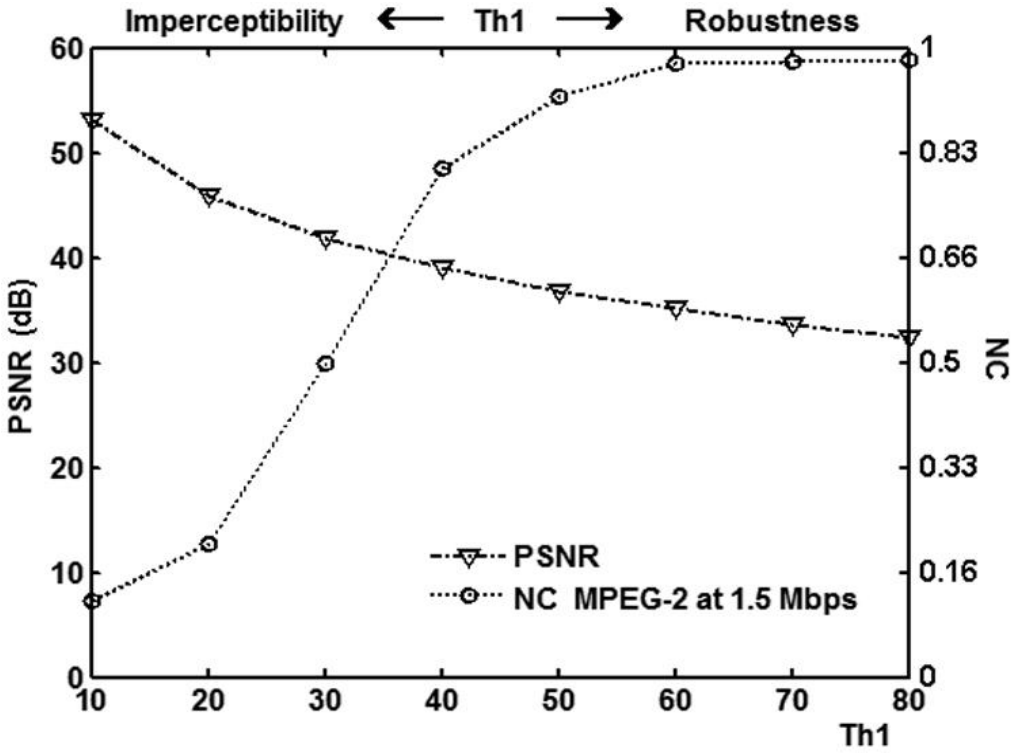


Figure 4. PSNR and NC curves of experimental results.

3.1 Imperceptibility

In order to evaluate the imperceptibility of the embedded binary watermark pattern using the proposed algorithm, two different forms of quality assessment are employed: the first one is an objective image quality assessment given by (13), in which the PSNR of the watermarked video respect to the original one is computed by [23].

$$PSNR_{sequence} = 10\log_{10}\left(\frac{255^2}{\frac{1}{RNM}\sum_{r=1}^{R}\sum_{n=1}^{N}\sum_{m=1}^{M}\left(x_{r,n,m} - y_{r,n,m}\right)^2}\right) \quad (13)$$

where $x_{r,n,m}, y_{r,n,m}$ are values of the *(m,n)* pixel in *r-th* frame of the original and watermarked video sequence, respectively, *M×N* is the frame size and R is the number of total frames. The average PSNR of 10 different video sequences calculated by (13) is approximately 38.95 dB. In the proposed algorithm, the information sub-band LL_1 is used as the watermark embedding domain, which is a most perceptual significant domain. From a watermark imperceptibility point of view, other sub-bands such as LH, HL and HH are appropriate to embed the watermark signal, as shown by Table 1. Two values for threshold Th_1 for each sub-band except LL are determined taking into account the watermark imperceptibility. The bigger value of Th1 provides lower PSNR. The first value of Th_1 of each sub-band provides approximately 40dB of PSNR, while the second Th1 provides approximately 45 dB of PSNR.

Wavelet Sub-band	Th_1	PSNR (dB)		
		Foreman	Bus	Carphone
LL	40	39.08	40.10	38.83
HL	27	39.45	40.27	39.31
	15	44.74	46.99	43.86
LH	27	39.42	40.24	39.22
	15	44.75	47.05	43.65
HH	23	39.66	40.32	39.45
	13	44.64	46.09	44.25

Table 1. Watermark imperceptibility when a different sub-band is used as watermark embedding domain.

The other evaluation is based on a subjective assessment based on the Mean Opinion Score (MOS), then for this evaluation, we apply a questionnaire to 500 people in which they should evaluate the quality of the watermarked video. To this end, firstly, we show the original video sequence without watermark pattern and then the video watermarked sequence is shown. Then the 500 people have to choose one of the five selectable options, shown by Table 2, that better represent the opinion about the quality of the protected video sequence. The average scores obtained are: "Foreman" = 4.3735, "Bus" = 4.3062 y "Carphone" = 4.3846. This evaluation results show that the watermark imperceptibility of the proposed scheme by the human visual system is fairly good. Figure 5 shows some examples used for evaluation of the imperceptibility of the proposed scheme.

Score	Quality of the watermarked video
1	Not acceptable quality
2	Higher distortion
3	Moderate distortion
4	Minimum distortion
5	Identical video sequences

Table 2. MOS Evaluation Criterion.

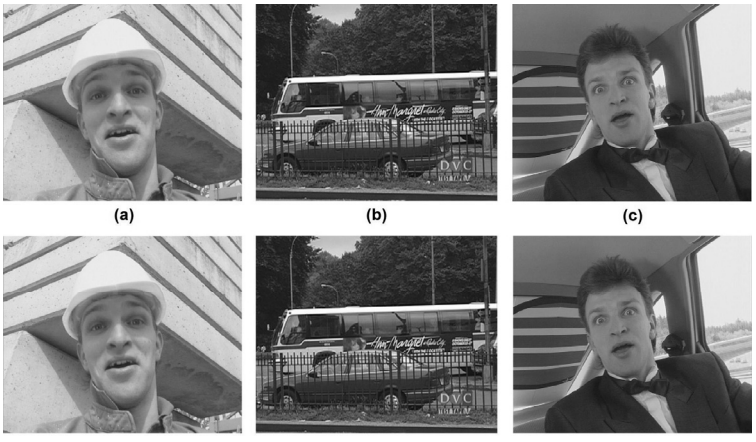


Figure 5. Imperceptibility test. (a)-(c) Original frame of the video sequences "Foreman", "Bus" and "Carphone", respectively; (d)-(e) Watermarked frame of the video sequences "Foreman", "Bus" and "Carphone", respectively.

3.2 Watermark Robustness

Several experiments have been carried out to evaluate the robustness of the proposed watermarking algorithm. For this purpose, some classical video sequence manipulations such as noise contamination, frame dropping, frame swapping, collusion attacks and MPEG-2 compression are used. The evaluation results are compared with previously reported methods [8], [10]-[12]. Actually, combined attacks with MPEG-2 video coding and other video attacks such as frame attacks and noise contamination commonly occurred for video sequences and because the video sequence is always stored in its compressed version, to evaluate substantial watermark robustness of the proposed method, combined attacks are evaluated. In all experiments, 10 different video sequences are used and the average NC value of all independent evaluation is computed.

3.2.1 Classical video attacks

Since digital video is usually compressed with MPEG standard and stored or distributed in compressed format, the robustness of the watermark to MPEG-2 coding at different bit rates from 1.5 Mbps to 15 Mbps is evaluated.

Because the digital video data has high temporal redundancy, the frame dropping or frame cutting, which removes some frames from the video sequence, is an effective video watermark attack because it does not damage the video signal but the embedded watermark can be eliminated. Frame dropping attack is given by (14):

$$V_{attacked} = V_{original} - \{F_{r1}, F_{r2}, ...F_{rn}\} \quad (14)$$

where $V_{attacked}, V_{original}$ are the attacked and original video signals, and are some video frames.

A collusion attack occurs when collections of the video frames are analyzed and combined to destroy the watermark signal without distorting the video sequence to produce copies without watermark signal. To this end some methods have appeared in the literature [24]. An example of such attack is the frame averaging, in which the average of the actual frame with the two nearest neighbors' frames is computed and used to replace the actual frame as given by (15):

$$F'_r(i,j) = \frac{1}{3}\left[F_{r-1}(i,j) + F_r(i,j) + F_{r+1}(i,j)\right] \quad (15)$$

Frame swapping attack, on the other hand, can destroy some dynamic composition of the video signal and also the embedded watermark. This attack is formulated by (16):

$$F_r(i,j) \Leftrightarrow F_{r+1}(i,j), \quad r = 1,3,5,\ldots,R-1 \quad (16)$$

Combined Attacks							
MPEG-2 (2Mbps) together with	**NC**						
	LL	**HL**		**LH**		**HH**	
	40dB	40dB	45dB	40dB	45dB	40dB	45dB
Impulsive Noise (Density=10^{-5})	0.96	0.48	0.24	0.46	0.22	0.31	0.11
Gaussian Noise (Variance 10^{-5})	0.98	0.57	0.27	0.58	0.29	0.29	0.13
Frame Dropping (20 Frames)	0.95	0.62	0.31	0.61	0.32	0.26	0.15
Frame Swapping (20 Frames)	0.92	0.54	0.26	0.51	0.28	0.23	0.12
Frame Averaging (20 Frames)	0.93	0.56	0.25	0.58	0.24	0.25	0.13

Table 3. Watermark robustness to the combined attacks in different embedding sub-bands, measured in terms of NC.

3.2.2 Relationship between watermark robustness and embedding sub-bands

Watermark robustness of the proposed scheme is evaluated in terms of normalized correlation (NC) given by (11). To obtain the relationship between the different wavelet sub-bands as embedding domain and watermark robustness to most common combined attack: the compressed video sequence by MPEG-2 with 2Mbps together with noise contamination or frame attacks. Table 3 shows NC values when the watermark is embedded into each one of four wavelet sub-bands with different threshold values Th_1 indicated in Table 1, providing the average PSNR between 40dB and 45dB.

This table shows that the embedded watermark is not robust when it is embedded into the detail sub-bands such as HL, LH and HH, although these sub-bands offer better watermark imperceptibility.

Figure 6 shows some extracted watermark patterns together with its corresponding NC value to show the relationship between the NC value and the distortion perceived by the human visual system. From this figure, it follows that, to obtain a visually recognizable watermark pattern that allows a rightful ownership claim, the NC value must be larger than 0.7. Therefore, from Table 3, the watermark pattern must be embedded in the LL sub-band.

3.2.3 Comparison with other Previously Reported Algorithms

The performance of the proposed algorithm was compared with other previously reported schemes in the literature [8],[10]-[12]. Table 4 shows the host video property (VSP), quality of the watermarked video (QWV PSNR), NC when MPEG2 compression at 2 Mbps (NC MPG2) is applied, NC when 5 and 20 frames are attacked (NC 5 / 20) by the following frame attacks: collusion attack (C), frame dropping (D), frame swapping (S) and NC when two different noise contaminations, impulsive noise (I) and Gaussian noise (G) are applied. The degradations caused by both noise contaminations are approximately 25 dB of PSNR respect to the watermarked image.

In Table 4, the proposed method shows good performance. The NC value of the extracted watermark pattern is 0.98, after the watermarked video is compressed by MPEG2 with a compression rate of 2Mbps. Although this value is the same as with Li's performance, Li's method requires considerably large additional data for watermark extraction, while our proposed method requires only two numerical keys to extract watermark pattern. About frame attacks, Zhuang's method provides slightly better performance compared with our method, however, again, Zhuang's method is not a completely blind scheme, in which the coded original watermark pattern is required in the extraction process. In the comparison of the proposed method with a completely blind scheme proposed by Fan [11], our proposed method shows better performance, except for the Gaussian noise contamination. In the table, notation '--' means that the data is not available.

3.2.4 Combined attacks with MPEG-2

Although digital technology has brought many benefits to the content creators and consumers, it has also increased the facility in which movies can

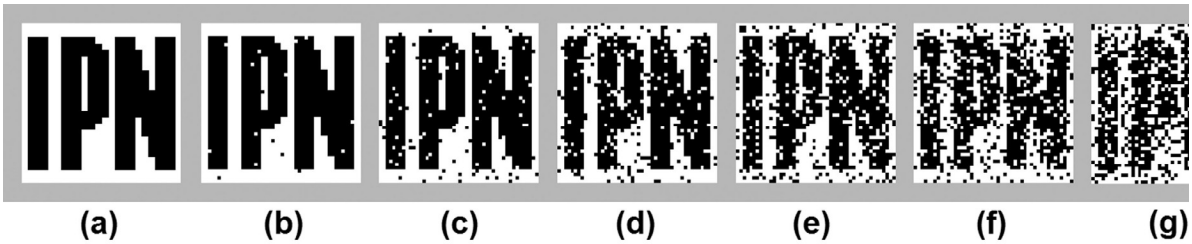
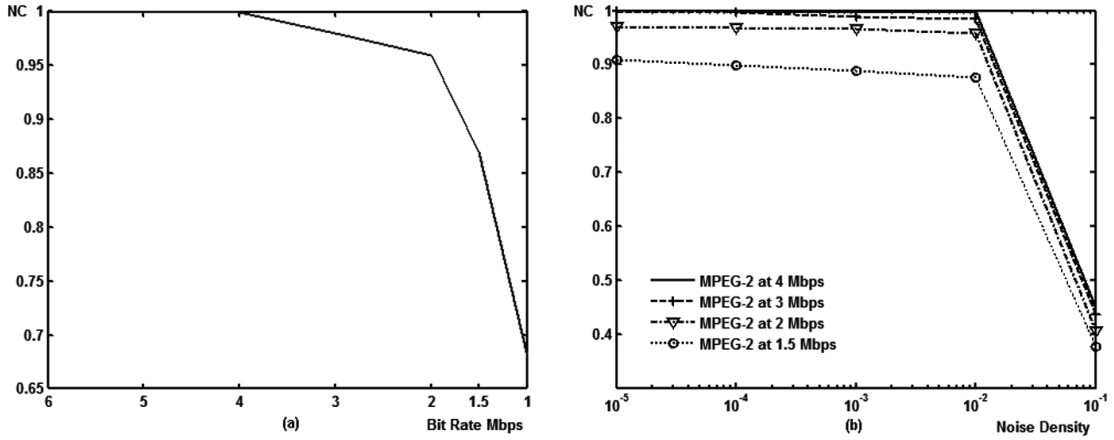


Figure 6. Extracted watermark with different normalized correlation NC respect to the original one; (a) original watermark, (b) NC=0.98, (c) NC=0.9, (d) NC=0.81, (e) NC=0.7, (f) NC=0.6 and (g) NC=0.51.

	VSP	QWV PSNR	MPG2 2 Mbps NC	Frame's Attacks NC			Noise attack NC at 25dB	
				C 5 / 20	D 5 / 20	S 5 / 20	I	G
Proposed Method	352x288 x250	38.95	0.98	0.98 / 0.95	0.98 / 0.97	0.98 / 0.97	0.85	0.75
Li [10]	352x288 x24	39.08	0.98	1.0 / 1.0	---	0.98 / 0.5	---	0.98
Zhuang [8]	352x288 x32	---	**---**	1.0 / 1.0	1.0 / 0.93	1.0 / 0.98	---	0.95
Fan [11]	720x480 x250	40.7	0.84	---	1.0 / ---	---	---	0.89
Khalilian [12]	170x170 x34	44	---	---	0.83 / ---	0.85 / ---	---	0.97

Table 4. Performance comparison of the proposed scheme.

be shared and edited in MPEG2 compressed format using personal computers. This method is commonly used by pirates who illegally duplicate, package, and distribute the movie files all over the world in MPEG2 compressed format. Furthermore, a movie file can be distorted by adding noise or by editing it in order to eliminate or degrade the watermark. Although these combined attacks are commonly used by pirates, experimental results over this kind of attacks are not always reported in literature. Next, we show the performance of the proposed scheme against combined attacks (i.e. frame or noise attacks over a video sequence with high rate MPEG-2 compression). Figure 7 shows the average NC of the extracted watermark under the combined attacks for the well-known video sequences mentioned above. In these experiments we have evaluated each video sequence 10 times and the results are the average values of independent experiments.



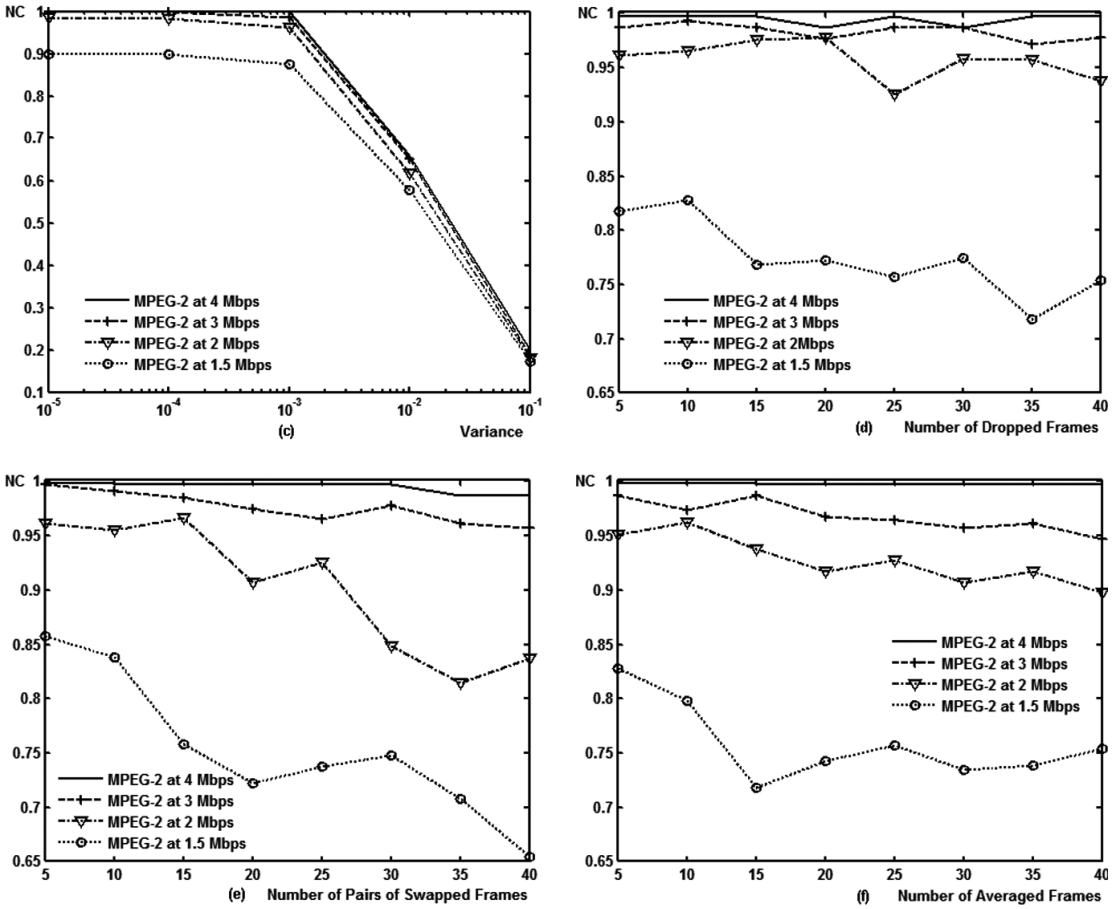


Figure 7. (a) Robustness against MPEG-2 Compression at different lower rates, (b) robustness to MPEG-2 Compression combined with impulsive noise at different densities, (c) robustness to MPEG-2 Compression combined with Gaussian noise at different variances, (d) robustness to MPEG-2 Compression combined with frame dropping, (e) robustness to MPEG-2 Compression combined with frame swapping, (f) robustness to MPEG-2 Compression combined with collusion attack.

We can see from Figure 7(a) that the normalized correlation NC is higher (0.85) even if the watermarked video sequence has been compressed using MPEG2 at a lower bit rate of 1.5 Mbps. The curves shown in Figures 7(b) and 7(c) denote the NC against MPEG2 compression at different bit rates together with impulsive and Gaussian noise, respectively. And they demonstrate that the extracted watermark is sufficiently clear (NC≈0.7), even if the density is 0.03 and the variance is 0.005. Figures 7(d), 7(e) and 7(f) show that the embedded watermark of the proposed scheme is robust against high rate MPEG-2 compression together with frame attacks. In all of these cases, the embedded watermark can be recovered with little or no damage even though up to 20% of the watermarked frames have been modified and the video signal has been compressed using MPEG-2 with a bit rate of 1.5 Mbps. In Figure 6, the NC values shown by Figure 7 are totally acceptable when the compression bit rate and the affected frame number by frame attacks are reasonable.

From the experimental results, the proposed scheme achieves very good performance over

classical video attacks and combined attacks with MPEG-2 compression and classical video attacks, with the advantage that it has a lower computational cost. The robustness of the proposed method is derived from redundant watermarking because the watermark pattern is entirely embedded into all frames. It prevents the attackers from removing the watermark by lossy compression, frame dropping, collusion, etc. If they try to remove one part of the watermark, they need to remove most of the video frames, causing a significant damage to the video signal.

3. Conclusions

A video watermarking algorithm for binary visually recognizable watermark signal was proposed. In the proposed algorithm, a completely blind watermark extraction scheme is used, which means that the watermark is extracted without requiring the original video, original watermark data or some additional information derived from the original video. It makes the video watermarking scheme useful for playback control or any other applications where the original content is not available at the decoder side. The development of a completely blind watermarking scheme is not a trivial task when visually recognizable patterns are used as watermark sequence. Actually, a few video watermarking scheme with completely blind extraction of visually recognizable pattern are reported in the literature [11]. The proposed algorithm is based on the DWT and to improve the watermark security and robustness, the original watermark is transformed into a noise-like pattern using the Chaotic Mixing method and then it is embedded in the video signal. Evaluation results show that the proposed scheme is robust against several classical video attacks such as lossy compression, noise attack, frame dropping, frame swapping, and collusion; and also, the combined attacks with lossy compression and classical video attacks, if the watermark pattern is embedded in the LL sub-bands. Robustness of the proposed method shows a better performance than other previously reported algorithms.

References

[1] Lin E., Eskicioglu A., Lagendijk R. and Delp E., Advances in Digital Video Content Protection, *Proceedings of the IEEE*, Vol. 93, No. 1, January 2005, pp. 171-183.

[2] Swanson M. D., Zhu B., and Tewfik A. H., Multiresolution Scene-Based Video Watermarking Using Perceptual Models, *IEEE Journal on Selected Areas in Communications*, Vol. 16, No. 4, 1998, pp. 540–550.

[3] Wolgang R. B. , Podilchuk C. I., Delp E. J., Perceptual Watermarking for Digital Image and Video, *Proceeding of the IEEE*, Vol. 87, No. 7, 1999, pp. 1108-1126.

[4] Cedillo-Hernández A., Nakano-Miyatake M., Rojas-Cardenas L., Pérez-Meana H., Tecnica de Marca de Agua para Video MPEG usando Sensibilidad Visual y Vectores de Movimiento, *Revista Internacional Información Tecnológica* (Spanish), Vol. 19, No.2. 2008, pp. 81-92.

[5] Podilchuk C. I., Zeng W., Image-Adaptive Watermarking Using Visual Models, *IEEE Journal on Selected Areas in Communications*, Vol. 16, No. 4, 1998, pp. 525-539.

[6] Barni M., Bartolini F., Piva A., Improved Wavelet-based Watermarking through Pixel-Wise Masking, *IEEE Trans. on Image Processing*, Vol. 10, No. 5, 2001, pp. 783-791.

[7] Maes M., Kalker T., Linnartz J., Talstra J., Depovere G. and Haitsma J., Digital watermarking for DVD video copy protection, *IEEE Signal Processing Magazine*, Vol. 17, No. 5, 2000, pp. 47–57.

[8] Zhuang H., Li Y. and Wu C., A Blind Spatial-temporal Algorithm Based on 3D Wavelet for Video Watermarking, *Proc. of IEEE International Conference on Multimedia and Expo*, Taipei, Taiwan, June, Vol 3, No. 1, 2004, pp. 1727-1730.

[9] Biswas S., Das S. and Petriu E., An Adaptive Compressed MPEG-2 Video Watermarking Scheme, *IEEE Trans. on Instrumentation and Measurement*. Vol. 54, No. 5, 2005, pp. 1853-1861.

[10] Li X. and Wang R.. A Video Watermarking Scheme based on 3D-DWT and Neural Network. *Ninth IEEE International Symposium on Multimedia* 2007, Taichung, Taiwan, December, pp. 110-115.

[11] Fan L. and Yanmei F., A DWT-Based Video Watermarking Algorithm Applying DS-CDMA, *IEEE Proc. of TENCON*, Hong Kong, November, Vol. 1, No. 1, 2006, pp. 1-4.

[12] H. Khalilian, S. Ghaemmaghami and M. Omidyeganeh., Digital Video Watermarking in 3-D Ridgelet Domain, *11t^h Int. Conf. on Advanced Communication Technology*, *ICACT* 2009, 15-18 Feb, Gangwon-Do, Korea, Vol. 3, 2009, pp. 1643-1646.

[13] Convert Direct, Moyea Software [Online]. Available: http://www.convertdirect.com

[14] Vixy Project, Farside Inc. [Online]. Available: http://vixy.net

[15] Media Convert, [Online]. Available: http://media-convert.com

[16] Hernández V., Nakano M., Pérez H., A Robust DWT-Based Image Watermarking Algorithm, *WSEAS Trans. on Communications*, No. 10, Vol. 4, 2005, pp. 1048-1057.

[17] Corona B., Nakano M., Pérez H., Adaptive Watermarking Algorithm for binary Image Watermarks, *Lecture Notes in Computer Science*, 2004, pp. 207-215.

[18] Reddy A. A. and Chatterji B. N., A New Wavelet Based Logo-Watermarking Scheme, *Pattern Recognition Letter*, Vol. 26, No. 7, 2005, pp. 1010-1027.

[19] First E., Xiaojun Q., A Composite Approach for Blind Grayscale Logo Watermarking*, IEEE Int. Conf. on Image Processing*, Vol. 3, 2007, pp. 265-268.

[20] Shapiro J. M., Embedded Image Coding Using Zero Tree of Wavelet Coefficients, *IEEE Trans. on Signal Processing*, Vol. 41, No. 12, 1993, pp. 3445-3462.

[21] Voyatzis G. and Pitas I., Embedding Robust Watermarks by Chaotic Mixing, *Proceedings of Conf. Int. Digital Signal Processing*, Santorini, Greece, July, Vol. 1, No. 1, 1997, pp. 213-216.

[22] Plataniotis K. and Venetsanopoulos A., Color Image Processing and Applications, Springer-Verlag, 2000.

[23] Olsson S., Stroppiana M. and Baína J., Objective Methods for Assessment of Video Quality: State of the Art, *IEEE Trans. on Broadcasting*, Vol. 43, No. 4, 1997, pp. 487-495.

[24] Su K., Kundur D. and Hatzinakos D.. Statistical Invisibility for Collusion-Resistant Digital Video Watermarking. *IEEE Transactions on Multimedia*, Vol. 7, No. 1, February 2005. pp. 43-51.

Acknowledgments

We thank Instituto Politécnico Nacional de México (National Polytechnic Institute of Mexico) and the National Council for Science and Technology (CONACyT) of Mexico for the support provided during the course of this research. Also, we thank the reviewer for the useful suggestions to improve the paper.

Appendix

An embedded watermark bit depends on the relationship between the central value V_c and the mean value M of a 3x3 subblock. When the difference value δ between V_c and *M*, $\delta = |V_c - M|$ are calculated and two threshold values Th_1, Th_2 are defined, the watermark embedding algorithm forces this relationship according to the corresponded watermark bit w=1 or -1 as shown by (a1).

$$\begin{aligned} &\text{if } w = 1 \text{ then } Th_2 < \tilde{\delta} < Th_1 \\ &\text{if } w = -1 \text{ then } 0 < \tilde{\delta} < Th_2 \end{aligned} \qquad \text{(a1)}$$

where $\tilde{\delta}$ is the new relationship of the block after a watermark bit is embedded, and it is given by $\tilde{\delta} = |\tilde{V}_c - \tilde{M}|$. Here $\tilde{V}_c$ and $\tilde{M}$ are the central and mean values of the block, after watermarking.

The proposed watermark embedding algorithm calculates $\tilde{V}_c$, adding or subtracting an adequate value to/from the original central value V_c, as given by (3)-(6) in the main text. Firstly if $\delta > Th_1$ then the central point can be considered as a part of then edge and some modification of this value caused visual distortion, therefore the watermark is not embedded into any block with this condition. So the range of δ and $\tilde{\delta}$ for watermark embedding

Is $[0, Th_1]$, threshold value Th_2 classifies binary watermark bit into two regions, therefore $Th_2 = Th_1/2$ is more suitable. Fig A.1 shows a visually scheme of enforcement of $\delta \to \tilde{\delta}$ in the watermark embedding.

Note that if the original is satisfied the condition (a1) then no action dose i.e. $\tilde{\delta} = \delta$.

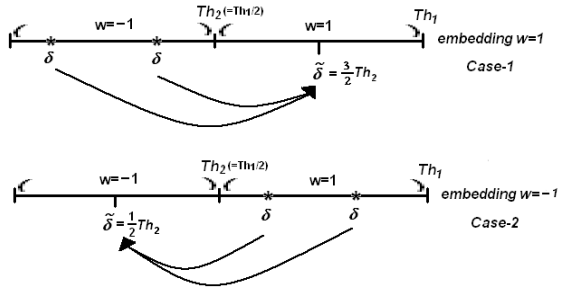


Fig. A1 Visual scheme of watermark embedding

More adequate enforced values $\tilde{\delta}$ of both cases must be determined under watermark imperceptibility and robustness constraints, and the center values of each region, $\tilde{\delta} = \frac{3}{2}Th_2$ in case-1, $\tilde{\delta} = \frac{1}{2}Th_2$ in case-2, are determined. Taking in account these values, the embedding formulas (3)-(6) are constructed. Demonstration is as follows.

From (a2) and $\tilde{M} = M - \frac{V_c}{9} + \frac{\tilde{V}_c}{9}$, formula (3) is got after the following manipulations.

$$\tilde{V}_c - \tilde{M} = \frac{3}{2}Th_2$$

$$\tilde{V}_c - \left(M - \frac{V_c}{9} + \frac{\tilde{V}_c}{9} \right) = \frac{3}{2}Th_2$$

$$\frac{8}{9}\tilde{V}_c = \frac{3}{2}Th_2 - \left(\frac{V_c}{9} - M \right) = \frac{3}{2}Th_2 - \left(V_c - M \right) + \frac{8}{9}V_c$$

$$\frac{8}{9}\tilde{V}_c = \frac{8}{9}V_c + \frac{3}{2}Th_2 - \delta$$

$$\tilde{V}_c = V_c + \frac{9}{8}\left(Th_2 - \delta \right) + \frac{9}{16}Th_2$$

where the intensity factor $\alpha = \frac{9}{16}Th_2$ in (3).

Using a same manner, formulas (4)-(6) can be drawn from (a3)-(a5), respectively, and the intensity factor in all cases is equal to $\frac{9}{16}Th_2$. Once Th_1 is determined experimentally, as shown in Fig.4, other factors in the embedding algorithm are determined by (12).

Authors´ Biographies

Rogelio REYES-REYES

He received the B.Sc. degree in communications and electronics engineering from the Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME), the M.Sc. and Ph.D. degrees in electronic and communications from the Graduate Section of the ESIME Culhuacan of the Instituto Politécnico Nacional (IPN), Mexico. He is a researcher and full-time professor at the Computer Department of the ESIME Culhuacan. From 2004 to present, he has been an assistant professor at the Graduate Section at ESIME Culhuacan-IPN. His main research lines are video and image processing, network security and related fields.

Clara CRUZ-RAMOS

She received the B.Sc. degree in communications and electronics from the Instituto Politécnico Nacional (IPN), Mexico City, in 1999, She obtained the M.Sc. degree in microelectronic and the Ph.D. degree in electronic and communications both from the Instituto Politécnico Nacional in 2003 and 2009, respectively. From January 2002 to present, she has been a researcher and lecturer in the Computer Department, and from 2004 to present, she has been an assistant professor at the Graduate Section at ESIME Culhuacan of the Instituto Politécnico Nacional. Her research and teaching interests are digital image processing, information security, watermarking and related fields.

Mariko NAKANO-MIYATAKE

She received the M.E. degree in electrical engineering from the University of Electro-Communications, Tokyo, Japan, in 1985, and her Ph.D. degree in electrical engineering from The Universidad Autónoma Metropolitana (UAM), Mexico City, in 1998. From July 1992 to February 1997, she worked at the Department of Electrical Engineering of the UAM, Mexico. In February 1997, she joined the Graduate Department of the Mechanical and Electrical Engineering School of the Instituto Politécnico Nacional of Mexico where she is now a professor. Her research interests are in information security, information hiding, adaptive systems and related fields. Dr. Nakano is a member of the IEEE, RISP and the National System of Researchers, Mexico.

Hector PEREZ-MEANA

He received his M.S. degree in electrical engineering from the Electro-Communications University of Tokyo, Japan, in 1986 and his Ph.D. degree in electrical engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 1989. From March 1989 to September 1991, he was a visiting researcher at Fujitsu Laboratories Ltd, Japan. From 2006 to 2009, he was the dean of the Graduate Section of the ESIME Culhuacan ofInstituto Politécnico Nacional of Mexico. In 1991, 1999 and 2000 he received the IEICE excellent Paper Award, the IPN Research Award and the IPN Research Diploma, respectively. In 1998 and 2009, he was the general chair of the ISITA and the MWSCAS. Prof. Perez-Meana is a senior member of the IEEE, member of The IEICE, member of The Mexican System of Researchers, level II, and member of The Mexican Academy of Science. His principal research interests are adaptive systems, image processing, pattern recognition watermarking and related fields.