Real-time Watermarking Algorithm of H.264/AVC Video Stream

Lotfi Abdi[1], Faten Ben Abdallah[2], and Aref Meddeb[2]
[1]National Engineering School of Tunis, University of Tunis-El Manar, Tunisia
[2]National Engineering School of Sousse, University of Sousse, Tunisia

Abstract: *Due to the extensive use of digital media applications, digital productions are easily copied and manipulated. Therefore, multimedia security and copyright protection is becoming important. Digital watermarking is an excellent tool to ensure security and protection of multimedia data by embedding some information into the digital production. For real time applications, such as Internet Protocol-Television (IP-TV) and digital TV broadcasting, a low complexity algorithm should be adopted, when video residing in a server has to be broadcasted by different stations and under different broadcasting rights. In this paper, a low complexity video watermarking scheme for H.264 has been presented. Our contribution is to attain lower complexity in embedding procedure and extracting watermark. At the same time, we avoid a Bit-Rate Increase (BIR) and improve the runtime-efficiency and embedding capacity without sacrificing quality. The watermark is embedded into a video sequence by modifying the number of nonzero-quantized Alternating Current (AC) coefficients in a 4×4 block of I frames. The experimental results show that the proposed method can prevent a BIR and improve the runtime-efficiency and embedding capacity without sacrificing the perceptual quality.*

Keywords: *H264/AVC, video watermarking, compressed domain, bit-rate preservation.*

Received September 9, 2014; accepted May 24, 2015

1. Introduction

The protection of the ownership and the copyright has become an essential task in the digital productions process. These letters can be easily copied and manipulated. Almost all digital video products today are distributed and stored in a compressed format such as Internet Protocol Television (IPTV), video surveillance, video conference and video-on-demand, which have a demand for a much higher compression to meet the bandwidth criteria and the best video quality as possible. However, there is a much scope for developing a low complexity algorithm to embed the watermark in a real time application. On the other hand, new security challenges of the video broadcast are needed to ensure that the media content has not been altered or destroyed whether intentionally or not and that it is accessible only by authorized persons. Digital watermarking has been proposed recently to address these needs, by embedding an imperceptible signature into the digital production. The main requirements of digital watermarking include imperceptibility, robustness and capacity.

In this paper, we have chosen to classify these techniques according to two main criteria: The mode of treatment and the insertion domain. Based on the first criterion, we can distinguish three classes: One representing the shame derived from static-2D-image watermarking, another integrating the temporal aspect, and the last one using the compressed flow. Every class can be subdivided into two under classes by referring to the criterion of the used insertion domain.

In the pre-compression stage, message embedding is performed before the compression process, where the insertion can be spatial by adding the mark directly to the picture (video frame). Otherwise, it can be performed either in the transform domain where the signature is inserted into the coefficients of a certain frequency transformation applied to the video. Several transformations are possible such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) [1] and Discrete Wavelet Transform (DWT) [12]. The video codec structure is the last candidate domain for data hiding. There has been much research activity in the field of video watermarking. The watermark can be added either into the uncompressed or compressed video. Almost all digital video products today are distributed and stored in a compressed format, which is very attractive.

The H.264/AVC video coding standard has become the most widely deployed video codec in almost all applications. As such, various watermarking methods tailored to the H.264/AVC are proposed. For example, Zou and Bloom [13] proposed a blind watermarking algorithm designed for authentication by applying a watermark directly to the entropy coded H.264/AVC stream. The watermark data is embedded in entropy-coded, which changes the H.264 encoded bit stream for watermarking. In [4], a non blind video watermarking schemes was proposed. The proposed scheme took advantage of the H.264 coding standard to embed and extract secret bits. The watermark information was embedded into the encoder by modifying the quantized Alternating Current (AC) coefficients. The Bit rate increase is one of the major problems of this method. In [6], a robust video watermarking algorithm for H.264 was presented. The watermark data was embedded into the last nonzero AC coefficient, with a better robustness, but this approach was relatively complex watermark. In [7], a blind watermarking algorithm for the H.264/AVC was proposed by embedding the message into coefficients of the 4×4 luminance blocks in I frames. These video watermarking techniques were vulnerable to conversion and re-encoding. In [3], a robust video watermarking method with a blind extraction process is proposed. The watermark data was embedded into the P-frames in H.264/AVC compressed video streams, but the increase in the video bit rate was quite high.

The other H.264/AVC watermarking method was proposed in [10], where the data is embedded into some 4×4 blocks of each selected 16×16 MB. The proposed scheme balanced the contradiction between robustness and imperceptibility, but there was a restriction on the watermark capacity. Another watermarking approach for the H.264/AVC is proposed in [11], where a watermark bit was inserted by modifying the quantized coefficient, which controlled the watermark influence towards the bit rate, video quality and security.

In this paper, an efficient technique to add a watermark for real time application has been presented using the H.264/AVC. The proposed scheme is robust against re-encoding and offers consistent payload capability to the H.264/AVC standard at different bitrates without adversely affecting the overall bit-rate and the Peak Signal-To-Noise Ratio (PSNR) of the video bit-stream. The rest of this paper is organized as follows: Section 2 describes our proposed method by elaborating its embedding and extraction steps. We present, in section 3 the experimental results and analysis. Finally, section 4 draws conclusions of this paper and indicates future research direction.

2. Proposed Method

In this section, we describe the procedure of the embedding and detecting watermark. By using the advantages of compressed domain, we analyze the syntactic elements of the H.264/AVC coding standard, whose Quantized I-frame steps (Qstep) are smaller than B and P frames; i.e., B and P frames are quantized more heavily than I frames [9]. So there is a more redundant space to embed watermark in I frames.

In order to guarantee visual imperceptibility, watermark data should be embedded into more textured blocks because the human eyes are less sensitive to noise in edge and detail regions rather than smooth areas. The residual block is a more textured region if there are more nonzero quantized coefficients. Therefore, the Number of Nonzero (NNZ) quantized coefficients can be considered to estimate the texture of residuals. Specifically, the more nonzero quantized coefficients indicate the higher possibility of spatial details in the corresponding block [8]. For reducing the degradation of video quality, watermark information should be embedded into residuals which have a higher value of NNZ.

In this paper, I-frames are chosen as the host frames. Watermark bits are embedded in all intra frames of the video sequence, by modifying the last nonzero quantized AC coefficients in a 4×4 block. The 4×4 block has two main advantages. First, it can be implemented with additions and shifts in 16 bit arithmetic only. Second, in contrast to floating point arithmetic, there is no problem of mismatch on the encoder and decoder side for integer arithmetic [5]. A secret key decides which 4×4 I-frame blocks and which coefficients will be embedded. Our contribution is to propose a robust watermarking scheme with a lower complexity of the embedding and extracting processes. This method is suitable for a real-time encoder system, such as a video conference, IPTV and video surveillance system. The detection procedure is simpler than the embedding one. The watermark can be acquired just by calculating the parity of nonzero quantized AC coefficients in a 4×4 block. The details of embedding and extraction procedure are described as follows.

2.1. Watermark Embedding

We detail in this section the construction of the insertion scheme of the proposed method. As mentioned previously, an algorithm of a strong and effective watermark has to take into account three essential criteria: The signature invisibility, the robustness against diverse attacks (intentional and unintentional), and the insertion capacity to increase the quantity of information to be hidden within the video.

In the proposed watermarking scheme the watermark information is embedded in I-frames by modifying the nonzero-quantized AC coefficients of 4x4 blocks. The original image is divided into 16x16 intra-Macro Blocks (MBs), each containing sixteen 4×4 blocks. Each block is transformed by a DCT transformation and it is quantified by using a specific quantization matrix of an H264/AVC standard. The algorithm only embeds bits into 4×4 blocks; the encoded message is embedded into the quantized luminance DCT coefficients, because the human eye and brain (human visual system) are less sensitive to brightness. As we will see later in this section, the intra prediction modes are prone to change when re-encoding is applied.

An error in the stream caused the decoder to lose synchronization. Moreover, changing some of the intra prediction modes of some blocks leads to different residuals, hence making the embedded watermark unachievable. The watermark embedding in I-4x4 blocks meets the demand of Human Visual System (HVS) [5], in which the human eyes are less sensitive to noises in edge and detail regions rather than in smooth areas. The security of the algorithm is granted by using a random I-4×4 block selection based on the generated content-based key for each MB.

The insertion is done directly on the compressed stream by selecting the nonzero high frequency DCT coefficients in the 4×4 blocks. Since the quantification is simple, it is desirable to insert the watermark after quantization to avoid erasing a possible watermark. The insertion of watermark in the transformed coefficients before quantization can be completely or partially damaged after quantization attacks. The traditional watermarking schemes are not robust against H.264/AVC compression. Our proposed scheme takes advantage of the H.264/AVC codec to embed the secret information. In addition, the entropy decoding and encoding are two fast procedures allowing signature insertion and detection in real time. Further, the mark insertion in these coefficients improves significantly the robustness of the watermarking algorithm and increases the energy of the mark, without a visible deterioration of the processed signal. The block selection using a pseudo random key enhances the security of the proposed method. The signature is transmitted over various frequencies so that the modified coefficients are low. The details of watermark embedding procedures are described as shown in Figure 1.

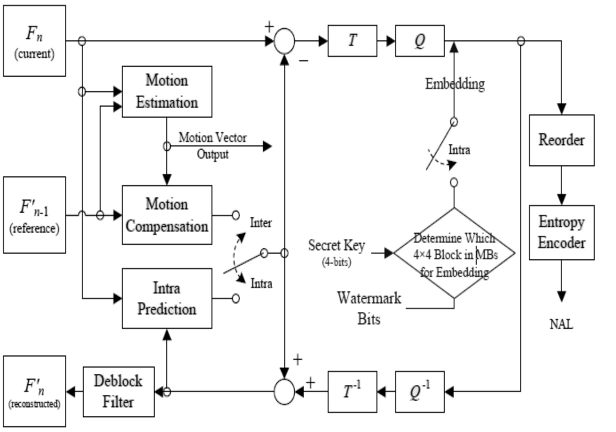

Figure 1. Proposed watermark embedding scheme in H.264/AVC encoder.

For the embedding process, the 4×4 block in which the value of NNZ is no less than threshold K are selected. After quantization, the NNZ AC coefficient in this block is counted. Then, the nonzero AC coefficient is marked as $NZAC_i$, where i is the order of this NZAC coefficient by Zig-Zag scan and a secret key decides which coefficients $NZAC_i$ will be embedded in the block as follows:

$$\text{if } W_j=0 \qquad AC_i = \begin{cases} AC_i & \text{if } 0=NZACi(\text{mod } 2) \\ AC_{i+1} & \text{if } 1=NZACi(\text{mod } 2) \text{ and } NZAC_i>0 \\ AC_{i-1} & \text{if } 1=NZACi(\text{mod } 2) \text{ and } NZAC_i<0 \end{cases}$$
$$\text{if } \mathrm{W_j}=1 \qquad AC_i = \begin{cases} ACi & \text{if } 1=NZACi(\text{mod } 2) \\ ACi+1 & \text{if } 0=NZACi(\text{mod } 2) \text{ and } NZAC_i>0 \\ ACi-1 & \text{if } 0=NZACi(\text{mod } 2) \text{ and } NZAC_i<0 \end{cases} \qquad (1)$$

Our contribution is to attain lower complexity in embedding procedure and extracting watermark. This scheme is suitable for real-time encoding systems such as video streaming of actively fingerprinted content. At the same time, we avoid a Bit-Rate Increase (BIR) and improve the runtime-efficiency and embedding capacity without sacrificing quality. In order to guarantee visual imperceptibility, watermark data should be embedded into more textured blocks. The residual block is a more textured region if there are more nonzero quantized coefficients. Therefore, the NNZ quantized coefficients can be considered to estimate the texture of residuals.

It is necessary to choose the coefficient values that do not affect the video quality and the bit-rate such as the quantized coefficients 0 and 1, which play a key role in the entropy coding step. The modification of the zero coefficient increases considerably the bit-rate and the modification of the bits 1 to 0 affects considerably the video quality. For that, only the NZAC coefficient in a block is changed to embed the watermark. Therefore, it can be used to avoid the watermark embedded into those blocks with all zero coefficients, and thus the change of the bit rate by watermark embedding can be guaranteed to be minor. The zero-valued quantized AC coefficients are also not used for embedding. Furthermore, nonzero coefficient cannot be changed to zero and vice versa, because changing the NNZ coefficients degrades significantly the visual quality and increases the video bit rate. Direct Current (DC) coefficients are not used for embedding because changing them may cause higher visual artefacts and may raise the video bit rate.

2.2.Watermarking Extraction

During the watermark extraction procedure, we use exactly the reverse process of watermark embedding to find the watermarked coefficients. The watermark extraction procedure is performed between entropy decoding and inverse quantization. The details of watermark extraction procedures are described as shown in Figure 2.

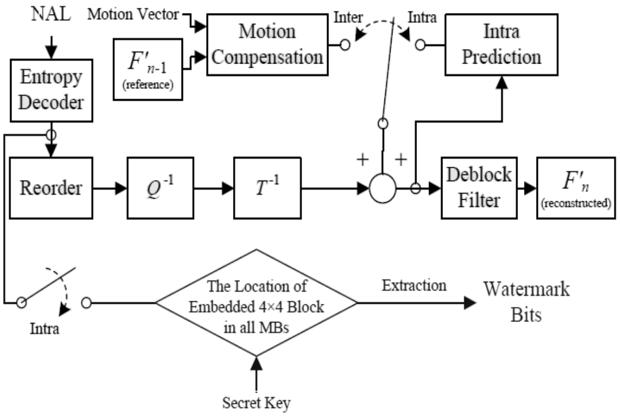

Figure 2. Proposed watermark extraction scheme in H.264/AVC decoder.

First, the decoder has to be informed about the secret key, which can locate the 4x4 embedded block k according to the secret key (the values of NNZ no less than threshold K are selected). Second, the decoder selects the coefficients $NZAC_i$ in the I-4x4 blocks. If it is an odd number, the watermark bit is {1}, otherwise it is {0}. If a H.264/AVC stream receiver suspects that the video stream is tampered with or intentionally modified for any reason, the watermark extraction and verification algorithm can be applied to confirm the authenticity and integrity. The main steps of the watermark extraction and verification are as follows:

$$Aci=\begin{cases} 0 & \text{if } NZAC_i \,(\text{mod } 2) = 0 \\ 1 & \text{if } NZAC_i \,(\text{mod } 2) = 0 \end{cases} \tag{2}$$

If a H.264/AVC stream receiver suspects that the video stream is tampered with or intentionally modified for any reason, the watermark extraction and verification algorithm can be applied to confirm the authenticity and integrity. Evidently, the extraction process is simple and fast, because the hidden authentication information can be detected solely from the nonzero AC residuals and the easily accessible intra/inters prediction modes.

3. Experimental Results

The proposed method is implemented using the H.264/AVC JM 17.4 of the reference software, along with CVLC entropy coding at Quantization Parameter (QP) value 28. To confirm the effectiveness of the proposed watermarking scheme, different benchmark video sequences have been used (“container”, “mother”, “news”, “hall”, “mobile”, “Stefan”) in a QCIF format (176×144). The standard video sequences are encoded into 300 frames at 30 frame/s and with an intra-period of 5 Group Of Picture (GOP) IBPBPB.

This experiment allows justifying the invisibility and robustness of our approach against various attacks that modify the inserted information. In the first step, we are interested in the PSNR, Structural Similarity Index Metric (SSIM) measures to conclude about the quality of the video after embedding the watermark and the BIR. In the second step, the technique robustness is tested against recompression. Finally, we compare the proposed approach with previous works.

3.1. Imperceptibility after Watermarking

To estimate visual imperceptibility of the watermark embedding algorithm, the PSNR is usually taken to evaluate the perceptual quality. For different video contents, the PSNR cannot be a reliable method for assessing the video quality. Another metric objective is also adopted to evaluate the perceptual quality: SSIM. The SSIM index lies in the range of [-1, 1] where -1 indicates zero correlation and 1 indicates that they are identical [7]. Since, the BIR is related to the embedded capacity, we define the BIR Ratio as the percentage of the BIR per embedded bit [11].

$$BIR = \frac{\overline{BR} - BR}{BR \times \textit{Embedded Capacity}} \times 100 \tag{3}$$

Where $\overline{BR}$ and BR are the number of bits for coding the original and watermarked sequences, respectively. The value of PSNR, SSIM, embedded capacity and the increase in the bit-rate (BIR×10^{-3}%) are tabulated in Table 1.

Table 1. Comparing between original video and watermarked sequences for QP=28, using PSNR and SSIM and BIR.

Video Sequence	Embedding Capacity (bits)	SSIM	PSNR decrease (dB)	Bit-Rate Increase (x10^{-3}%)
“container”	1125	0.999	0.07	0.125
“mother”	1068	0.999	0.11	0.165
“news”	1817	1	0.07	0.0448
“hall”	1043	0.999	0.19	0.06
“mobile”	1068	1	0.02	0.0116
“Stefan”	1362	0.999	0.09	0.0135

Table 2. Analysis of the proposed algorithm in terms of PSNR, BIR and embedding capacity for different QP values for the “container” sequence.

QP	Embedding Capacity (bits)	PSNR Decrease (dB)	Bit-Rate Increase(x 10−3 %)
20	5996	0.28	0.056
22	4058	0.17	0.061
24	3097	0.14	0.079
26	2129	0.1	0.1
28	1125	0.07	0.125
30	722	0.08	0.11

The experimental results of Table 2 demonstrate an excellent performance of approach in terms of PSNR, BIR and Embedding capacity for different QP values. For video watermarking, the larger challenge is the bit rate increase. Such an increase could become an important problem when dealing with high definition video sequences.

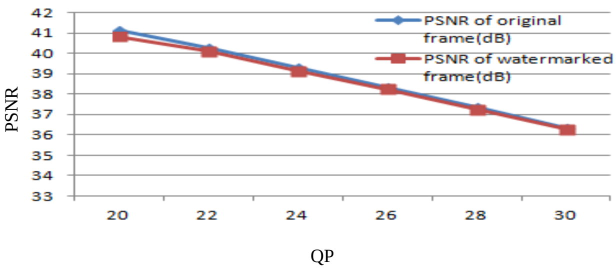

Figure 3. The PSNR before and after watermarking for the "container" sequence.

From Figure 3, we can see that the PSNR of the embedded frames are slightly different from the original frames. The proposed method requires significantly less distortion about 0.09 dB, the SIMM values are all above 0.999 and the increase of bit-rate is less than 0.08 10^{-3} % on average. It is almost impossible to detect the degradation in video quality caused by watermark embedding, which demonstrate that watermark embedding introduces little influence to the video quality, for the reasons of the small differences between the watermarked video sequences and the reference.

3.2. Robustness Against Recompression

Robustness is the resistance of an embedded watermark against intentional attack and normal signal processing operations [13], whereas the re-compression is the most traditional non intentional attack against watermarked videos. For testing the robustness against re-encoding, we attack our video under re-encoding. Bit Error Rate (BER): is defined as the frequency of bit errors when detecting a multi-bit watermark message [7].

$$BER = \frac{Number\ of\ error\ bits}{Total\ number\ of\ bits\ sent} \tag{4}$$

Table 3. Watermark detection rate under re-encoding at different QP values (originally encoded at QP value of 28).

Video\ QP	28	30	32	34
"container"	1.00	0.98	0.83	0.78
"mother"	1.00	0.95	0.81	0.76
"news"	0.98	0.79	0.72	0.77
"hall"	1.00	0.91	0.82	0.78
"mobile"	1.00	0.92	0.87	0.79
"stefan"	0.99	0.86	0.72	0.69

The experimental results of Table 3 show that the watermark is successfully detected and indicates that the algorithm has a good vulnerability. The lowest correct rate is still above 69%. We find that the watermark can be extracted completely in re-compressed videos, even in highly distorted and very low quality video sequences (encoded with a high QP).

3.3. Real-Time Performance

The presented technique avoids full decoding and re-encoding in both embedding and extracting phases. It is of low computational complexity and can meet the requirement of real time performance for IP-TV and digital TV broadcasting. Results related to the Real-timing are tabulated in Table 4.

Table 4. Real-time coding of different video sequences.

Video Sequence	Original Sequence(sec)	Watermarked Sequence(sec)
"container"	279.954	280.522
"mother"	305.156	305.363
"news"	293.863	294.137
"hall"	339.552	340.080
"mobile"	303.471	303.112
"Stefan"	355.534	355.667

The process of detection and extraction should be lightweight to respond in an appropriate time, it can meet the requirement of real-timing. Note that, the proposed method is very suitable for real-time and the BIR is negligible. This is a significant advantage compared to previously proposed methods, which lead to an increase in bit-rate of the watermarked video.

3.4. Comparison with Previous Works

Providing a fair comparison between our proposed method and previous works is difficult since each scheme has special properties under different conditions. For example, we compared the performances of proposed watermarking system with [2] in terms of PSNR and the BIR. We show in Table 5 a performance comparison with [2] in terms of PSNR and BIR.

Table 5. Comparison between the proposed method and the method in [2].

Video Sequence	Proposed method		Method in [13]	
	PSNR (dB)	BIR (%)	PSNR (dB)	BIR (%)
"mother"	0.11	0.00016	0.06	3.97
"hall"	0.19	0.00006	0.15	3.41
"mobile"	0.02	0.00001	0.33	3.84

In comparison to [2], for example the "hall" video sequence we compared the performance in terms of bit-rate increase, PSNR decrease, and payload. In [2], the increase in the bit-rate for I and P frames is 3.41 and 0.66 %, the payload is 3043 and 645bits, and the PSNR decrease is 0.15 and 4.39dB, respectively. In our method, the increase in the bit-rate for I frames is 0.06 10^{-3} %, the payload is 1043bits and the PSNR decrease is 0.19dB.

Our scheme yields better results with an average BIR around 0.07 10^{-3} % and a PSNR decrease under 0.1dB. However, we should witness that the method proposed in [2] offers a higher embedding capacity, but also leads to a higher bit-rate increase. For the sake of comparison with recent work on H.264/AVC watermarking, our approach is faster, more transparent and robust against H.264/AVC recompression. In addition, low complexity, simplicity, ease of implementation, and efficiency in terms of capacity, transparency, and security, make our method an excellent solution for real-time video authentication.

4. Conclusions

In this paper, we have proposed a robust video watermarking algorithm for the H.264/AVC in the compressed domain with a blind extraction process where original video data are not required in order to retrieve the embedded watermark. To design an efficient and low complexity method, the embedding and extracting of watermarks are integrated with the coding and decoding routines of the H.264/AVC. The experiment results show that our scheme can get the same visual effects and a negligible effect on the visual quality. The selection of appropriate blocks, the embedding algorithm, and the use of a pseudo random key preserve the bit-rate and enhance the security of the proposed method. This is a significant advantage compared to previously proposed methods, which lead to an increase in the bit-rate of the watermarked video. Another advantage of our proposed scheme is its runtime efficiency.

Acknowledgments

This work was performed under the MOBIDOC device, part of the Support to Research and Innovation System project (PASRI), funded by the European Union (EU) and administered by the National Agency for Promotion of Scientific Research (ANPR).

References

[1] Amirgholipour S. and Sharifi A., "A Pre-Filtering Method to Improve Watermark Detection Rate in DCT Based Watermarking," *The International Arab Journal of Information Technology*, vol. 11, no. 2, pp. 178-185, 2014.

[2] Bouchama S., Aliane H., and Hamami L., "Reversible Data Hiding Scheme for the H. 264/AVC Codec," *in Proceeding of Information Science and Applications*, Suwon, pp. 1-4, 2013.

[3] Dutta T., Sur A., and Nandi S., "A Robust Compressed Domain Video Watermarking in P-Frames with Controlled Bit Rate Increase," *in Proceeding of Communications*, New Delhi, pp. 1-5, 2013.

[4] Fallahpour M., Semsarzadeh M., Shirmohammadi S., and Zhao J., "A Realtime Spatio-Temporal Watermarking Scheme for H. 264/AVC," *in Proceeding of Instrumentation and Measurement Technology Conference IEEE International*, Minneapolis, pp. 872-875, 2013.

[5] Hamid N., Yahya A., Ahmad R., and Al-Qershi O., "Image Steganography Techniques: an Overview," *International Journal of Computer Science and Security*, vol. 6, no. 3, pp. 168-187, 2012.

[6] Li J., Liu H., Huang J., and Zhang Y., "A Robust Watermarking Scheme for H. 264," *in Digital Watermarking, Springer*, Berlin, pp. 1-15, 2009.

[7] Li Q. and Wang R., "Watermarking in H. 264/AVC Compressed Domain Using CAVLC," *Journal of Computers*, vol. 8, no. 12, pp. 3126-3133, 2013.

[8] Lin S., Chuang C., and Chen M., "A CAVLC-Based Video Watermarking Scheme for H. 264/AVC Codec," *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 11, pp. 6359-6367, 2011.

[9] Liu Z., Cheung G., and Ji Y., "Unified Distributed Source Coding Frames for Interactive Multiview Video Streaming," *in Proceeding of Communications*, Ottawa, pp. 2048-2053, 2012.

[10] Mansouri A., Aznaveh A., Torkamani-Azar F., and Kurugollu F., "A Low Complexity Video Watermarking in H. 264 Compressed Domain," *Information Forensics and Security*, vol. *5*, no. 4, pp. 649-657, 2010.

[11] Shen J., Hu Q., Qiao P., Zhang W., and Liu R., "A Blind Watermarking Method in H. 264 Compressed Domain," *in Advances in Image and Graphics Technologies*, vol. 363, pp. 109-116, 2013.

[12] Shahid Z., Chaumont M., and Puech W., "Considering the Reconstruction Loop for Data Hiding of Intra-and Inter-Frames of H. 264/AVC," *Signal Image and Video Processing*, vol. 7, no. 1, pp. 75-93, 2013.

[13] Zou D. and Bloom J., "H. 264/AVC Stream Replacement Technique for Video Watermarking," *in Acoustics, Speech and Signal Processing*, Las Vegas, pp. 1749-1752, 2008.

Lotfi Abdi is a PhD student in Communication Systems at the National Engineering School of Tunis, Tunis. He received the graduate degree in computer science from the Higher Institute of Applied Sciences and Technology of Sousse, Tunisia, in 2009. He received his Engineer degree in Computer Science from the the National Engineering School of Sousse, Tunisia, in 2012. He received the master degree in Intelligent and Communicating Systems from the National Engineering School of Sousse, Tunisia, in 2013. His research interests include Intelligent Transport Systems, Computer Vision and Augmented Reality.

Faten Ben Abdallah received the Engineering and the MSc degrees from the National Engineering School of Tunis, University of ELMANAR, Tunis, Tunisia, in 2003 and 2004, respectively, and the PhD Degree in Telecommunication from the University of Rennes 2, France in 2009. Since 2010, she is an Associate Professor with the National Engineering School of Sousse, Sousse, Tunisia. She is also an active team member with the Innovation of Communicant and Cooperative Mobiles Laboratory, Higher School of Communications of Tunis, University of Carthage. Her research interests include digital signal, image and video processing for communications and the study of complexity and performance tradeoffs in hardware implementations, with applications in wireless communications.

Aref Meddeb obtained his Engineer’s degree from the National School of Engineering of Tunis, Tunisia, in 1992, and his MS and PhD degrees, both in Electrical Engineering and Computer Science, from Ecole Polytechnique of Montreal , Canada , in 1995 and 1998, respectively. He worked with Alcatel (Tunisia/France), INRS (Canada), Teleglobe (Canada), and Nortel (France). From 2002-2010, he was assistant professor and vice director at the Higher Institute of Computer Science and Communication Technology, University of Sousse where he also headed the Telecommunications Department from 2003-2005. Since 2011, he joined the faculty staff of the National School of Engineering, University of Sousse as Associate Professor where he also heads the Master Degree program in Telecommunications. His research interests include Internet of Things, Sensor Networks, and Intelligent Transport Systems. He mainly focuses on Security, Quality of Service, and Optimization.