Hindawi Publishing Corporation
International Journal of Digital Multimedia Broadcasting
Volume 2016, Article ID 6950592, 9 pages
http://dx.doi.org/10.1155/2016/6950592

Research Article

A Novel Steganography Technique for SDTV-H.264/AVC Encoded Video

Christian Di Laura, Diego Pajuelo, and Guillermo Kemper

School of Electrical Engineering, Peruvian University of Applied Sciences, Lima 33, Peru

Correspondence should be addressed to Christian Di Laura; christian.dilaura@gmail.com

Received 26 September 2015; Accepted 6 April 2016

Academic Editor: Massimiliano Laddomada

Today, eavesdropping is becoming a common issue in the rapidly growing digital network and has foreseen the need for secret communication channels embedded in digital media. In this paper, a novel steganography technique designed for Standard Definition Digital Television (SDTV) H.264/AVC encoded video sequences is presented. The algorithm introduced here makes use of the compression properties of the Context Adaptive Variable Length Coding (CAVLC) entropy encoder to achieve a low complexity and real-time inserting method. The chosen scheme hides the private message directly in the H.264/AVC bit stream by modifying the AC frequency quantized residual luminance coefficients of intrapredicted I-frames. In order to avoid error propagation in adjacent blocks, an interlaced embedding strategy is applied. Likewise, the steganography technique proposed allows self-detection of the hidden message at the target destination. The code source was implemented by mixing MATLAB 2010 b and Java development environments. Finally, experimental results have been assessed through objective and subjective quality measures and reveal that less visible artifacts are produced with the technique proposed by reaching PSNR values above 40.0 dB and an embedding bit rate average per secret communication channel of 425 bits/sec. This exemplifies that steganography is affordable in digital television.

1. Introduction

Over the past decade, digital media have become, without a doubt, part of our daily life. The recent technological achievements in electrical and communications engineering have made feasible the existence of a digital connected world and enormous amounts of data exchange. However, this situation has lately exposed digital media to eavesdropping, counterfeit, and even sabotage, turning it into a major security problem. In pursuit of secure communications, data ciphering techniques have been typically applied and preferred rather than other hiding methods. Notwithstanding, these strategies have failed to protect the reliability of the message itself and have made it completely vulnerable to malicious attacks. In view of this, data concealment techniques, such as steganography, have increased their relevance and catched the attention of researchers. "Steganography," from the Greek *steganos graphos*, means "covered writing" and is considered the art of hiding secret data into a carrier medium so as to convey the confidential message in such a way that it cannot be noticed or detected [1]. A basic steganography framework consists of an embedder and a detector. The first introduces the secret data using a special algorithm into the cover work, generating the so-called stegoobject, and the latter is responsible for extracting the hidden message using the right algorithm.

As of this writing, there have been plenty of research works on the use of media files, such as audio, images, and video, as cover files for steganography. However, they are not designed and applied to current leading technologies, for example, digital television.

Nowadays, digital terrestrial television broadcasting has been successfully implemented. This technology implies the coding and compression of a high quality audio and video source, using a digital video standard and subsequent digital transmission. In order to reach digital television, several video standards have been proposed: H.261 [2], H.262 [3], H.264/AVC [4], and the latest H.265/High Efficiency Video

Coding (HEVC) [5] (which is still under development for digital television). H.264/AVC, the standard most used in practice, has introduced several improvements on the hybrid video encoding paradigm by adding new coding techniques in the spatial, transform, and residual domain, in search of compression. These changes are mainly seen in the use of new prediction schemes for intra- and interprediction, of variable block size within macroblocks, of a new transform core, of the first entropy coding tools that take into account the importance of the context of the data being coded, and of adaptive strategies to reduce the bit rate. The first television specification using H.264/AVC was the Brazilian Digital Television Standard (SBTVD-T), and it is expected that all digital terrestrial television standards will start using it in the coming years.

Under these circumstances, the lack of steganography techniques and applications designed for digital television becomes a field of much interest. Currently, there are no steganography techniques designed for digital television. Furthermore, similar implementations are limited to the use of audio [6] and images [7, 8] as cover media. The most important related works consist of academic articles on watermaking (similar to steganography with the important difference that the data to be concealed is related to the cover file). Nevertheless, only a few of them are suitable for digital television broadcasting, where a real-time, medium embedding-strength, no bit rate increasing technique is desired.

In [9], for example, an interesting watermarking technique was applied by making use of the coding properties of the CAVLC and inter-prediction. The secret message is embedded in the sign bit of the high frequency coefficients, coded as trailing ones, and in fixed bit codes used in transform blocks of inter-predicted frames. Although the original bit rate is not changed, this technique does not consider the error propagation originated by intra-prediction and leaves the possibility of embedding more data into the video stream.

On the other hand, in [10], a self-detection, random watermarking technique using a key-dependent strategy was proposed. The odd and even characteristics of the quantized residual coefficients are used to hide and identify watermarking bits. As a result, a bit rate increment of less than 1% is achieved using this algorithm. This proposal does not take in account the changes on the local context properties and the final perception of the viewer, as it selects the watermark coefficient randomly, so creating possible visual artifacts.

In [11], the authors suggested the use of a perceptual analysis in order to create a robust watermarking technique for H.264/AVC video. This method uses a human vision model created by Watson [12] that embeds the watermark bits in the quantized residual luminance coefficients of which the quantization step size is at least changed by one. By this procedure, embedding capacity is gained. Even if the human perception is considered, this technique increases the bit rate by more than 5% and demands more computational resources. In addition, the perception model from Watson was initially thought for Joint Pictures Expert Group (JPEG) still images based on the Discrete Cosine Transform (DCT). H.264/AVC uses another type of transform: the Integer Cosine Transform (ICT), of which the properties tend to be those of the discrete cosine transform but are indeed not completely the same.

Finally, the works cited use only objective quality measures in order to validate their simulation results and the embedding strength of their techniques. However, they do not consider the human real perception of the resultant encoded video sequences. Hence, subjective quality measures must be considered in future works.

This paper aims to present a real-time, low-complexity, self-detection, and reduced-error-propagation-oriented algorithm, which maintains the bit rate of the stegovideo sequences for digital television. For this purpose, secret messages are hidden in the high frequency coefficients of intrapredicted luminance blocks in an interlaced way and making use of the properties of the entropy coder. In addition, simulation results are analyzed with an objective and subjective perception criterion.

The paper is organized as follows: Section 2 briefly presents the extraction and insertion process of video from digital television and discusses details of the embedding, detection, and enhanced features of the steganography proposal. Section 3 shows the experimental results from objective and subjective quality measures. Finally, Section 4 describes the most remarkable conclusions and provides guidelines for future works.

2. Scheme Proposed

In order to apply steganography to H.264/AVC video sequences from digital television, these need to be separated from the raw digital television bit stream. The way the scheme proposed solves this issue is part of the preprocessing stage of the final algorithm. The digital television stream contains video, audio, control, and synchronization information of different television programs, specially packed using the MPEG-2 Systems specification, also known as transport stream (TS) [13, 14]. The TS standard explains how different television programs composed of audio and video packets, both considered Packetized Elementary Stream (PES), control information, and Programs Specific Information (PSI) composed of the Program Association Tables (PAT), Program Map Tables (PMT), and timing information provided by the Program Clock Reference (PCR), are alternately addressed and labeled with a Packet Identifier (PID) and joined into one compliant bit stream. The selected scheme extracts the Elementary Stream (ES) corresponding to the H.264/AVC video of one of the television programs. The insertion mechanism operates in the same way, but in reverse order. A detailed description of both processes, including the embedding of the secret message using steganography and new features of the proposal, is depicted in Figure 1. It is important to emphasize again that there are currently no state-of-the-art steganography techniques designed for digital television.

2.1. H.264/AVC Detection from MPEG-2 TS. A MPEG-2 TS is composed of 188-byte-long transport packets that contain video, audio, data, and control information of the television

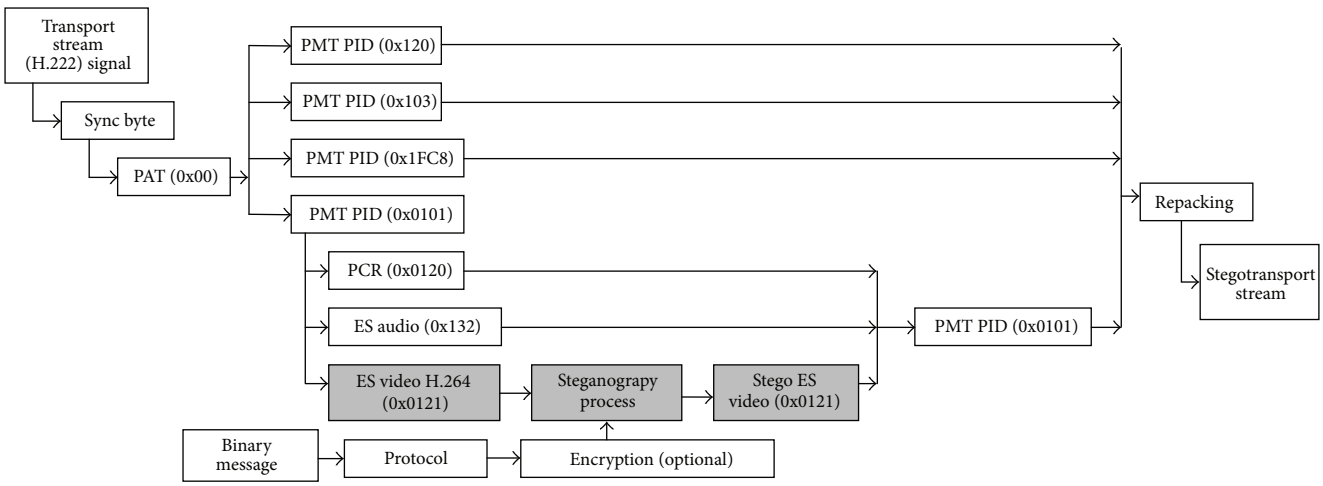


Figure 1: Overview of the scheme proposed.

programs. All of these signals are multiplexed in one bit stream. The first step in the entire preembedding process is to extract the video ES of the chosen program from the TS. The procedure works as follows:

(i) *Synchronizing with the transport stream*: The decoder fetches the synchronization byte in the TS, of which the value is always 0x47 base 16 (HEX). Each synchronization byte must be 188 bytes spaced, without considering any additional data introduced for Forward Error Correction (FEC), before its pattern is repeated.

(ii) *Program Specific Information (PSI)*: There are two relevant tables that describe the instantaneous structure of the transport stream and are sent as part of the control information. The first table is the PAT, which is identified when the PID value equals 0x000 HEX as specified in the standard. This table shows the total programs being carried in the TS and their related PID labels. The second table is the PMT. This table allows associating each PID of an ES, such as video, audio, or additional control data, with its corresponding television program.

(iii) *Accessing a program*: After the PIDs of all ES have become known, it is possible to have access to any program carried by the TS and, therefore, to distinguish between different ES. Assuming that the video and audio PID values are 0x121 HEX and 0x132 HEX, respectively, the stream packets of which the PID value equals 0x121 HEX will be assembled into one video ES and supplied to the next decoding phase (the same will happen if the TS is fetched for the audio ES).

After splitting the TS, one video ES is chosen for embedding purposes. Normally, the first video frame to be decoded is called Intraframe (or I-frame), as it is predicted from samples previously decoded belonging to the same frame. In addition, the TS bit stream format allows the detection of I-frames by using a special byte known as *random access indicator*. In some cases, the first frame will have two partitions or slices: the top is predicted by intraprediction and the bottom by interprediction (also known as P-slice), as is predicted from samples previously coded belonging to other frames or slices.

2.2. Data Hiding Procedure in the H.264/AVC Sequence. The I-frame, where the secret data will be embedded, is divided into 16 × 16-pixel regions defined as macroblocks (this way of splitting is done for coding and compression efficiency purposes). Depending on the intraprediction scheme selected during the coding process, they are once more divided into 4 × 4 or 8 × 8 block sections. H.264/AVC offers three types of intraprediction modes, mainly intra-16 × 16, intra-4 × 4, and intra-8 × 8 (used in high profiles and some television applications). Generally, intra-16 × 16 is chosen for frames or slices (part of a frame) with predominant smooth areas and the intra-4 × 4 for the ones that contain rich amount of details. Intra-8 × 8 is an especial case and will not be considered in this work. Likewise, since human eyes are more sensitive to changes in flat areas, only intra-4 × 4 macroblocks have been chosen for data embedding.

Take into account an I-frame, containing a macroblock region that is coded using intra-4 × 4 prediction mode and divided into block sections of 4 × 4 dimensions (further known separately as "T" blocks). Now, define "$P(i, j)$" as the pixel values of "T" and "$I(i, j)$" as the corresponding intraprediction block, where "i" and "j" stand for the discrete indexes of the rows and columns of the frame, respectively. Their difference, or residual matrix, is labeled as "$R(i, j)$."

H.264/AVC uses the ICT, based on a 4 × 4 dimensional and standardized core, for coding luminance and chrominance residual blocks. Thus, "$R(i, j)$" is transformed, scaled, and quantized warranting the orthogonality and orthonormality properties during the process as explained in [15], generating "$C'(u, v)_t$." Consider "$C'(u, v)_t$" as the residual quantized ICT coefficients of block "T," "$S(u, v)_t$" as the steganography data (in binary form) to be embedded, "$C''(u, v)_t$" as the residual quantized ICT coefficients to which steganography has been applied, "Trc" as an

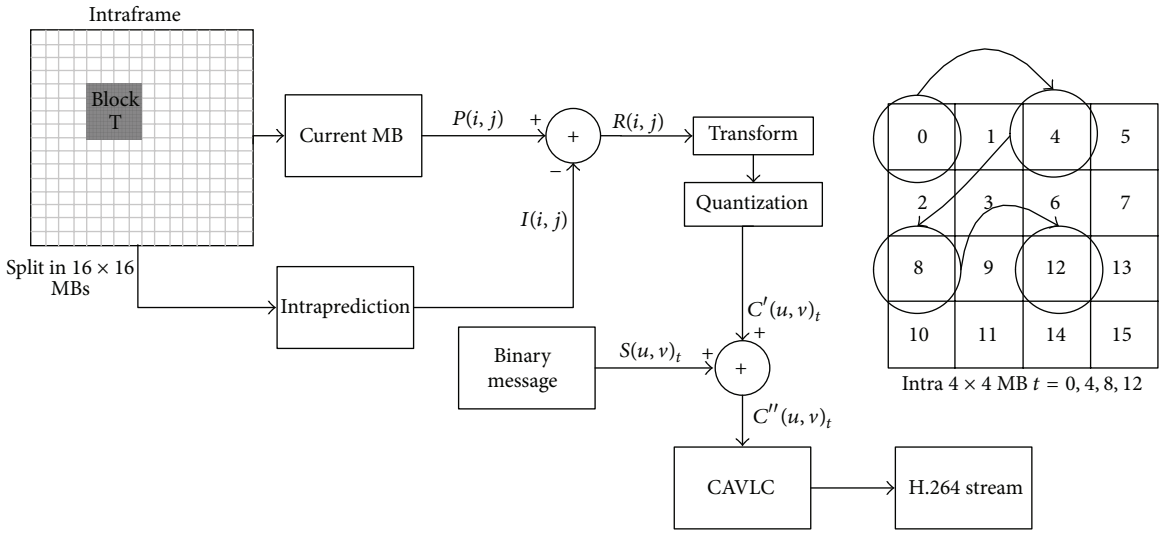


Figure 2: Steganography in H.264/AVC.

experimental-achieved threshold, and "u," "v," and "t" as discrete indexes within block "T." The embedding strategy works as follows.

If "$S(u,v)_t = 0 \wedge C'(u,v)_t >$ Trc." then

$$C''(u,v)_t = \begin{cases} C'(u,v)_t - 1; & \text{if } C'(u,v)_t \bmod 2 = 1 \\ C'(u,v)_t; & \text{if } C'(u,v)_t \bmod 2 = 0 \end{cases} \quad (1)$$

$$u = 0, 1, 2, 4,\ \ v = 0, 1, 2, 4,\ \ t = 0, 4, 8, 12,$$

where "$C'(u,v)_t \bmod 2$" returns the remainder after "$C'(u,v)_t$" is divided by "2." The sign of the result is the same as the divisor.

If "$S(u,v)_t = 1 \wedge C'(u,v)_t >$ Trc." then

$$C''(u,v)_t = \begin{cases} C'(u,v)_t; & \text{if } C'(u,v)_t \bmod 2 = 1 \\ C'(u,v)_t - 1; & \text{if } C'(u,v)_t \bmod 2 = 0. \end{cases} \quad (2)$$

According to Figure 2, the steganographic algorithm proposed works at a quantization level because the sending is a lossless operation and information embedded will not change in reception. The embedding algorithm consists in separating the embeddable block from closer neighbors, inside a macroblock, and leaving one macroblock of space between embeddable macroblocks. The separate spaces where the message is to be hidden are used to reduce visible artifacts, so that subjective quality is not degraded.

There is an exceptional case where the self-collusion attack must be avoided. This is accomplished when "$C'(u,v)_t = \text{Trc} + 1 \wedge S(u,v)_t = 0$." The expected result using (1) would be the same coefficient reduced by one level. However, at the receiver side, the original bit of the hidden message will be lost and the recovering processes will fail. For this reason and only for this special case, the coefficient level is incremented by one. It should be noted that the binary message being embedded could be distributed to make this singular condition less probable. In addition, the stego TS produced does not differ from the original bit stream structure. This is achieved since the bit stream alienation and Program Clock Reference (PCR) are respected and preserved. The algorithm makes use of CAVLC features for limited control of bit rate. The target is to maintain the same H.264 sequence length or decrease some bytes in order to be able to insert the stego-H.264 sequence in the same amount of TS packets.

Four facts must be considered so as not to increase the bit rate:

(i) Not hiding in zero macroblocks.

(ii) Not choosing Trailing Ones coefficients (T1s), as they have a defined code.

(iii) Not choosing zero coefficients in any nonzero macroblock, as the length will be increased.

(iv) Reducing luminance ICT coefficients in one level that will produce a smaller length than the original.

Finally, the resultant I-frame is repacked into the TS and so ready to be transmitted.

2.3. Hidden Message Extraction. The retrieval of the hidden message is fast and simple. By applying the same process shown in Figure 2 to extract an I-frame, and after entropy decoding the H.264/AVC video, embeddable macroblocks are chosen and ready to extract the hidden message. The way the secret message is recovered, bit by bit, is given in

$$S(u,v)_t = \begin{cases} 0; & \text{if } C''(u,v)_t \bmod 2 = 0 \\ 1; & \text{if } C''(u,v)_t \bmod 2 = 1. \end{cases} \quad (3)$$

2.4. Embedding Protocol and Ciphering. With the purpose of enhancing the security of the embedded message and

warranting self-detection at the target destination, the proposal ciphers the hidden message prior to the steganography technique using the RC4 algorithm [16] and wraps it into a special designed protocol, which ensures self-detection at the end-peer. RC4, which was chosen due to its programming simplicity and performance [17], encrypts the message by using a private key. Thus, if the steganographic algorithm is broken, the enemy would have to know the secret key and cipher algorithm.

To sum up, in this section a novel and low-complexity steganographic algorithm for digital television was presented. The proposed scheme first decodes the TS from digital television, extracting H.264/AVC video sequences. Afterwards, these are decoded and searched for intrapredicted luma regions, where the secret and previously ciphered messages are hidden into the ICT high frequency residual coefficients using an interlaced embedding strategy and exploiting the properties of the CAVLC entropy encoder, depicted in the steganographic method. Finally, the resultant stegovideo sequences are repacked into the TS stream.

3. Experimental Results

A software simulation of the proposed steganography technique was implemented by mixing MATLAB 2010 b and Java development environments. The most important achievements of the program are the MPEG-2 Systems and H.264/AVC integration, a proprietary code that meets standards. In addition, a novel CAVLC entropy encoder scheme using a lookup-table strategy extracted from [18] is accomplished. This allowed improving the overall encoding and decoding speed for residual luminance coefficients. All experiments are conducted using a transport stream sample from a typical free-to-air television channel, from which three different cover video sequences from the daily program list were extracted. The selected video sequences differed in the changes within the scenes and were addressed as static, moderate, and highly variant.

Static video is characterized by slow and almost null motion in the scene, where the focus of the camera is commonly centered on capturing one object. The moderately variant video is characterized by some scene changes, and highly variant video is distinguished by the fast alternation of uncorrelated scenes. In order to prove the embedding capacity of each video sequence and the amount of distortion introduced, three different randomly selected and different-length secret messages were prepared. Simulation results were compared using two different quality measures. One of them was the objective quality measure known as Peak Signal to Noise Ratio (PSNR) [19] which is a widely adopted method used in engineering to measure the amount of distortion introduced by compression, comparing the original with the stegovideo frames in a pure mathematical way, and the other was the subjective perceptual criterion known as Subjective Difference Grade (SDG), based on ITU-R BS.1116 [20]. The latter was successfully implemented in [21] and is now applied to digital television.

Unlike PSNR, SDG considers the viewer's opinion by taking a survey. The SDG procedure works as follows: There are three different digital television sequences labeled as "A," "B," and "C." "A" is always the original sequence, while "B" and "C" are randomly scrambled and one of them contains the original and the other the stegosequence. The viewer is asked to watch "A" and informed that this is the original one and then "B" and "C" without telling them about the content of both sequences. Then, the viewer is requested to punctuate the distortion perceived in "B" in relation to "A" and "C" in relation to "A." The possible marks that can be chosen for this subjective test are detailed in Figure 3, where 5 is assigned when no difference is perceived and 1 when it is very annoying.

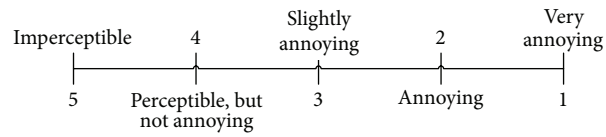


Figure 3: Subjective test scores.

After the survey, the SDG value is calculated as a special quality measure function. In this paper, the SDG value is obtained from the difference between the punctuation assigned to the stegofile and the original, as shown in

$$\mathrm{SDG} = \mathrm{Score}_{\mathrm{Stego}} - \mathrm{Score}_{\mathrm{Original}}. \quad (4)$$

If the SDG value becomes highly negative, it means that noticeable distortion has been introduced by the steganography technique. If it turns positive or close to zero, however, it can be inferred that perceptual degradation has not been perceived and subjective quality is better.

3.1. Simulation Conditions. The sequences used during the simulations had the following common properties: All are coded in H.264/AVC high profile, use the CAVLC entropy coder and a frame rate of 30 fps, and have a spatial resolution of 720 × 480 pixels. In addition, the quantization parameter of each macroblock is not fixed and varies adaptively within the different frames, as well as the scan order which could be interlaced or progressive. Furthermore, each test sequence lasts 15 seconds. The opinion survey consists of 27 different questions with a sample of 30 people aged between 20 and 30 years in a well-illuminated environment. These tests consolidate three different message lengths and three different steganography techniques. The steganographic methods are composed of [10], an earlier version of the proposed technique without considering the interlaced strategy explained in Figure 2 and with the main difference that the discrete index "t" had the range $t = 0, 1, \ldots, 15$ and the final proposal. Likewise, the method complexity of [10] and the proposal is depicted in Table 1. The message lengths are estimated as a percentage of the maximum embedding capacity of each video excerpt using the technique in [10].

3.2. Simulation Results. Figure 4 depicts the PSNR of frame 30 for the method proposed in [10], for the steganographic method without interlaced strategy, and for the final proposal, tested with three different messages lengths and three

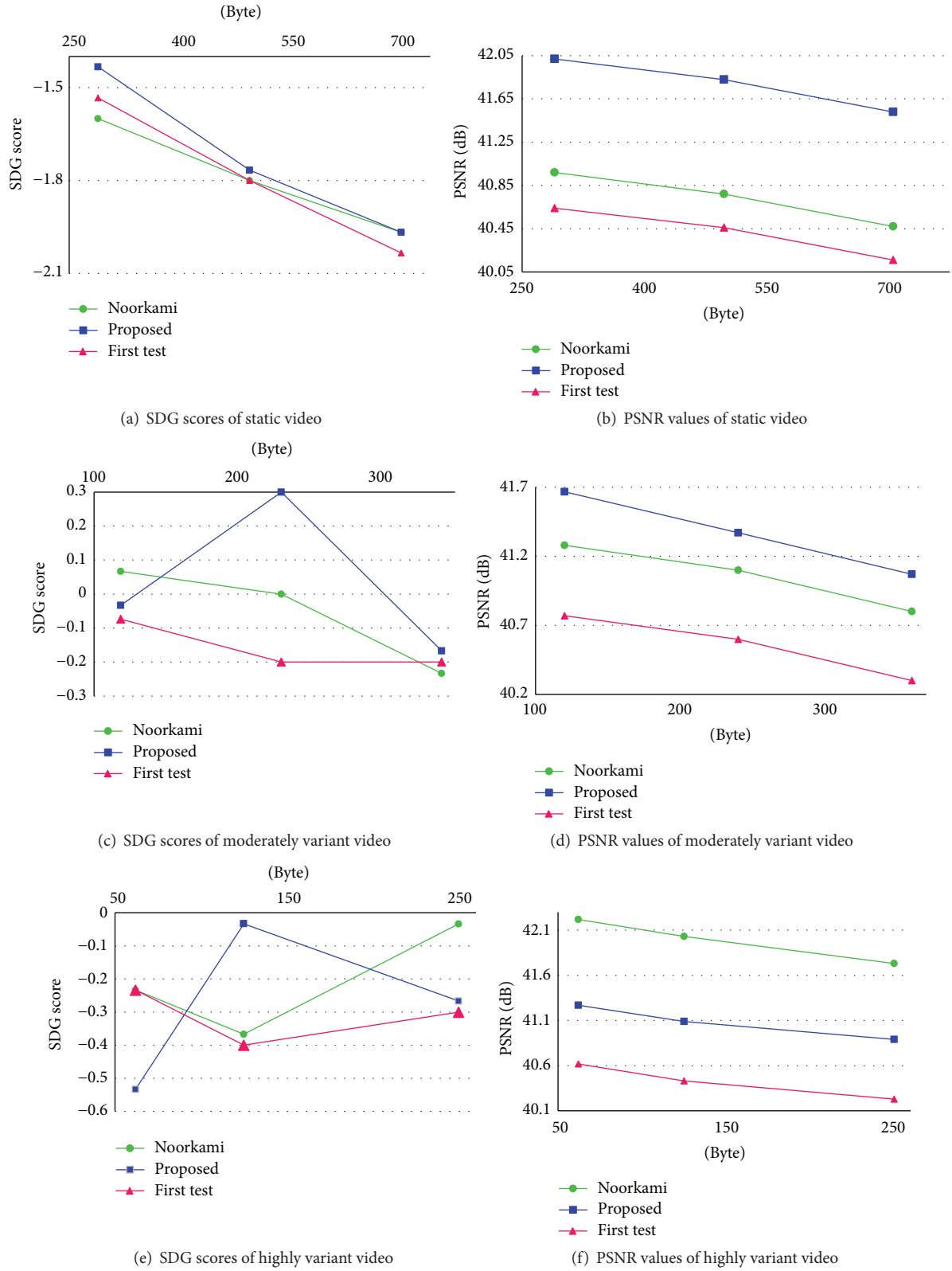


Figure 4: SDG scores and PSNR values achieved with the first test, proposed algorithm, and [10].

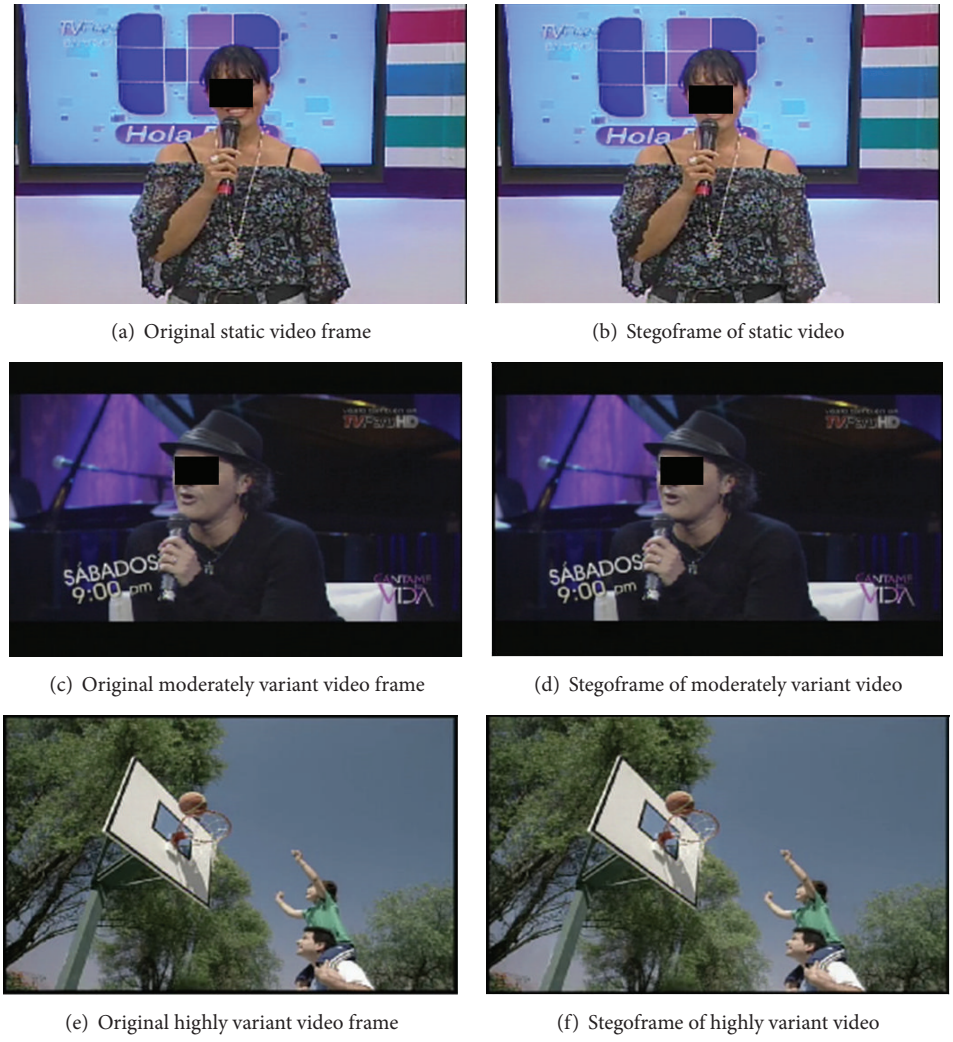
Table 1: Comparative table of the technique proposed and [10].

Technique	Hiding component	Applied to	Security	Computational complexity	Maximum embedding bits/Macroblock	Perceptual awareness	Key feature
Reference [10]	CAVLC code word	Intrapredicted I-frames (luminance samples)	Key-dependent strategy based on a public key extracted from the local macroblock features and a private key owned at the target destination	Low	One	No: the algorithm can change low and high frequency residual ICT quantized coefficients	Hidden data randomness due to a key and local macroblock derivatives dependent algorithm
Proposed	CAVLC code word	Intrapredicted I-frames (luminance samples)	The secret message is ciphered using a private key [16] prior to the embedding process and divided into byte units	Lower (security does not rely on the local macroblock features, which demands higher computational resources)	Four	Yes: the algorithm is designed to change only high frequency residual ICT quantized coefficients and in an interlaced way, in order to try to avoid perceptual degradation and error propagation.	Deep understanding of the coding properties of the CAVLC entropy encoder for bit rate control and rapid embedding algorithm purposes

different digital television sequences, respectively. The simulation results show that the PSNR values tend to decrease as the embedded message size increases. However, all the PSNR values are above 40 dB, which is an acceptable range for steganography techniques in the H.264/AVC. In addition, this denotes that the objective quality of the stegosequences is good and that few errors are introduced by the embedding techniques. The results also illustrate that better PSNR values are achieved by the technique proposed for moderately variant and static video, slightly outperforming both [10] and the technique without interlaced strategy. Figure 5 depicts frame 30 of the original video frame, the secret data, and the stegoframe for the different types of video.

Dissimilar results from the PSNR analysis are obtained with respect to the SDG values. These are shown in Figures 4(a), 4(c), and 4(e) and are tested under the same simulation conditions depicted in Figures 4(b), 4(d), and 4(f). First of all, the static sequence clearly shows that as the embedding data length increases, the SDG value rapidly decreases due to high light intensity and fewer camera movements, because the camera is focusing on the center of the scene where the presenter is talking. However, it is a fact that the human eye gets easily used to quasi-invariant scenes and smaller changes are quickly recognized. On the other hand, it is interesting to note that some highly and moderately variant excerpts got positive or near to zero SDG values during the survey. This can be only justified by the movement between the scenes, which becomes an important topic for the analysis, since changes mask the slight distortions introduced by the steganography technique and increase the complexity of the viewer's choice. For this reason, the PSNR is not sufficient criterion to decide if the designed steganography technique outperforms the other ones. For example, the static video has acceptable PSNR values, but it is the viewer's opinion that it is of bad quality. In this context, it should be pointed out that the steganography technique of the proposal slightly outperforms the rest of hiding methods in the SDG simulations. The technique proposed does not change the ICT coefficient randomly as in [10]. Furthermore, the free spaces left between embeddable macroblocks and the special strategy to select the embeddable blocks manage to reduce visible artifacts and improve the objective and subjective quality of the stegosequences on average. Finally, Table 2 shows the embedded bit rates reached by the proposal and by [10] for several video sequences from digital television, as well as the bit rate increase in percentage related to the original video excerpts.

It should be noted that the technique proposed reached an average embedded bit rate of approximately 425 bits/sec per secret communication channel, without increasing the original video bit rate, but slightly decreasing it instead, and so exemplifying the bit rate control of the proposal over the CAVLC encoder. Table 2 is relevant, as it describes the possible bandwidth limits that applications of steganography in SDTV will face.



(a) Original static video frame (b) Stegoframe of static video

(c) Original moderately variant video frame (d) Stegoframe of moderately variant video

(e) Original highly variant video frame (f) Stegoframe of highly variant video

Figure 5: Stegovideo frames excerpts after hiding a secret message (secret data of 80-byte length: "*the two companies are at the forefront of a tantalizing wireless communications concept that has proved hard to produce on a big scale: reduce cellphone costs by relying on strategically placed Wi-Fi routers. And when there are no routers available, fall back on the traditional cellular network*").

Table 2: Embedded bit rate in bits/sec for the technique proposed and that of [10].

Test sequence	Reference [10]		Proposed	
	Embedded bit rate in bits/sec	Bit rate increase in %	Embedded bit rate in bits/sec	Bit rate increase in %
Highly variant	402	0.33	400	−0.16
Moderately variant	544	0.51	464	−0.02
Static	384	0.79	416	>−0.01

4. Conclusion

In this paper, a novel, real-time, affordable, and compressed domain steganography technique for SDBTV digital television sequences is discussed. The secret message is hidden in the high frequency luminance ICT coefficients of intrapredicted 4 × 4 macroblocks using an interlaced embedding strategy. Furthermore, self-detection at the target destination and enhanced security features are achieved by applying a special embedding protocol and ciphering the secret data prior to the steganographic process.

Simulation results show that the technique proposed maintains a good subjective quality of the stegosequence and that the PSNR analysis is not sufficient criterion to assure that the perceptual quality will not be degraded during the steganographic process. It is very important to take into account the viewer's real perception. This was proved by the different results achieved between the SDG and PSNR measure. Finally, it is worth mentioning that a special care should be provided to static sequences, where slight changes may cause annoying visual artifacts.

A first steganography technique designed for digital television is here presented. In future works, the scheme proposed will be based on intrapredicted 8 × 8 macroblocks

with an adaptive brightness algorithm to reduce the embedding capacity in static sequences and thus preserve subjective quality. In addition, new standardized algorithms for an objective quality measure are under investigation.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

The authors would like to thank the Peruvian Institute of Radio and Television (IRTP) for providing the digital television sequences that the work was based on.

References

[1] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermaking and Steganography*, Morgan Kauffmann, 2008.

[2] ITU-T, "Video codec for audiovisual services at p × 64 kbit/s," Recommendation H.261, ITU-T, 1993.

[3] ISO/IEC 13818-2 and ITU-T Rec. H.262.0, "Information technology—generic coding of moving pictures and associated audio information: video," ISO/IEC JTC 1 and ITU-T, 1995.

[4] ISO/IEC and ITU- T, "Advanced video coding for generic audio-visual services," ISO/IEC 14496-10 and ITU- T Recommendation H.264, ISO/IEC JTC 1, ITU-T, 2010.

[5] G. J. Sullivan, J.-R. Ohm, W.-J. Han, and T. Wiegand, "Overview of the high efficiency video coding (HEVC) standard," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, no. 12, pp. 1649–1668, 2012.

[6] G. Nehru and P. Dhar, "A detailed look of audio steganography techniques using LSB and genetic algorithm approach," *International Journal of Computer Science Issues*, vol. 9, pp. 402–406, 2012.

[7] K.-C. Chang, C.-P. Chang, P. S. Huang, and T.-M. Tu, "A novel image steganographic method using tri-way pixel-value differencing," *Journal of Multimedia*, vol. 3, no. 2, pp. 37–44, 2008.

[8] Y.-F. Sun, D.-M. Niu, G.-M. Tang, and Z.-Z. Gao, "Optimized LSB matching steganography based on Fisher information," *Journal of Multimedia*, vol. 7, no. 4, pp. 295–302, 2012.

[9] B. Mobasseri and Y. N. Raikar, "Authentication of H.264 streams by direct watermarking of CAVLC blocks," in *Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505 of *Proceedings of SPIE*, The International Society for Optical Engineering, San Jose, Calif, USA, January 2007.

[10] M. Noorkami and R. M. Mersereau, "Compressed-domain video watermarking for H. 264," in *Proceedings of the IEEE International Conference on Image Processing (ICIP '05)*, vol. 2, pp. 890–893, Genova, Italy, September 2005.

[11] M. Noorkami and R. M. Mersereau, "A framework for robust watermarking of H.264-encoded video with controllable detection performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 1, pp. 14–23, 2007.

[12] A. B. Watson, "DCT quantization matrices visually optimized for individual images," in *Human Vision, Visual Processing, and Digital Display IV*, vol. 1913 of *Proceedings of SPIE*, pp. 202–216, San Jose, Calif, USA, September 1993.

[13] ISO/IEC and ITU-T, "Information technology—generic coding of moving pictures and associated audio information: systems," ISO/IEC 13818-1 and ITU-T Recommendation H.222.0, ISO/IEC JCT 1, ITU-T, 2006.

[14] J. Arnold, M. Frater, and M. Pickeking, *Digital Television Technology and Standards*, John Wiley & Sons, 2007.

[15] I. E. Richardson, *H.264 and MPEG-4 Video Compression: Video Coding for Next-Generation Multimedia*, John Wiley & Sons, New York, NY, USA, 2003.

[16] W. Stallings, *The RC04 Stream Encryption Algorithm*, 2005, http://cse.spsu.edu/afaruque/it6833/RC4.pdf.

[17] S. O. Sharif and S. P. Mansoor, "Performance analysis of stream and block cipher algorithms," in *Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10)*, pp. V1522–V1525, Chengdu, China, August 2010.

[18] Y. Yi and B. C. Song, "High-speed CAVLC encoder for 1080p 60-Hz H.264 codec," *IEEE Signal Processing Letters*, vol. 15, pp. 891–894, 2008.

[19] S. Winkler and P. Mohandas, "The evolution of video quality measurement: from PSNR to hybrid metrics," *IEEE Transactions on Broadcasting*, vol. 54, no. 3, pp. 660–668, 2008.

[20] ITU-R, "Methods for the subjective assessment of small impairments in audio systems including multichannel sound systems," ITU-R Rec. BS.1116-1, 1997.

[21] G. Kemper and Y. Iano, "An audio compression method based on wavelets subband coding," *IEEE Latin America Transactions*, vol. 9, no. 5, pp. 610–621, 2011.