Multimedia Systems 9: 217–227 (2003)
Digital Object Identifier (DOI) 10.1007/s00530-003-0093-4

Multimedia Systems

Encryption and watermarking for the secure distribution of copyrighted MPEG video on DVD ⋆

Dimitrios Simitopoulos[1,2], **Nikolaos Zissis**[3], **Panagiotis Georgiadis**[2], **Vasileios Emmanouilidis**[1], **Michael G. Strintzis**[1,2]

[1] Informatics and Telematics Institute, 1st Km Thermi-Panorama Road, 57001 (PO Box 361), Thermi-Thessaloniki, Greece
[2] Electrical and Computer Engineering Department, Aristotle University Thessaloniki, 54124, Thessaloniki, Greece
[3] MLS Laserlock Int. Inc., 79, 17 Noemvriou St., 54352, Thessaloniki, Greece

Abstract. This paper presents a complete system for the secure distribution of a copyrighted MPEG-1/2 video stored on a DVD-ROM disc. A combined selective watermarking and encryption method that operates in the compressed MPEG domain is introduced. Watermarking resistant to a number of attacks is used for copyright protection. The video quality deteriorates significantly due to encryption, thus restraining unauthorized viewers from viewing it. The video can only be viewed using the developed Secure MPEG Player, which performs real-time decryption of the encrypted video. The decryption requires a secret key that is extracted from the DVD-ROM disc in a cryptographically secure manner.

Key words: Encryption – DVD copy protection – Watermarking – Copyright protection

1 Introduction

The recent progress in computer technologies has made the distribution and usage of multimedia data through DVD or the Internet popular and commercially attractive, even to home users. However, these advances in technology must inevitably be accompanied by techniques that will guarantee the secure delivery of multimedia content and also the protection of the intellectual property rights (IPR) of its creator/owner. Unfortunately, in the case of digital video, the MPEG standard [9] has no inherent security and copyright protection mechanisms. Thus providing an external mechanism for enhancing MPEG video with security attributes has become a field of extensive study, and many suggestions have been made.

In order to resolve the copyright protection issue, numerous watermarking techniques have been proposed. However, very few of them deal with the very important issue of compressed domain watermarking for video [4,6,8,12,15]. In [8], the authors proposed a technique that partially decompresses the MPEG stream, watermarks the resulting discrete cosine transform (DCT) coefficients, and reencodes them into a new compressed bitstream. However, the detection is performed in the spatial domain, requiring full decompression. Chung et al. [4] applied a DCT domain embedding technique that also incorporates a block classification algorithm to select the coefficients to be watermarked. In [11], a faster approach is proposed that embeds the watermark in the domain of quantized DCT coefficients but uses no perceptual models so as to ensure the imperceptibility of the watermark.

In parallel with the development of watermarking techniques for copyright protection, various encryption schemes have been proposed to prevent unauthorized copying or viewing of MPEG video. Encryption of the entire video stream generally does not allow real-time viewing, and for this reason partial encryption was adopted in most solutions [1–3,13, 20,22,25]. In [2], the authors also presented a secure way for delivering the decryption key to the authorized users in the case of networked distribution of video.

As can be seen from the above, encryption and watermarking techniques have been developed independently. The two techniques have been combined in [25] for the secure delivery of copyrighted video through a network. However, the use of such a unified scheme that applies watermarking for copyright protection and encryption for copy protection of MPEG-coded multimedia material stored on a DVD-ROM disc has not been addressed in the literature.

In this paper, a fast compressed domain watermarking technique is combined with a partial encryption technique in one application. In order to reach a satisfactory compromise between robustness and imperceptibility of the embedded watermark, perceptual analysis [24] and block classification techniques [18,4] operating in the DCT domain are combined for the selection of the coefficients to be watermarked and of the strength of the watermark for each I-frame of the video sequence. The proposed method first watermarks the selected I-frame data and then encrypts them using the IDEA [19] encryption algorithm. In the presented scenario, the resulting partially watermarked and encrypted MPEG files are stored on a DVD-ROM disc. For viewing these files, the Secure MPEG Player (SMP) was developed. The SMP operates on a Microsoft Windows-based PC using the DirectX platform. The SMP performs real-time decryption of the MPEG video using a decryption key that is securely extracted from the DVD itself,

⋆ This work was supported by the EU IST Project "ASPIS".
Correspondence to: M. G. Strintzis
(e-mail: strintzi@vergina.eng.auth.gr)

employing a novel technique. The decryption key is hidden in a specially manufactured area of the DVD-ROM disc so that it cannot be copied. In this way, copy protection is achieved. In addition, even if a pirated copy of unencrypted but watermarked video becomes available to a pirate, the copyright ownership can be proven by detecting the embedded watermark, which was found to be robust to many types of attacks.

The paper is organized as follows. In Sect. 2, the combined selective watermarking and encryption method is analyzed. Sect. 3 describes the structure and the operation of the SMP. The secure handling of the decryption key in DVD-ROM media is presented in Sect. 4. In Sect. 5, the watermark detection process is described. In Sect. 6, the results of the experimental evaluation are presented. Finally, conclusions are drawn in Sect. 7.

2 Watermarking and encryption

The proposed system performs watermark embedding and encryption. These operations are applied to the I-frame data and performed in the compressed domain. This choice offers a number of advantages. First, it is very often impractical (due to high storage capacity requirements) or indeed entirely not feasible to decompress and then recompress the entire video stream. In addition, decoding and reencoding an MPEG stream would also significantly increase the processing time. Furthermore, I-frame encryption is fast and creates MPEG videos having significant quality loss so that they are useless to anyone who does not have the decryption key. Additionally, in order to play back the encrypted MPEG video, the decryption of only the I-frames is needed, which does not hinder the real-time performance of the video player. Finally, as will be analyzed in Sect. 5, embedding the watermark only to the I-frames of a video results in watermarking nearly all its frames because the watermark is transferred from intraframes to interframes during decoding.

In the following, first the methodology for processing MPEG multiplexed streams for watermarking and encryption is analyzed, and then the watermarking process and the encryption process are described.

2.1 Processing of MPEG multiplexed streams

MPEG multiplexed streams contain at least two elementary streams i.e., an audio and a video elementary stream. An obvious approach for processing MPEG multiplexed streams would be to de-multiplex the stream, then watermark and encrypt the video data and finally multiplex the two elementary streams. The above process however is extremely costly computationally.

In order to achieve lower complexity, a technique was developed that does not fully demultiplex the stream before the watermark embedding and the encryption but instead deals with the multiplexed stream itself. Specifically, first the video elementary stream packets are detected in the multiplexed stream. For the video packets that contain I-frame data, the encoded video data are extracted from the video packets and variable length decoding is performed in order to obtain the quantized DCT coefficients. The headers of these packets are left intact. This procedure is schematically described in Fig. 1. The quantized DCT coefficients are first watermarked. The watermarked coefficients are then variable length coded and encryption is performed. The encrypted video data are partitioned so that they can fit into video packets that use the original headers. Audio packets and packets containing interframe data are not altered. Basically, the stream structure remains unaffected and only the video packets that contain coded I-frame data are altered.

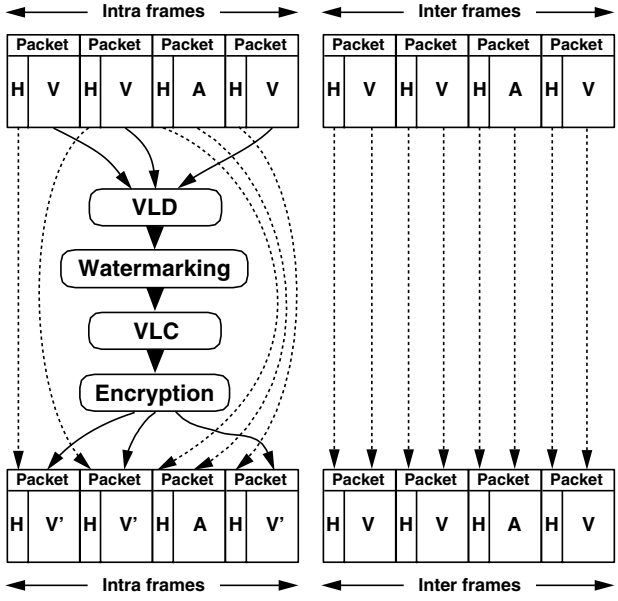


Fig. 1. Operations of the proposed watermark embedding and encryption scheme performed on an MPEG multiplexed stream (V: encoded video data, A: encoded audio data, H: elementary stream packet header, Packet: elementary stream packet, V′: watermarked and encrypted video data, VLC: variable length coding, VLD: variable length decoding)

2.2 Imperceptible watermark embedding in the quantized DCT domain

The values of the embedding watermark sequence W are either -1 or 1. This sequence is produced from an integer random number generator by setting the watermark coefficient to -1 when the generator output is a negative number and to 1 when the generator output is positive. The result is a zero mean, unit variance process. The random number generator is seeded with the result of a hash function. The MD5 algorithm [19] is used to produce a 128-bit integer seed from a meaningful message (owner ID). The watermark is generated in such a way because, as explained in [26], even if an attacker finds a watermark sequence that leads to a high correlator output, he cannot find a meaningful owner ID that would produce the watermark sequence through this procedure and therefore cannot claim to be the owner of an image/video frame. This is ensured by the use of the hashing function included in the watermark generation.

The proposed watermark embedding method (see Fig. 2) alters only the quantized AC coefficients $X_{\kappa,\lambda}(m,n)$ (where

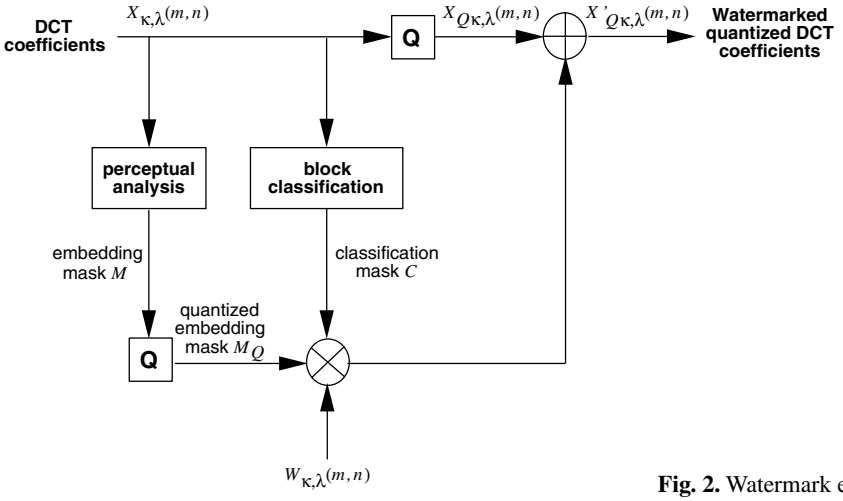


Fig. 2. Watermark embedding scheme

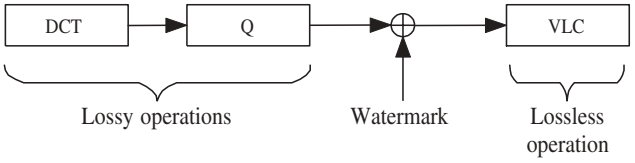


Fig. 3. MPEG encoding operations

κ is the index of the current macroblock, λ is the index of the block within the current macroblock, and m, n are indices indicating the position of the current coefficient in an 8×8 DCT block) of luminance blocks of I-frames and leaves the chrominance blocks unaffected. In order to make the watermark as imperceptible as possible, perceptual analysis [24] and block classification techniques [4] are combined as in [21]. These are applied in the DCT domain in order to select the coefficients that are the most suitable for watermarking. For each selected coefficient in the DCT domain, the product of the embedding watermark coefficient $W_{\kappa,\lambda}(m,n)$ with the corresponding parameters that result from the perceptual analysis (embedding mask $M_{\kappa,\lambda}(m,n)$) and block classification (classification mask $C_{\kappa,\lambda}(m,n)$) is added to the corresponding quantized coefficient:

$$X'_{Q\kappa,\lambda}(m,n) = X_{Q\kappa,\lambda}(m,n) + C_{\kappa,\lambda}(m,n) M_{Q\kappa,\lambda}(m,n) W_{\kappa,\lambda}(m,n) \quad (1)$$

where $M_{Q\kappa,\lambda}(m,n)$ is the quantized value of $M_{\kappa,\lambda}(m,n)$.

It should be noted that if the watermark were embedded in the DCT coefficients, the quantization process could alter it or even possibly eliminate it entirely. Clearly, this would make the detection process unreliable. Thus, in order to avoid reduced detection performance due to MPEG quantization, the watermark is embedded in the quantized DCT coefficients, since the MPEG coding algorithm performs no other lossy operation after quantization. Therefore, any information embedded as in Fig. 3 does not run the risk of being eliminated by the subsequent processing, and the watermark exists intact in the quantized coefficients when detection is performed.

In order to evaluate the imperceptibility of the watermark embedding method, various videos were watermarked and viewed. The viewers were unable to locate any degradation in the quality of the original videos. Table 1 presents the mean of the PSNR values of all the frames of some commonly used video sequences, which were watermarked as described above. In addition, Table 1 shows the mean of the PSNR values of the I-frames (watermarked frames) of each video sequence.

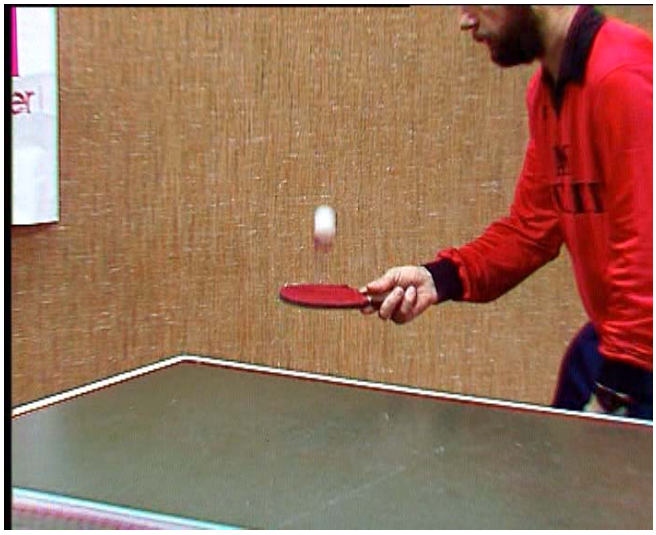
Table 1. Mean PSNR values for the frames of 4 watermarked video sequences (MPEG-2, 6 Mbit/s, PAL)

Video sequence	Mean PSNR for all video frames	Mean PSNR for I-frames only
Flowers	38.6 dB	36.5 dB
Mobile and calendar	33.1 dB	30 dB
Susie	45.6 dB	40.4 dB
Table tennis	35.6 dB	33.2 dB

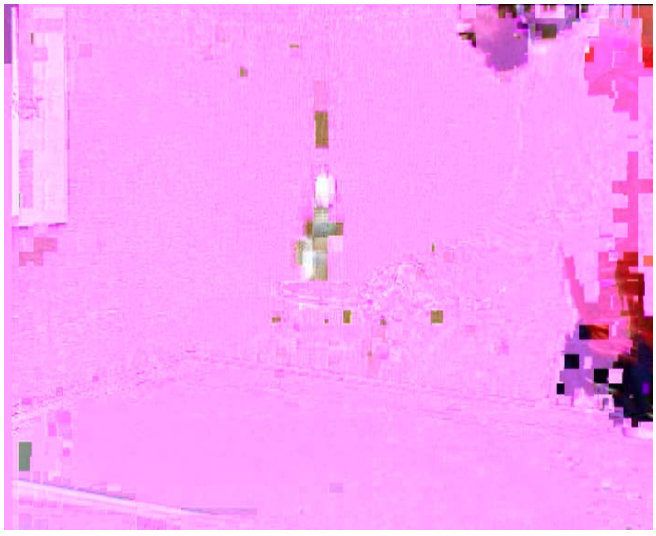
2.3 Encryption

In order to prevent unauthorized viewing of the watermarked video stream, partial encryption is employed. As will be explained in the following, if an illegal copy of the encrypted video stream is obtained (we assume that the decryption key is not available), only a highly distorted version of the original video can be seen.

The proposed encryption scheme encrypts only the I-frames, as was hyphenation also proposed by other researchers [13,22], in order to save encryption and decryption time. Figure 4 presents a typical decoded frame from the original and the encrypted *Table Tennis* video sequence. Due to the MPEG coding structure, distorting the intraframes i.e., encrypting the I-frames, leads at the same time to reproducing distorted P- and B-frames. However, the MPEG encoders sometimes produce P- or B-frame macroblocks that are intracoded. These macroblocks will not be encrypted, hence they will be correctly decoded even if the I-frame of the same group of pictures (GOPs) is encrypted. In such a case, the corresponding decoded macroblocks of the P- or B-frames will not be distorted, leading to video frames with visible parts even without



a



b

Fig. 4a,b. A typical decoded frame from the MPEG-2 *table tennis*. **a** Original video sequence. **b** Encrypted video sequence

carrying out decryption. For some applications, such as confidential video conferencing [1] or military applications, this security level may be insufficient. However, the use of the proposed method for encrypting a video clip or a movie leads to videos that, when viewed without decryption, have unacceptable quality. Since our aim is preventing unauthorized viewing of this type of videos, the I-frame encryption is a good compromise between security and speed.

The encryption scheme uses the IDEA encryption algorithm [19]. The IDEA is a symmetric algorithm that offers a very good level of security and a decryption speed that is affordable in real-time applications such as a video player. In our implementation, one 128-bit encryption key is used for the encryption of all I-frames. This key, which is also the decryption key, is hidden in specially manufactured DVD-ROM discs and is extracted, as will be described in Sect. 4.

3 Secure MPEG player

In order to allow authorized users to view the encrypted video files, we implemented a software application with video and audio playback capabilities, the Secure MPEG Player (SMP). The SMP is stored in the DVD-ROM disc together with the encrypted video files. The SMP runs on computers using the Microsoft Windows operating platform, which currently appears to be the most favorite platform for multimedia applications.

The SMP facilitates all the functions that current commercial video players offer such as play, stop, pause, seek, zoom, and full-screen and volume-control capabilities. Its main feature is that it can play back multiplexed MPEG-1/2 streams that contain an encrypted (using the technique described in Sect. 2.3) video stream, provided that the proper decryption key is available.

The SMP is based on the DirectX technology. Specifically, it uses DirectShow [14], a subset of the DirectX programming interface, which provides the infrastructure for programming applications with media-streaming functionality. The structure of the SMP is shown in Fig. 5. Each one of the boxes depicted in Fig. 5 represents a DirectShow filter. The gray box is the video decryption filter, which performs two operations:

- Extraction of the I-frame encrypted data from the elementary video stream obtained from the MPEG demultiplexer filter.
- Decryption of the I-frame encrypted data using the IDEA algorithm.

Naturally, the implementation of the video decryption filter allows the real-time performance of the SMP.

4 Secure handling of the decryption key in DVD-ROM media

4.1 The secure decryption key extraction concept

In the approach chosen, the decryption key is extracted from the DVD-ROM disc in a secure way using a commercially available software protection system for optical discs [10]. The protection system is based on a specially manufactured optical disc (DVD-ROM) that contains an authentication signature. This is a unique feature of custom format that is produced on the DVD-ROM stamper with the use of mastering equipment. The authentication signature is produced with a special technology that has been used commercially since 1996; it was initially used for CD-ROM discs, and recently, for the purpose of this research, it was expanded to DVD-ROM discs. The key feature of the authentication signature is that it cannot be copied by any DVD-WR recording equipment, whether commercial or industrial. The authentication signature is checked by the protection software for verification of the authenticity of the optical disc. The authentication signature also contains specific areas of standard DVD-ROM format [23] that contain the value of the decryption key. Any attempt to copy a DVD-ROM disc that contains this authentication signature results in complete failure of the copying process. Alternatively, any attempt to skip the signature copying will result in the formation of an illegal copy that will not be verified as authentic. In addition, this copy will not contain the decryption key needed

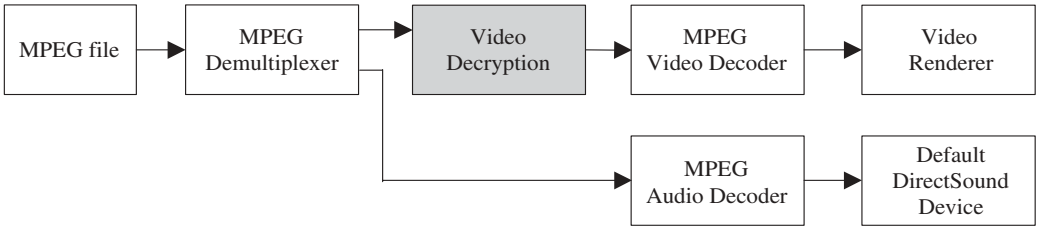


Fig. 5. Secure MPEG Player structure

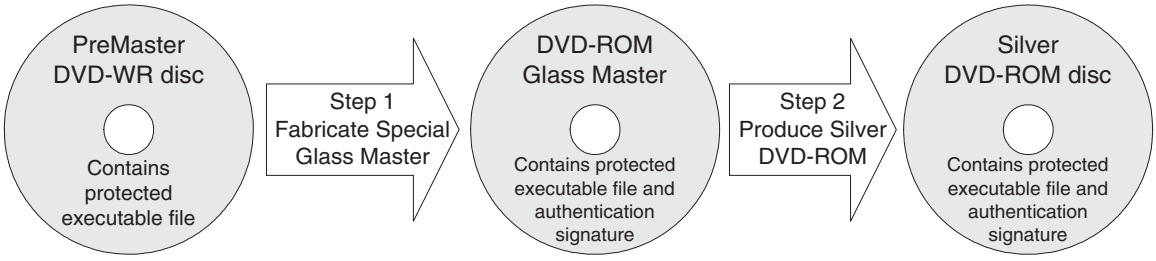


Fig. 6. Authentication signature fabrication steps

for decrypting the encrypted video. On the contrary, if the authentication signature verification is successful, the decryption key is extracted from the disc and the video can be decrypted.

Therefore, based on the copy prevention features of the authentication signature, it is ensured that the decryption key is stored in a safe place. In addition, the SMP executable file is protected so that it is not possible for pirates to obtain the decryption key after it is extracted from the disc.

4.2 The authentication signature

The authentication signature is produced using a special process of DVD-ROM Glass Master fabrication as seen in Fig. 6. The fabrication of the authentication signature is completed in two general steps. It begins with the processing of an optical disc called PreMaster DVD-WR disc. This disc contains the protected SMP executable file and the encrypted video files. The file layout is arranged so that the required disc space for the authentication signature is not used. The PreMaster DVD-WR disc is produced with the use of standard DVD recording equipment.

During the first step, a special process is used for the fabrication of the Glass Master. This process places the authentication signature inside the DVD-ROM Glass Master at a predefined position (i.e., specific absolute sectors) within the user data area. The authentication signature can only be created during a glass mastering process. Its security is due to the fact that it cannot be copied by any DVD recording system. The main reason for this is that the custom format chosen violates the DVD-ROM standard [23] and is not acceptable by DVD-ROM drives when any attempt is made to copy the authentication signature. In such a case, the PC system either halts or crashes and eventually quits. Thus no copy can be created.

The Glass Master is used for creating the Production Stamper hyphenation [17]. The Production Stamper is used for the production of the silver DVDs at the pressing factory. This is the second step of the process where the final DVDs containing the protected SMP executable and the authentication signature are produced.

As mentioned above, a glass mastering process is required for the creation of the authentication signature. This is impossible to do with any DVD recording software system because all such systems are manufactured to produce DVD-WR discs in the standard format so that they are readable by all DVD-ROM drives. In practice, if it were possible to produce a signature with a DVD-WR writer drive, this would mean that this drive would have implemented into its hardware nonstandard DVD-ROM formats. But there is no DVD-WR drive available worldwide with such features. On the other hand, only during the glass mastering process is it possible with the use of the CAD (computer-aided design)/CAM (computer-aided manufacturing) software to manufacture the signature.

Furthermore, the authentication signature consists of areas of custom format that cannot be read and areas of standard format that can be read and contain the video decryption key. The decryption key is protected by adjacent custom format areas (unreadable sectors) of the authentication signature. The custom format areas simply prevent copying because they cannot be read when copying with a DVD-WR recording system. However, when the protected SMP executable reads the signature, it reads specific areas of standard format using direct access mode, in contrast to the serial access mode used during a copying process.

4.3 Protection for the SMP executable file

It was found essential that the SMP executable be protected in order to achieve the highest possible level of security. If the SMP file is unprotected and receives the decryption key from an external DLL (dynamic link library), then a pirate could monitor the way the executable handles this value and

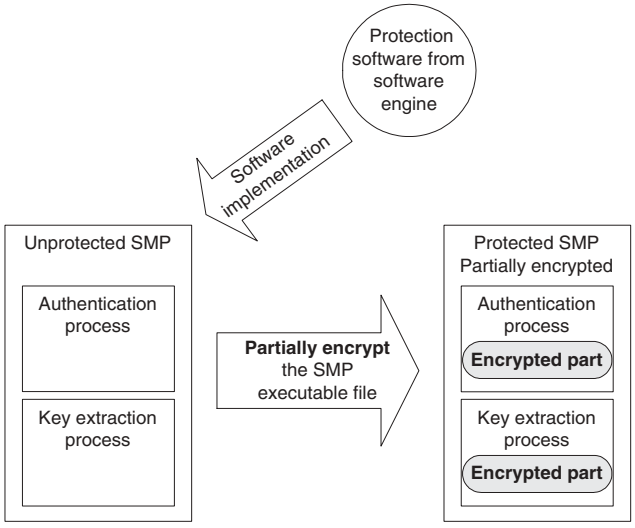


Fig. 7. Creation of the protected SMP executable file

possibly capture this value using a debugger. The protection of the SMP executable involves: (a) the implementation of protection software into its source code and (b) the partial encryption of the executable format, as seen in Fig. 7.

First, the protection software is generated in a software engine. The protection software, which contains the authentication and key extraction processes, is implemented into the SMP file. The operation of these processes will be explained in the following subsection. Then the SMP file is partially encrypted. In this way, both the authentication process and the key extraction process of the executable are found partially encrypted after the process is complete. The aim is not to allow any attempt to "read" the SMP executable file in low-level machine code format and possibly find the position inside the file format where the decryption key is used. In addition, due to partial encryption, it is not possible for a hacker to disassemble the executable using disassembler tools that reverse-engineer the executable in Assembly source code, thus allowing someone to "read" the source code and remove the protection system from the executable. The above attacks, in connection with the use of a debugger system, could allow a reverse engineering of the code and capture of the video decryption key value. However, the use of a debugger is prevented by the debug prevention system used by the protection system [10]. This protection method is a new version of an already commercially available protection system under the trademark Laserlock for CD-ROM discs. More than 30,000,000 CDs worldwide are protected with this system, and, due to its nature, there is no "generic crack" for this system available on Internet hacker sites.

The software protection system contains a special decryption algorithm that uses a set of keys in order to decrypt on the fly the encrypted parts of the authentication process and the key extraction process. This is a custom-made algorithm aligned for 32-bit processors optimized for the highest execution speed. This algorithm initially extracts the decryption keys from predefined readable areas inside the authentication signature [10]. These keys can be derived only from the original DVD-ROM discs that contain the authentication signature. Furthermore, the extraction of these keys is guarded by the debug prevention system, so that it is not possible for the hacker to attack this process and capture these values using a debugger.

4.4 Operation of the protected SMP executable

The operation of the protected SMP executable is shown in Fig. 8. Upon execution the protected SMP executable initializes the protection system that verifies the authenticity of the DVD-ROM disc. In order to do this, initially only the authentication process section of the SMP file is decrypted on the fly in the computer RAM memory and transformed back to the standard executable format that can be executed.

In the authentication process, first the debug prevention system checks whether any debugger system is active. If an active debugger is detected, the SMP execution terminates. This is necessary in order to avoid the reverse engineering of the protected application when executed through a debugger system, which is a standard tool used by all hackers. The debug prevention system is always active and looks for the presence of a debugger in the system. Thus, it is active for all the time that the executable runs. At any time that a debugger is activated, the application terminates. The debug prevention system was developed after careful and detailed study of the characteristics of a large number of available system debuggers. If no debugger is active, then the system verifies the authenticity of the authentication signature. If the DVD-ROM disc is found to be authentic, then the SMP execution continues. Alternatively, if the DVD-ROM disc is found to be an illegal copy of a protected DVD, then the SMP execution terminates.

Upon successful authentication signature verification, the rest of the SMP file that includes the key extraction process decrypts itself on the fly. Then the system searches for the decryption key that is hidden inside the authentication signature and provides it to the protected application. The key is extracted by reading at a predefined sector within the authentication signature, and then the SMP proceeds with its standard operation described in Sect. 3.

4.5 Assessment of the security level

The proposed system is based on both hardware and software components. The software component consists of the encryption algorithm, the debug prevention system, and the authentication process. The hardware component consists of the authentication signature that is a custom (nonstandard) format of the DVD-ROM. Thus, the security of the system is based primarily on the following:

- The DVD signature cannot be copied by any DVD-WR recording system presently available. This is due to the inherent characteristic of all DVD-ROM drives that they must read only the standard DVD-ROM format and regard a DVD-ROM disc as corrupt if it contains any other format. The key is extracted from readable areas of the authentication signature. The key will never be extracted from a copy that has skipped the authentication signature.

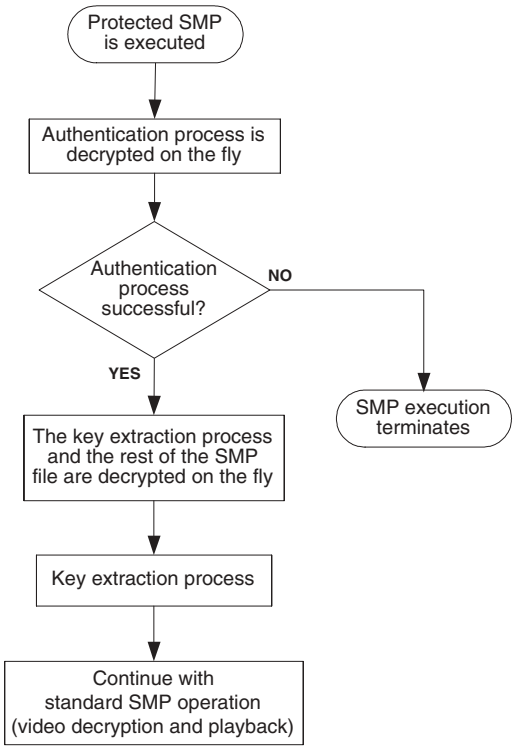


Fig. 8. Operation steps of the protected SMP executable

- The debug prevention system searches for the presence of a system debugger. This constantly monitors the operating system activity to verify any known activities related to the use of a debugger. The detailed study of debugger systems has led to the development of software modules that anticipate such system activity.
- The high level of security provided by IDEA even against brute force attacks or cryptanalysis attacks makes it immune to attacks from a hacker. Such an attack should combine ingenious software debugging tricks with exceptional cryptanalysis techniques. This is an extremely tedious process to be carried out at the low-level environment of a debugger system.

In conclusion, the present system would require not only the attack on an advanced encryption algorithm like IDEA but in addition the violation of a debug prevention system along with the copying of an authentication signature. The protection is based on the combination of the security features offered by both software and hardware components of the chosen protection system.

5 Watermark detection

The proposed scheme offers two levels of security for the protection of the video content. A first level of security is provided by the encryption of the video content combined with the decryption key extraction mechanism. Watermarking provides a second level of security. Watermarking is used for copyright protection so that even if a pirated copy of unencrypted but watermarked video becomes available to a pirate, the copyright ownership can be proven by detecting the embedded watermark. The detection of the watermark is performed *without* using the original data. The original meaningful message that produces the watermark sequence W is needed in order to check if the specific watermark sequence exists in a copy of the watermarked video. Then a correlation-based detection approach, similar to that analyzed in [26], is taken.

Variable length decoding is first performed to obtain the quantized DCT coefficients. Then inverse quantization provides the DCT coefficients for each block. The block classification and perceptual analysis procedures are performed as in the embedding procedure in order to define the set $\{X\}$ of the N coefficients that are expected to be watermarked with the sequence W. Finally, each coefficient in the set $\{X\}$ is multiplied with the corresponding watermark coefficient $W_{\kappa,\lambda}(m,n)$, producing the data set $\{X_W\}$. The correlation metric c for each frame is calculated as

$$c = \frac{mean \cdot \sqrt{N}}{\sqrt{variance}} \tag{2}$$

where

$$mean = \frac{1}{N}\sum_{l=0}^{N-1} X_W(l) \tag{3}$$

is the sample mean of $\{X_W\}$, and

$$variance = \frac{1}{N}\sum_{l=0}^{N-1} (X_W(l) - mean)^2 \tag{4}$$

is the sample variance of $\{X_W\}$.

The correlation metric c is compared to the threshold T_c. If the correlation metric exceeds the threshold, the examined frame is considered watermarked with the specific owner's watermark and the copyright ownership can be proven.

The threshold T_c is defined according to the allowed false-alarm probability P_{FA} of the detection scheme. The scheme aims to minimize the probability of false negative errors (failure to detect the watermark, although it is embedded) while keeping false alarms at an acceptable rate (Neyman-Pearson criterion). In order to calculate the threshold based on a fixed false-alarm probability, the statistical properties of the correlation metric are needed. As argued in [26], if the number N is large enough, the central limit theorem [16] is applicable, and hence when the video frame is not watermarked, the correlation metric c given in Eq. 2 will follow a Gaussian distribution $N(m,\sigma) = N(0,1)$. Therefore, given a fixed false-alarm probability P_{FA}, the threshold is calculated as follows:

$$P_{FA} = Q\left(\frac{T_c - m}{\sigma}\right) = Q(T_c) \Rightarrow T_c = Q^{-1}(P_{FA}) \tag{5}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt$.

5.1 Detector implementation

The proposed correlation-based DCT domain detection described above can be implemented using two types of detectors.

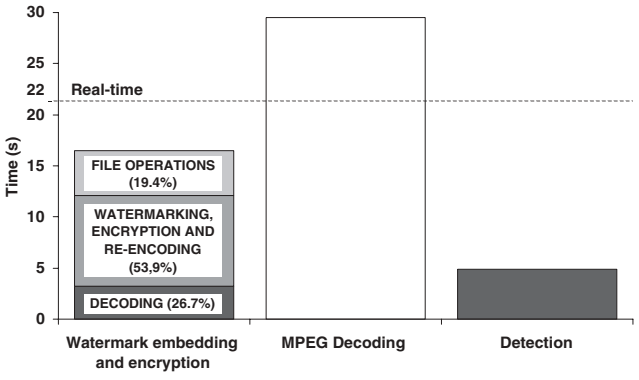


Fig. 9. Speed performance of the watermark embedding and encryption scheme, and the detection scheme

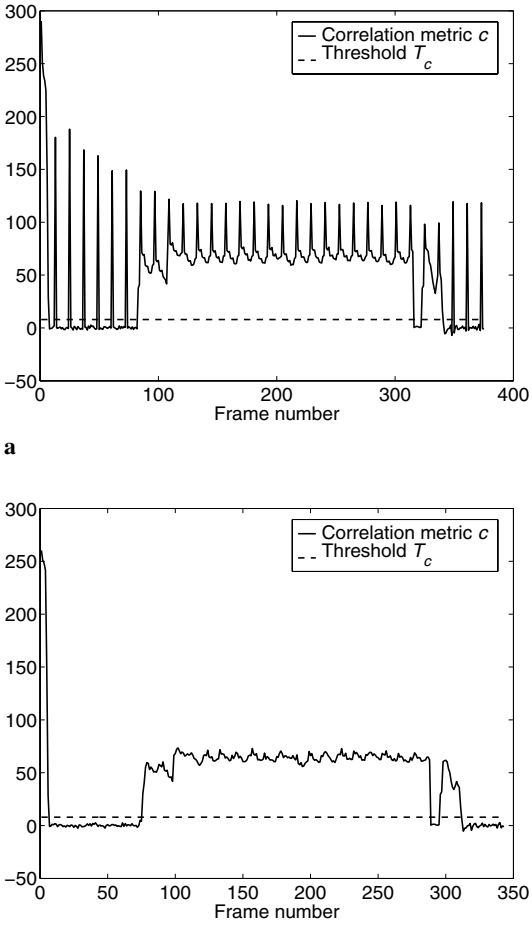


Fig. 10. a Correlation metric plot for the 375 frames of the 8 Mbit/s MPEG-2 video *Table Tennis*. **b** Correlation metric plot for the same video sequence with the I-frames skipped (this video sequence contains all but the frames that were encoded as I-frames before the skipping was performed)

The first detector (*detector-A*) assumes that the sequence under examination is the original watermarked sequence or has the same GOP structure with the original watermarked sequence but is encoded at a different bit-rate using one of the techniques proposed in [7]. Therefore, this detector simply detects the watermark only in I-frames during their decoding by applying the procedure described in Sect. 5. The detection is very fast, and it introduces negligible additional computational load to the decoding operation.

The second detector (*detector-B*) assumes that the GOP structure may have changed during transcoding, e.g., frames that were previously coded as I-frames may now be coded as B- or P-frames. This detector decodes each frame and then detects the watermark in the DCT domain using the technique described in the first part of Sect. 5. The decoding operation performed by this detector may also consist of the decoding of non-MPEG compressed or uncompressed video streams.

It should be noted that in the case where transcoding and I-frame skipping are performed on an MPEG video sequence, then *detector-B* will try to detect the watermark in frames that were previously coded as B- and P-frames. If the motion of the objects in the scene is not intense or a slow camera zoom or pan has occurred, then the watermark will be detected in B- and P-frames because the decoding has transferred it to these frames. Otherwise, the watermark may not be detected in any of the video frames. Note, however, that in the latter case, the quality of the transcoded video will be highly decreased due to frame skipping (jerkiness in scenes will be created or visible motion blur will appear if interpolation is used), and for this reason it is very unlikely that an attacker will use such an attack.

6 Experimental evaluation

A software simulation of the proposed system was implemented and executed using a Pentium III 866-MHz processor. The system is applicable to constant and variable bit-rate MPEG-1/2 main profile multiplexed and video-only streams.

The first class of experiments presented in this section involves the performance evaluation of the proposed system in terms of speed. The performance of the watermark embedding and encryption subsystem was tested first. The MPEG-2 video *sportnews*, which contains two fast-motion scenes and is part of a TV broadcast, was used for the test. This is an MPEG-2 program stream, i.e., multiplexed stream that contains video and audio. It was produced using a hardware MPEG-1/2 encoder from a PAL VHS source.

The total execution time of the embedding and encryption subsystem for the 22-s MPEG-2 (5 Mbit/s, PAL resolution) video sequence *sportnews* is 75% of the real-time duration of the video sequence. Execution time is allocated in three major operations: (a) file operations (read-write headers and packets), (b) partial decoding, and (c) watermarking, encryption, and partial encoding, as shown in Fig. 9. In Fig. 9, the execution time is also compared to the decoding time (without saving each decoded frame to a file) using the software decoder of MPEG Software Simulation Group (MSSG). Clearly, the embedding time is significantly shorter than the decoding and reencoding time that would be needed if the watermark embedding were performed in the spatial domain. Figure 9 also presents the time required for detection using the *detector-A* described in Sect. 5.1. Detection time (partial I-frame decoding and detection) is only 23% of the real-time duration of the video sequence.

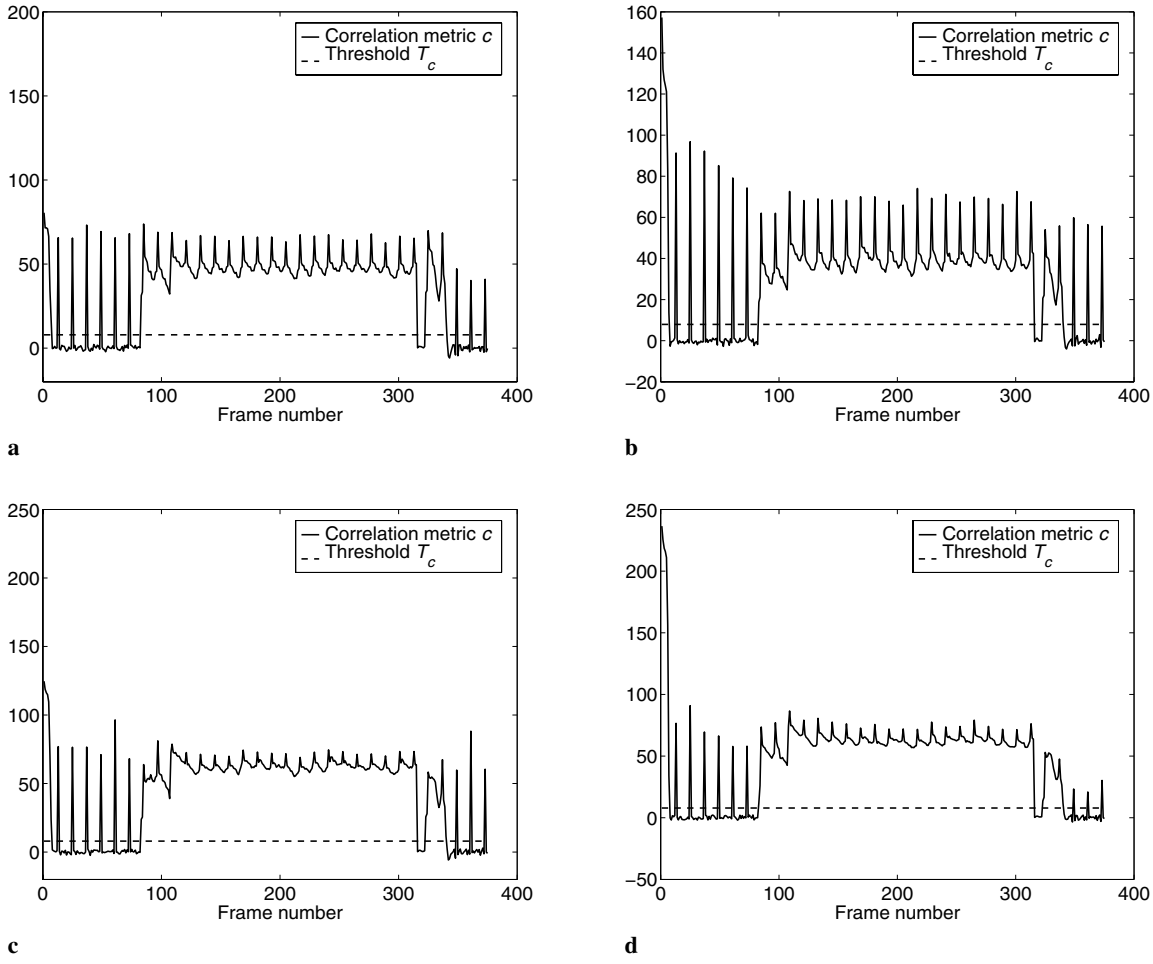


Fig. 11a–d. Plots of the correlation metric for all frames of the 8 Mbit/s MPEG-2 video *Table Tennis* after various attacks: **a** Blurring. **b** Cropping 64% of the frame area. **c** MPEG transcoding to 4 Mbit/s. **d** Conversion to MPEG-4 (2 Mbit/s and keyframes every 1 s)

The duration of the authentication and key extraction processes was also tested for the case where the video files are stored on a DVD-5 optical disc [23]. The authentication process takes between 5–15 s depending on the DVD-ROM drive unit and the operating system. The key extraction process is in all cases very fast, typically on the order of 1 ms. This is the time needed for the DVD-ROM drive to read a standard DVD-ROM sector.

Videos with various duration, GOP size, resolution, and bitrate were used to evaluate the performance of the SMP. Its real-time performance was verified in all cases. In addition, the reduction in decryption time due to the use of partial encryption instead of encrypting the entire file was investigated. Table 2 presents the partial decryption time for some video sequences as a percentage of the time that would be required for the decryption of the entire file. As can be deduced from the results presented, the time saving due to partial decryption is significant and ranges from 47% to 57%.

Finally, the performance of the watermarking method was evaluated by performing a number of tests with the PAL resolution 8-Mbit/s MPEG-2 video sequence *Table Tennis* using *detector-B*. Figure 10a presents the correlation metric for the 375 frames of the video sequence. As seen, the correlator output exceeds the adaptively calculated threshold for all I-frames. The correlator output is also above the threshold for the P- and B-frames of scenes where slow motion occurs. For example, for the P- and B-frames between the 84th and the 312th frames the correlator output is above the threshold. In cases where slow motion occurs, an attacker may remove the I-frames from the video sequence without causing severe degradation to its quality. In such cases, the watermark will be detected in the rest of the frames of the video sequence where slow motion occurs, as depicted in Fig. 10b.

Table 2. The time required for partial decryption as a percentage of the time that would be required for the decryption of the entire file

Video sequence	Percentage
Table tennis (MPEG-2, 8 Mbit/s, PAL)	43%
Mobile and calendar (MPEG-2, 6 Mbit/s, PAL)	47%
Flowers (MPEG-2, 4 Mbit/s, PAL)	53%
Susie (MPEG-2, 1.5 Mbit/s, Half PAL)	52%

The robustness of the embedded watermark in the case of common video processing attacks was also tested. The attacks include low-pass filtering (blurring), cropping 64% of the frame area, transcoding to a lower bit-rate (4 Mbit/s) MPEG

Table 3. Correlator output results for watermark detection on the 15th I-frame (frame 168) of the MPEG-2 *Table Tennis* video sequence

Attack	W	W'	Threshold
Original – no attack	121.1	−0.78	7.94
Blurring	67.7	−0.64	7.94
Cropping 64%	71.2	−0.03	7.94
Transcoding to 4 Mbit/s	75.3	−0.36	7.94
MPEG-4 conversion (2 Mbit/s)	72.8	0.55	7.94

stream, and conversion to MPEG-4 video format (2 Mbit/s and keyframes every 1 s). Table 3 shows the correlator output for the 15th I-frame of the *Table Tennis* video sequence when the owner's watermark W and a false watermark W' is used. In addition, the constant threshold $T_c = 7.94$ is given in the last column of the table. This threshold was determined using Eq. 5 and by setting a negligible false-alarm probability $P_{FA} = 10^{-15}$. Note that this probability is far lower than the maximum acceptable false-alarm probability (10^{-6}) suggested in [5] for copyright protection. It is easy to observe that the correlator output was significantly higher than the threshold for all cases of attacks. In addition, detection with a false watermark led in all cases to correlator outputs very close to zero and always below the threshold.

In the rest of the experiments, the above attacks were applied to all frames of the watermarked MPEG-2 video *Table Tennis*. The correlation metric plots for each one of the attacks are given in Fig. 11. The watermark survived in all I-frames and was still detectable in interframes of scenes where slow motion occurred.

7 Conclusions

We presented a complete system for the secure distribution of copyrighted MPEG-1/2 video stored on a DVD-ROM disc. The system offers a high level of security using encryption and watermarking techniques. The encrypted video files are decrypted on the fly and reproduced using the developed SMP. This operation is realized only if an authentic specially manufactured DVD-ROM disc containing the decryption key is available. The watermark, which is embedded in the video, is robust to several attacks and may be detected in order to prove the copyright ownership in case a pirate is able to capture the unencrypted but watermarked video.

The proposed system offers a solution that does not require any additional hardware (apart from a PC equipped with a DVD-ROM drive) on the user's part to offer the necessary security. It can be used to protect the MPEG-1/2 coded video content of an electronic encyclopedia, a video clip, or even a movie.

References

1. Agi I, Gong L (1996) An empirical study of secure MPEG video transmissions. In: Proceedings of the symposium on network and distributed system security (SNDSS '96), San Diego, 22–23 February 1996, pp 137–144
2. Alattar AM, Al-Regib GI (1999) Evaluation of selective encryption techniques for secure transmission of MPEG-compressed bit-streams. In: Proceedings of the IEEE international symposium on circuits and systems (ISCAS '1999), Orlando, 30 May–2 June 1999, vol 4, pp 340–343
3. Cheng H, Li X (2000) Partial encryption of compressed images and videos. IEEE Trans Signal Process 48(8):2439–2451
4. Chung TY, Hong MS, Oh YN, Shin DH, Park SH (1998) Digital watermarking for copyright protection of MPEG-2 compressed video. IEEE Trans Consumer Electron 44(3):895–901
5. Cox IJ, Miller ML, Bloom JA (2000) Watermarking applications and their properties. In: Proceedings of the international conference on information technology: coding and computing (ITCC 2000). Las Vegas, 27–29 March 2000, pp 6–10
6. Dittmann J, Stabenau M, Steinmetz R (1998) An empirical study of secure MPEG video transmissions. In: Proceedings of the 6th ACM international conference on multimedia, Bristol, UK, 12–16 September 1998, pp 71–80
7. Eleftheriadis A, Anastasiou D (1995) Constrained and general dynamic rate shaping of compressed digital video. In: Proceedigns of the IEEE international conference on image processing (ICIP '95), Washington, D.C., 23–26 October 1995, pp 396–399
8. Hartung F, Girod B (1998) Watermarking of uncompressed and compressed video. Signal Process 66(3):pp. 283–301
9. ISO/IEC 13818-2 (2000) Information technology – generic coding of moving pictures and asscociated audio: video. International Standards Organization, Geneva
10. Kamatakis J, Skalkos P, Kamatakis N (2000) CD-ROM Software Protection System. U.S. Patent 6,101,476, 8 August 2000
11. Langelaar GC, Lagendijk RL, Biemond J (1998) Real-time labeling of MPEG-2 compressed video. J Visual Commun Image Represent 9(4):256–270
12. Langelaar GC, Lagendijk RL (2001) Optimal differential energy watermarking of DCT encoded images and video. IEEE Trans Image Process 10(1):148–158
13. Li Y, Chen Z, Tan SM, Campbell RH (1996) Security enhanced MPEG player. In: Proceedings of the international workshop on multimedia software development, Berlin, 25-–26 March 1996, pp 169–175
14. Linetsky M (2001) Programming Microsoft DirectShow. Wordware Publishing, Plano, TX
15. Nahrstedt K, Qiao L (1998) Non-invertible watermarking methods for MPEG video and audio. In: Proceedings of the multimedia and security workshop at ACM Multimedia, Bristol, UK, 12 September 1998, pp 93–98
16. Papoulis A (1991) Probability random variables and stochastic processes, 3rd edn. McGraw-Hill, New York
17. Pohlmann K (1992) The compact disc handbook. A-R Editions, Middleton, WI
18. Rao KR, Hwang JJ (1996) Techniques and standards for image, video and audio coding. Prentice-Hall, Upper Saddle River, NJ
19. Schneier B (1995) Applied cryptography: protocols, algorithms, and source code in C, 2nd edn. Wiley, New York
20. Shi C, Bhargava B (1998) An efficient MPEG video encryption algorithm. In: Proceedings of the 17th IEEE symposium on reliable distributed systems. West Lafayette, IN, 20-–23 October 1998, pp 381– 386
21. Simitopoulos D, Tsaftaris SA, Boulgouris NV, Strintzis MG (2002) Digital watermarking of MPEG-1 and MPEG-2 multiplexed streams for copyright protection. In: Proceedings of the IEEE international conference on multimedia and expo. Lausanne, Switzerland, 26-–29 August 2002, pp 569–572
22. Spanos GA, Maples TB (1996) Security for real-time MPEG compressed video in distributed multimedia applications. In:

Proceedings of the IEEE 15th annual international Phoenix conference on computers and communications. Phoenix, AZ, 27–29 March 1996, pp 72–78
23. Standard ECMA-267 (2001) 120 mm DVD – Read-Only Disk, 3rd edn
24. Watson AB (1993) DCT quantization matrices visually optimized for individual images. In: Proceedings of the SPIE conference on human vision, visual processing and digital display IV, vol 1913, Bellingham, WA, February 1993, pp 202–216
25. Wu TB (1997) Selective encryption and watermarking of MPEG video. In: Proceedings of the international conference on imaging science, systems, and technology (CISST '97), Las Vegas, NV, 30 June–2 July 1997
26. Zeng W, Liu B (1999) A statistical watermark detection technique without using original images for resolving rightful ownerships of digital images. IEEE Trans Image Process 8(11):1534–1548