Reconfigurable Hardware Solutions for the Digital Rights Management of Digital Cinema

G. Rouvroy[1,2] F.-X. Standaert[1,2] F. Lefèbvre[3] J.-J. Quisquater[1,2] B. Macq[3] J.-D. Legat[2]

[1]UCL Crypto Group [2]Laboratoire de Microélectronique [3]Laboratoire de Télécommunications et Télédection
Place du Levant, 3
B-1348 Louvain-la-Neuve, Belgium
{rouvroy,fstandae,quisquater,legat}@dice.ucl.ac.be
{lefebvre,macq}@tele.ucl.ac.be

ABSTRACT

This paper presents a hardware implementation of a decoder for Digital Cinema images. This decoder enables us to deal with image size of 2K with 24 frames per second and 36 bits per pixels. It is the first implementation known nowadays that perfectly fits in one single Virtex-II® FPGA and includes AES decryption, JPEG 2000 decompression and fingerprinting blocks. This hardware offers therefore high-quality image processing as well as robust security.

Keywords

DRM, Digital Cinema, JPEG 2000, FPGA, AES, watermarking

1. INTRODUCTION

35mm films have been used since 1895 when the Lumière brothers presented the first cinematographic show in Paris. For more than 100 years, celluloid film has been at the heart of the Movie Industry. It is always used as the major medium for recording, storing and projecting images. The ease of 35mm film, known today by the more technical term *interoperability*, largely contributed to the success of this technology. Now, a new system is taking the place of film as the prime medium for studios and projection theaters. Widely known as Electronics Cinema (E-Cinema) and Digital Cinema (D-Cinema or DC), it replaces conventional 35mm films and projectors with computer workstations, hardware decoders and high resolution electronic video projectors. Behind Digital Cinema, a global concept and a complete system are hidden, covering the entire movie chain from acquisition with digital camcorders to post-production, distribution and exhibition, all the data being stored with bits and bytes instead of 35mm reels.

The concept of Electronic Cinema is actually quite old, dating back to the first half of the 20th century. Electronic cinema was indeed discussed before the introduction of television. DC started to develop in 1990, when the Hughes/JVC ILA (Image Light Amplifier) projector became available. This electronic projector was the first to deal with large cinema screens and produce pictures of good quality. However, the ILA projector suffered from maintenance and alignment issues.

A new system for cinema, called Digital Light Processing (DLP) projector, was first publicly demonstrated in 1999. This was the result of many years of innovative works undertaken by Texas Instruments® and based on collaborations with Hollywood studios. This projector proposed a wider color space with regards to television and a pixel array of 1280 x 1024. DLP projectors are based on MEM technology (Micro-Electro-Mechanical). It utilizes about 1 million mirrors that can flip between reflecting light to the projection lens and away from the projection lens. This projector has proved to be consistent and reliable in theaters with no maintenance problems. In 2003, a second generation of DLP Cinema projectors was introduced, dealing with a resolution of 2K (2048 × 1080 pixels) images. Recently in June 2004, Sony® presented the first prototype of 4K (4096 × 2160 pixels) projector using a Silicon X-tal Reflective Display (SXRD) imaging device that enables them to achieve nearly four times the pixel count of current HD displays. This chip enables the projection of very high-quality images with rich and precise color tonal reproduction.

Today, it is commonly considered that, without DLP technology, it would not be possible to have a current and significant development in Digital Cinema.

Now, the industry exploits a small part of Digital Cinema. The Movie Industry is not different from any other one in its search to contain and reduce costs, increase revenues and improve customer satisfaction. Nevertheless, a complete Digital Cinema rollout means important changes and new challenges.

Digital Cinema is still taking its sweet time coming to theaters. Today, digital movies can only be seen on about 350 cinema screens worldwide (only 0.2% of the estimated 150,000 cinema screens around the globe). This is a tiny but deliberate penetration. These sites are not the beginning of the complete rollout, but are just considered as "test sites".

The major contribution of this paper concerns the achievement of a reconfigurable hardware image decoder for Digital Cinema. It analyzes the feasibility to fit decryption, decompression and fingerprinting blocks in one single Virtex-II®

DRM'04, October 25, 2004, Washington, DC, USA.

FPGA. We also achieve designs that meet the main requirements of Digital Cinema. The decryption step covers the study of a well-adapted AES core in terms of resources and throughput. We currently get the best AES design in terms of *Throughput/Area* ratio. The decompression part proposes the implementation of JPEG 2000 adapted to 2K images. Complete JPEG 2000 IPs are scarce and we achieve the first FPGA solution that can efficiently deal with large images. Finally, we get a fingerprinting design that allows an efficient solution to track illegal camcorder capture in theaters. We currently achieve the first academic hardware implementation of a watermarking scheme.

This paper is structured as follows. Section 2 explains why the rollout to Digital Cinema is so gradual. It details the financial and technical issues and the major players involved in the DC process. Section 3 presents the future Digital Cinema system and its main interesting features. Our developed image decoder in an FPGA is presented in Section 4. Section 5 analyzes the security of our FPGA solution against traditional piracies of 35mm system. Finally, Section 6 concludes this paper.

2. GRADUAL DIGITAL CINEMA ROLLOUT

Today, for Hollywood studios and exhibitors, a global system, suitable for a wide-spread rollout, does not exist. Some *financial* and *technical* issues still persist.

2.1 Financial Issues

Principal financial issues are published in the literature and concern four distinct aspects.

1. The global *system cost* is a major difficulty. Indeed the value of a new digital projection unit is around \$150,000 for one third the lifetime ($\simeq$ 3 years) of a new 35mm film projector, which costs about \$30,000.

2. *Benefits for distribution* are incredibly huge. Studios would probably save more than 800 million dollars annually, replacing the conventional 35mm reel (between \$1,500 and \$3,000 per single print of a movie) with a digital distribution ($\pm$ \$200). *Theaters* would not generate any other additional benefits if the ticket prices remain as nowadays.

3. DC could never drive enough extra traffic through its box offices to purchase digital projection systems. A *financial contribution* from the studios is therefore vital.

4. A last and indirect aspect is the *piracy* issue. In general, piracy is important when the value (for the pirate) of the pirated content exceeds the cost to mount piracy. In traditional 35mm systems, piracy is a serious problem. The goal of a movie pirate is to get an unprotected copy of film, which can be electronically distributed all over the internet without any restrictions. This illegal redistribution becomes especially relevant using file sharing systems such as Edonkey and Kazaa. This wide availability of movie copies (shortly after their release) is responsible for income loss of several million dollars (evaluated by the studios to two billion dollars annually). An important question therefore subsists concerning the true security of current digital projection prototypes. The search for solutions to solve or at least decrease the problem is really worth the burden. In this view, Digital Cinema offers great opportunities.

The first three aspects do not seriously influence the technical issues. Only the piracy problem has a significant impact on technical and security considerations. Therefore, we devote additional arguments detailing this current piracy.

Well-known attacks of 35mm systems can have one of the following forms:

1. Pirates are involved in the production chain and can directly hack the film content before its distribution around the globe.

2. Piracy results from direct thefts of physical reels in distribution processes or in box offices where reels are stored.

3. Pirates (*i.e.* projectionists) are able to duplicate original movies without any evidences (against them) of provable thefts. In addition, it is almost impossible to identify the pirate among all cinema projectionists.

4. Camcorder capture of projected movies (in the theater) is a significant attack against celluloid systems. It is asserted that seventy percent of the copies are made using camcorders in theaters [18] (*e.g.* seventy percent of those copies have been traced from theaters in the area of Manhattan).

2.2 Technical Issues

Today, all *technical* documents are only drafts under construction and mostly unpublished. Nevertheless, we can outline the following requirements:

- *Full interoperability* has to be achieved in order to enable a worldwide rollout. In Digital Cinema, it means that when someone sends you bytes, your equipment understands them and the resulting process is correctly achieved. Many steps require interoperability: the manner in which numerical content is digitally packaged when sent by the distributor, the file formats themselves, the distribution of security keys, the processes of decryption and decompression within the exhibition theater, and the control data that accompanies image and audio content for use by pictures and sound decoders. Any variation in any one of these steps creates a negative impact on interoperability. For the decoder, it therefore means that the system must comply with the current drafts and also easily evolve to future norms, which requires fast upgrades without the removal and change of hardware devices.

  Today, four different commercial systems are in place (Avica, GDC, EVS and QuVIS), requiring four individual mastering processes to guarantee that a digital movie can be played on each system. These test sites are therefore not fully interoperable. Nevertheless, these test theaters are very useful for studios, distributors, exhibitors and equipment makers to learn the practical issues of Digital Cinema.

- *Image quality* has to be really optimal in order to offer better quality entertainment than celluloid films

and current DVDs and digital home videos. A *visually lossless quality* must therefore be promoted.

For specialists, Digital Cinema can offer better quality than celluloid films. Special demonstrations with digital projection side-by-side with film were achieved in order to evaluate the digital screening. The major conclusion is that there are important differences. Nevertheless, not everyone agrees that digital projection today is efficient enough to replace the traditional film. Exhibitors claim that it must be arguably better than film in order to justify the expense of Digital Cinema rollout.

- *Multi-resolution* is one of the major flexibility of future norms. It means that all servers (in projection rooms) are able to store compressed movie files with 2K or 4K resolutions and that all decoders are designed in order to display those contents. It also promotes two decoder/projector generations: the 2K and 4K.

- Security is a generic term that covers the encryption of images, subtitles and audio contents, the key exchange, the conditional access, the monitoring system, the fingerprinting and the physical robustness against attacks of various form. Therefore, it covers the Digital Rights Management (DRM) of Digital Cinema.

2.3 Major Players Involved

In January 2000, the first open meetings of SMPTE[1] Digital Cinema Technology (DC28) were held in Los Angeles. Nowadays, the current Committee counts more than 100 members representing worldwide experts. DC28 is divided into seven study groups: Mastering, Compression, Conditional Access, Transport and Delivery, Audio, Theater Systems, and Projection units. The term "study group" is well chosen. The purpose of these groups is to uncover and discuss the various issues that the full deployment of DC faces. The DC28 Committee is chartered to provide engineering guidelines, recommendations and standards to ensure interoperability, compatibility, performance and support for future innovation in Digital Cinema. This Committee has therefore to solve the first two issues exposed in Subsection 2: the digital and cinema problems, respectively corresponding to the interoperability and the projection quality.

The high cost of the equipment and the prudence of electronic distribution request in this view a business negotiation[2]. Groups have thus been created: The National Association of Theater Owners (NATO) and a new American group called Digital Cinema Initiatives (DCI). Recently, these two organizations announced the enforcement of the legal framework for a business negotiation.

NATO is the largest exhibition trade organization in the world, representing more than 26,000 movie screens in more than 20 countries worldwide. Current membership includes the largest cinema chains in the world and hundreds of independent theater owners.

DCI was created in March 2002, as a joint venture of the seven major American motion picture studios (Disney®, Fox®, MGM®, Paramount®, Sony Pictures Entertainment®, Universal® and Warner Bros.® studios). DCI's primary purpose is to establish and document specifications [6] for an open architecture for Digital Cinema that ensures a uniform and high level technical performance, reliability and quality control. DCI will also facilitate the development of business plans and strategies to help the deployment of digital systems in movie theaters. It represents then studio inputs to the SMPTE DC28 process [22, 28]. The issue of the final version of the DCI Technical Specifications is expected for autumn 2004.

An equivalent European group of DCI is the European Digital Cinema Forum (EDCF). It was formed at a meeting in June 2001 which gathered thirty representatives of institutions, companies and trade associations within the European film, TV, video and telecom sectors. Inputs to the DC28 process are also provided by this European consortium.

Since the beginning of DC, a real progress has been made simultaneously on business and technical issues. It is commonly claimed that, even if the road ahead may be rough, Digital Cinema still continues to evolve and profit from significant developments.

3. FUTURE DIGITAL CINEMA SYSTEM

A digital system will involve many components built by different manufacturers. The system will have to support various contents from different providers. Open and uniform standards must then be developed to promote competition, worldwide compatibility and interoperability. SMPTE DC28, EDCF, and especially DCI are therefore chartered to provide these standards.

Even if the writing of the following subsections gives the impression of definitive Digital Cinema specifications, current works on global systems are only draft specifications, mostly unpublished [6, 28]. Next subsections do not pretend to be exhaustive: hundreds of pages would be necessary. It only tries to introduce the global system and major Digital Cinema characteristics to allow the reader to understand the whole significance of this paper.

3.1 Global System Overview

In order to describe the specific requirements and standards for Digital Cinema, it is useful to subdivide the system into a framework of blocks. A functional framework of a Digital Cinema encoding and a decoding system is respectively shown in Fig. 1 and 2.

The major illustrated components are the following ones:

- *Digital Cinema Distribution Master* (DCDM) corresponds to the uncompressed, decrypted set of files containing the content and its associated data.

- *Compression* is a process that reduces redundancies in source essence data. System requirements related to this process and its inverse (decompression) are under construction. In June 2004, a worldwide standard was selected. The chosen algorithm was JPEG 2000 (Part 1: Core coding system [11]).

- *Security* contains system requirements that deal with the protection of the intellectual property rights. Processes for encryption, decryption, key management, link encryption, and fingerprinting are constituent elements of the security scheme. Advanced Encryption Standard (AES, [19]) with 128-bit key will be the chosen encryption algorithm.

[1]Society of Motion Picture Television Engineers.
[2]Third issue in Subsection 2.

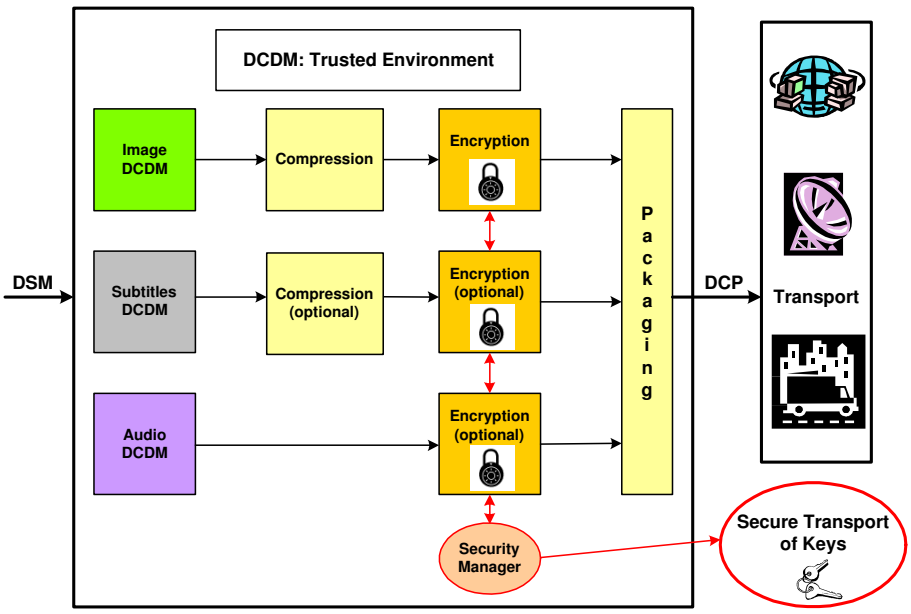

Figure 1: Functional encoding flow

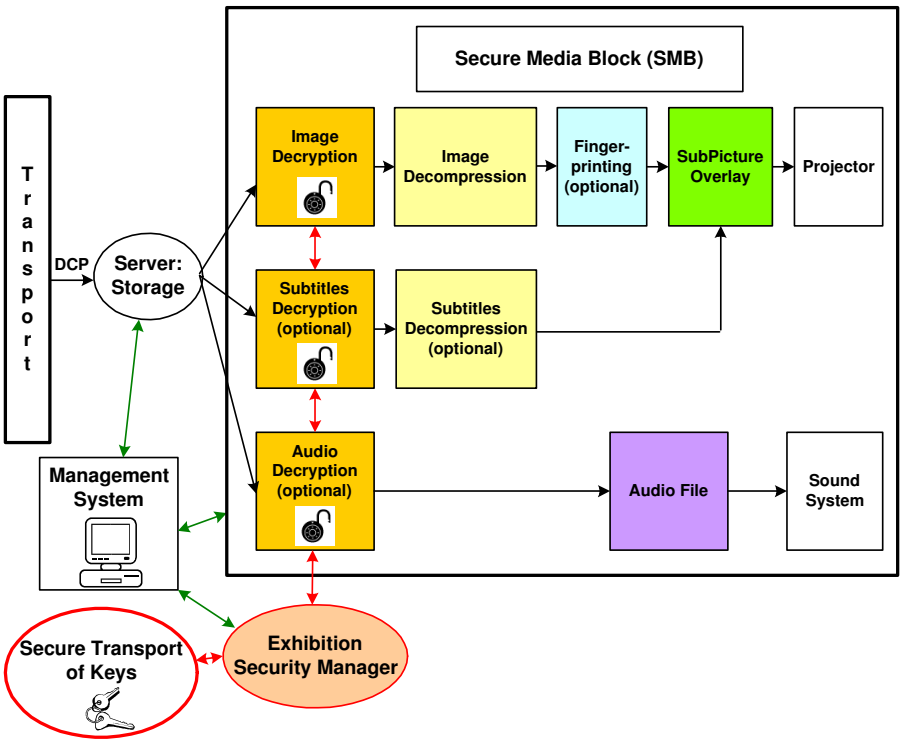

Figure 2: Functional decoding flow

- *Packaging* illustrates the process of wrapping and unwrapping compressed and encrypted files for distribution and play-out. The frame encapsulation should probably be the MXF standard.
- *Transport* deals with the distribution of the packaged media through satellite links, internet or boxes of DVDs.
- *Theater Management System* includes the required system equipment installed at a theater for control, scheduling, logging, diagnostics and system monitoring.
- *Projection* is the system that has the performance characteristics used to display the images on the screen in 2K or 4K format.

3.2 Important Technical DC Requirements

This subsection briefly details some potential important technical DC requirements in order to place the next sections of this paper into the right context.

3.2.1 Digital Cinema Distribution Master

The purpose of the DCDM is to set rules for exchanging images, subtitles, audio and auxiliary data to encoding systems and to the Digital Cinema decoder system. The DCDM is the output of the post production Digital Source Master (DSM) and is also the image, subtitle and audio structures. These structures are mapped into file formats that encompass the DCDM. A quality control check is then performed in order to verify items like synchronization, image size, number of frames per second and so on. This requires the DCDM files to be played directly to the final decoding devices in their native decrypted, uncompressed and unpackaged form.

If the content does not meet this DCDM specification, it is the content creators and DSM responsibility to convert it to the DCDM format before it can be used for Digital Cinema.

Once the DCDM is encoded, encrypted, and packaged for distribution, it is considered to be the Digital Cinema Package (DCP). This term is used to distinguish the package from the raw files collection defined as the DCDM.

3.2.2 Multi-Resolution Image Structure

The DCDM requires a multi-resolution image structure that provides both 2K and 4K resolution files, so that studios can choose to deliver either 2K or 4K masters and both 2K and 4K projectors can be deployed and supported. This interesting and very important feature is illustrated in Fig. 3. 2K is the typical size of the best current DC resolution in production. 4K will be the top quality resolution in the future knowing that the first prototype of 4K Digital Cinema projector (developed by Sony) was demonstrated to the Hollywood community in June 2004.

This multi-resolution scheme implies that all servers are able to store a compressed DCDM of 2K or 4K resolution. The decoder for 2K projector needs to extract and display the 2K resolution file from 2K or 4K DCDM file. The future 4K projector also requires to display both DCDM formats, therefore capable to resize 2K DCDM files. This scheme deals with 12 bits per component (36 bits per pixel (bpp)) which can give visually lossless quality. 2K mastering also works with 24 or 48 frames per second (fps) even though 4K mastering is only interested in 24 fps.

3.2.3 Secure Media Block

The storage and Media Block (MBlk) are components of the theater system. The storage is the hardware that holds the packaged content for eventual playback. Knowing that a 2-hour movie requires from 300 to 800 GBytes, the storage resources must be incredibly huge. The MBlk is the hardware device (or devices) that converts the packaged content into streaming data that finally turns into images and sound in the theater. It achieves real-time decryption, decompression and eventually fingerprint processes. The decryption process needs to deal with peak throughput of 300, 600, or 800 Mega bits per second (Mbps) respectively for 2K (24 fps), 2K (48 fps) and 4K (24 fps). The decompression and fingerprinting outputs range from 1.8 to 7.2 Giga bits per second (Gbps) for decoders from 2K (24 fps) to 4K images (24 fps). Storage and MBlk components can be physically merged together or separated from each other. In a separated MBlk, the decryption step needs to occur in this block to ensure its security. It is therefore called the Secure Media Block (SMB) as detailed in the right part of Fig. 2. A large part of this paper aims at defining and proposing a secure, modular and real-time SMB for 2K images (24 fps, 36 bpp) for Digital Cinema. Our paper only investigates implementations on image processing and does not consider subtitles and audio problems. In addition, our modular approach allows us to easily adapt our decoder to the top quality 4K images, however increasing the physical cost of our solution.

3.2.4 Component Design

In order to reach interoperability, the hardware and software used in the global system, and especially in the SMB, have to be easily upgraded as discoveries in technology are made. Upgrades need to be achieved in such a way that the content can be distributed and be compatible with the latest hardware and software as well as earlier adopted equipment installations.

The Digital Cinema system should provide a reasonable path for upgrading to future technologies. It is important to make it possible for susceptible components to be replaced or upgraded without the replacement of the complete system.

3.2.5 Global Reliability

Reliability is the key part of Digital Cinema systems. In future digital theater, the show should not be interrupted regularly. Equipment could break down but the expected average between failures has to be about 10,000 hours.

4. RECONFIGURABLE HARDWARE DECODER

The major contribution of this paper concerns the achievement of a reconfigurable hardware image decoder for Digital Cinema, called Secure Media Block (SMB) by the DCI. It was implemented in one single reconfigurable hardware, a Xilinx Virtex-II® FPGA (XC2V6000-4, [34]) where all blocks fit in it and are developed in such a way that no data flow transits outside the FPGA, except the input and output data. Currently, neither universities nor industrial groups propose such a global solution that fully meets current DC drafts. Only separated blocks from different groups were published. They are presented below and are not always relevant solutions.

Fig. 4 shows the proposed image decoder for Digital Cin-

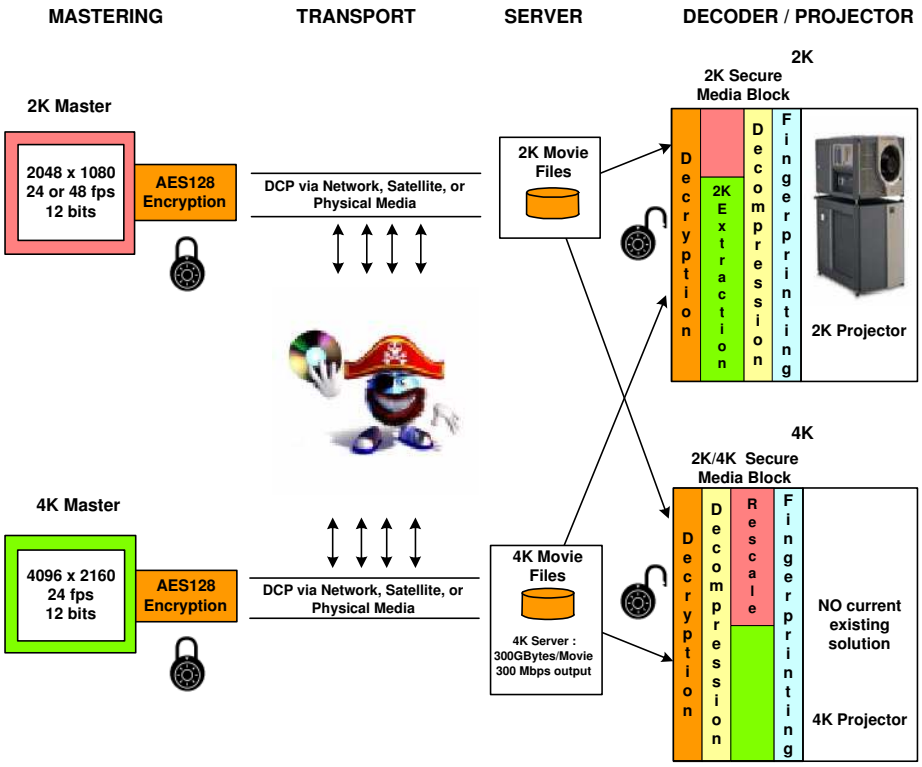

Figure 3: Multi-resolution image structure

ema. It enables us to draw up our research frame in three major parts: the decryption, the decompression and fingerprinting steps.

4.1 AES Decryption

4.1.1 Requirements of Digital Cinema

This cryptographic block is the first and most important protection layer applied to high-value digital media content. It allows the confidentiality of the DCP (Digital Cinema Package) for foreign users and a conditional access for Secure Media Blocks (SMBs) in authorized theaters.

The encryption/decryption method will be based on the AES cipher in Cipher Block Chaining (CBC) mode with 128-bit keys. Image frames will be encrypted as independently-decipherable units in order to deal with unexpected projection breaks and to support mid-show restarts. Each frame will have a random 128-bit Initialization Vector to start the new CBC mode. The secret key will be kept constant at least during a thousand frames, maybe during a complete film of 2 hours. To be accurate, the CBC mode requires the length of the plaintext to be padded to a multiple of the cipher block size, which is 16 bytes for the chosen AES. The padding method will potentially add one to fifteen constant bytes.

AES with 128-bit key is estimated to remain a suitable and secure solution for the next decades. The CBC is a natural choice considering that this mode is widely used. Indeed, if the whole picture has two identical plaintext blocks, both resulting ciphertexts will be completely different in contrast to the ECB mode.

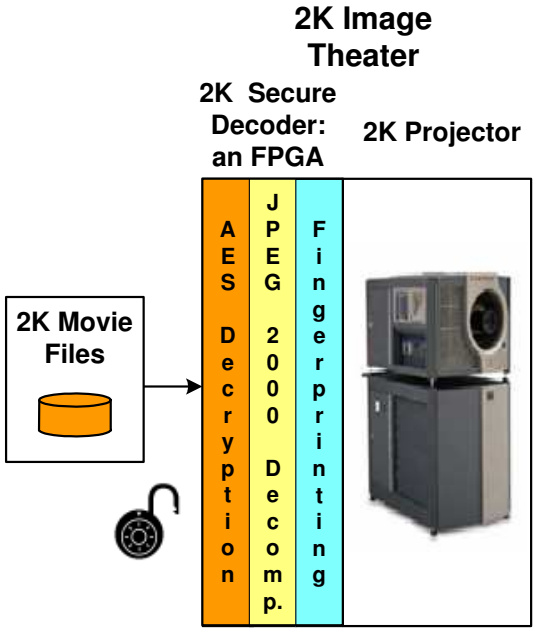

Figure 4: Image decoder for Digital Cinema

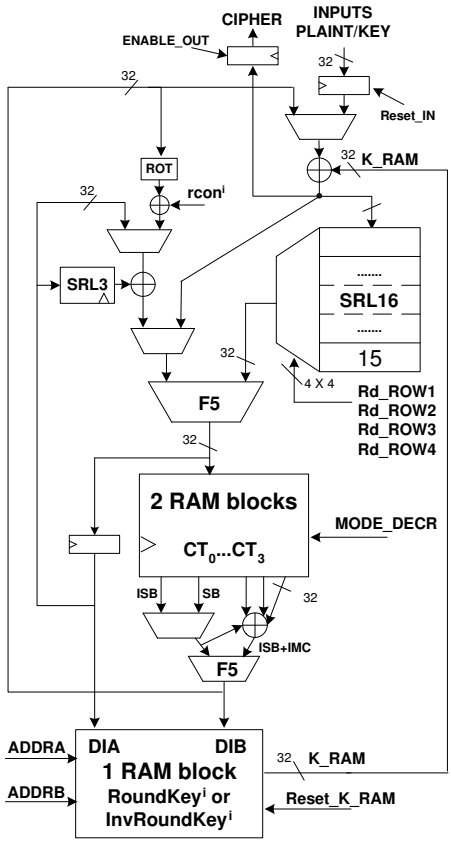

Figure 5: Our complete AES design

4.1.2 FPGA Implementation and Results of AES

Implementation choices are not detailed in this paper. However, the reader can refer to paper [25] for more technical information.

Our AES design combines the data-path part and the key scheduling part. Since the key scheduling is done with precomputation, this part does not work simultaneously with the encryption/decryption process. It is therefore possible to share resources between both circuits. Both parts of the circuit were thought to perfectly fuse together without additional ressources. This allows reaching very high frequency. The global design is shown in Fig. 5. We fused the key and plaintext inputs to one register. The input and output registers are packed into IOBs to improve the number of resources used and the global frequency of the design. We also focuss on a design that enables CBC mode of operation.

The final implementation results are given in Table 1 for Spartan-3® and Virtex-II® devices. Spartan-3 ([35]) device is mentioned to enable comparisons with another design. Our FPGA module can deal with a throughput of 300 Mbps. We currently achieve the best AES encryptor/decryptor known nowadays (in terms of $Throughput/Area$ ratio) with a maximum data rate of 342 Mbps.

Table 2 compares our AES solution into a Spartan-3 device with the previous best solution [10] (Sept. 2003) into a Spartan-II component.

We finally achieve an implementation of AES in CBC mode which is 63% better in terms of $Throughput/Area$ ratio assuming that Spartan-II and Spartan-3 are equivalent.

Device	XC3S50-4	XC2V40-6
LUTs used	293	288
Registers used	126	113
Slices used	163	146
RAM blocks	3	3
Latency (cycles)	46	46
Output every (cycles)	1/44	1/44
Frequency (MHz)	71.5	123

Table 1: Final results of our complete sequential AES

AES Algorithm	Gaj's	**Ours**
Device	XC2S30-6	**XC3S50-4**
RAM blocks	3	**3**
Slices	222	**163**
Latency (cycles)	44	**46**
ECB Throughput (Mbps)	166	**208**
ECB Throughput/Area (Mbps/slices)	0.75	**1.26**
CBC Throughput (Mbps)	166	**199**
CBC Throughput/Area (Mbps/slices)	0.75	**1.22**

Table 2: Comparisons with the best previous sequential AES implementation

4.2 JPEG 2000 Decompression

4.2.1 Requirements of Digital Cinema

Image compression for Digital Cinema has to work with data reduction techniques to decrease the size of the data for economical delivery and storage. Compression is typically used to ensure transmission bandwidth or media storage limitations. Indeed, a raw movie of 2 hours (2K images, 24 fps, 36 bpp) represents more than 1700 GBytes. Therefore, compression ratios of about 5-8 are usually considered in DC.

The system has to use perceptual coding techniques in order to achieve an efficient compression ratio with a good image quality. The image quality is therefore dependant on the scene content and the compressed bit-rate. Digital Cinema image compression does not directly rely on bandwidth or storage requirements. In DC, the bit-rate must be adapted to the desired image quality rather than the reverse.

Hereunder, we enumerate the fundamental requirements of the DC compression algorithm:

1. The selected compression algorithm must be *license free* or with very reasonable terms and conditions for the Digital Cinema use.

2. The Digital Cinema image compression system will use only one *worldwide-standardized* image compression specification. Public specification must be available with sufficient algorithmic details in order to enable any society to build encoders and decoders.

3. The image compression must be *visually lossless* under normal viewing conditions. Visually lossless means that human eyes should not be able to distinguish differences between the reconstructed picture after decompression and their original raw image during a normal projection in a theater.

4. A *constant image quality* approach with a variable bitrate must be promoted instead of a constant throughput with a variable image quality.

5. The selected compression algorithm must easily deal with a *multi-resolution* image structure as previously detailed .

6. The selected algorithm must deal with *error detection and resilience*. However, Digital Cinema will be transmitted over relatively low-noise channels. Efficient error concealment for DC may be less necessary than for television applications.

7. The compression system must support *random access* functionalities in order to deal with power failures and undesired interruptions.

All separated points, but especially 1, 5 and 7, promoted Motion JPEG 2000 ([11, 12, 13]) in place of MPEG-2, MPEG-4, H.264/ AVC, or other standardized algorithms. This work does not pretend to fairly compare Motion JPEG 2000 with other compression systems: hundreds of pages would be necessary. Good academic papers and reports [17, 27, 36] exist. The first paper exposes the superior rate-distortion performance of Motion JPEG 2000 for high resolutions and bitrates in comparison with pure intra coding H.264/AVC. The second paper demonstrates the functionalities improvements provided by JPEG 2000. The last technical report concludes that Motion JPEG 2000 propose good compression efficiency, error resilience and video quality in comparison with Motion JPEG and MPEG-2. Nevertheless, papers [17, 36] commonly consider that the Motion JPEG 2000 compression algorithm has a high computation complexity to meet real-time software applications.

Therefore, this paper investigates a hardware solution of this complex and efficient compression algorithm in order to reach the DC requirements. We only give results concerning our 2K image decoders (24 fps, 36 bpp). Nevertheless, our design methodology (based on a modular and scalable design) is also valid to deal with 4K images if additional hardware resources (larger or multiple FPGAs) are available.

4.2.2 FPGA Implementation and Results of JPEG 2000

Due to space constraints, implementation details are not mentioned. Nevertheless, the reader can refer to previously published paper [9].

The global architecture has been implemented in VHDL and synthesized and routed in an FPGA (XC2V6000-4). Table 3 presents the resources used with this configuration. As it can be seen, only 61.8% of the RAM resources are used. Further development could make use of these free resources.

Table 4 presents the bit-rates achieved by our architecture. As we can see, this configuration yet enables real-time 4:4:4 video decoding for the 2K images (24 fps, 36 bpp) and a compression ratio of 20. For a compression ratio of 11, the same format is supported with 4:2:2 images. No information is given concerning a 4K image decoder. Nevertheless, our modular FPGA design approach allows us to easily achieve this requirements provided that larger Virtex-II® devices exist or that multiple use of FPGAs are allowed.

Device	XC2V6000-4
LUTs used	51,416 over 67,584 (76.1%)
Slices used	30,323 over 33,792 (89.7%)
RAM blocks used	89 over 144 (61.8%)
Frequency (MHz)	89.9

Table 3: Final results of our complete JPEG 2000

Compression ratio	Complete Scheme [#(2K images)/sec]
1:10	14.63
1:14	18.20
1:20	25.92
1:32	42.94

Table 4: Bit-rates achieved by the proposed architecture

Several other JPEG 2000 hardware implementations have been developed. The main coding options differences between three recent implementations and the proposed architecture are listed in Table 5. A comprehensive comparison of their performances (bit-rates achieved) is difficult as the output bit-rate strongly depends on the compression ratio targeted. For example, the architecture in [1] offers good performance while allowing large tile size. Nevertheless, more details than those provided on their website would be necessary to achieve a valuable comparison. Our FPGA solution is therefore the first academic one presenting a modular and efficient FPGA solution dealing with large image size.

4.3 Fingerprinting

4.3.1 Requirements of Digital Cinema

The fingerprinting process only prevents piracies based on an illegal camcorder recording (in the projection room) and on a "probing attack" between the decoder and the projector. If this process remains robust, the purpose of Digital Cinema fingerprints is to provide event-specific forensic evidences in these cases of theft.

Current DC drafts do not recommend a specific fingerprinting process. It will probably be the responsibility of the content owners to select their algorithm.

Nevertheless, the following set of desirable features are suggested.

- Fingerprints must not perceptibly degrade the quality of the image in which the marks are embedded.

- Embedded watermarks must be sufficient to identify the time, location, projection room, and other relevant details of the theft.

- Fingerprints must be reliably extracted from hacked materials.

	Barco Silex[4]	Arizona Univ.[2]	Analog Devices[1]	**Proposed architecture**
Technology	FPGA XC2V3000	ASIC 0.18μm	ASIC ?	**FPGA XC2V6000-4**
Max. tile size	128×128	128×128	$2,048 \times 4,096$	$512 \times 4,096$
Max. cblk size	32×32	32×32	not provided	$2,048$ **coeff.**
Wavelet filters used	(5,3)-lossless (9,7)-lossy	(5,3)-lossless (9,7)-lossy	(5,3)-lossless (9,7)-lossy	**(5,3) lossy and lossless**
Number of Entropy coders	8	3	3	**10**

Table 5: Differences between recent implementations and our architecture

- Fingerprints have to be robust enough in order to allow recovering from distorted stolen images. Marks have also to resist image processing intended to obscure the fingerprinting data.

- Detection and extraction does not need to occur in real-time.

4.3.2 *FPGA Implementation and Results of our fingerprinting scheme*

The selected fingerprinting scheme for our decoder is a watermarking algorithm developed in our UCL telecommunication laboratory (TELE) and presented in many conferences [7, 8, 16, 26]. This algorithm ensures a strong resistance against some attacks such as print and scan, compression, noise, cropping, translation and rotation. It is a spatial domain algorithm based on secret 56-bit keys. Copyright and tracking are practical applications for this watermarking algorithm. This hidden 64-bit mark contains enough information (such as theater location, projection room and time) to track the corrupted and illegal movie files.It was used successfully in several European projects ([3] and [5]).

Once again, the goal of this paper does not attempt to detail this algorithm but tries to validate the feasibility of a complete hardware image decoder for Digital Cinema.

The final implementation results are given in Table 6 for a Xilinx Virtex-II® FPGA (XC2V500-4). We detail the resources used for two frame sizes (1024×768 and 2K images).

Our design is able to fingerprint all 2K video frames even if we need to project at a dataflow over 48 fps. Therefore, we fully meet the DC requirements for the 2K format. Concerning 4K images, the throughput has to be increased by a factor of two. A more parallelized design must be achieved, dealing with two or four pixels per clock cycle.

Device	XC2V500-4	XC2V500-4
Frame size	1024×768	2048×1080
LUTs used	2474	4045
Registers used	1136	1142
Slices used	**1562**	**2349**
RAM blocks used	4	4
Multipliers used	4	4
Latency (cycles)	3080	6152
Output every (cycles)	1	1
Frequency (MHz)	143.9	143.9
Throughput (Mbps)	**5180**	**5180**
Number of fps	**182.98**	**65.06**

Table 6: Final results of our complete fingerprinting scheme

Other designs of fingerprinting schemes are also rare. Today, only a few universities and societies (such as Thales and Philips) propose schemes designed for DC applications. Most of currently solutions come from commercial schemes. Nevertheless, very small algorithmic details are published.

4.4 Reconfigurability Feature

It is worth noting that our global solution really innovates in terms of *reconfigurability*.

In order to reach interoperability, our hardware SMB can be easily upgraded as discoveries in technology are made. Upgrades need to be achieved in such a way that the content can be distributed and be compatible with the latest hardware as well as earlier adopted equipment installations.

Our Digital Cinema decoder based on a Virtex-II® FPGA provides a perfect path for upgrading to future technologies. For traditional dedicated hardware (ASICs), the complete SMB or some hardware components would have to be replaced in case of upgrades. We propose a FPGA solution that efficiently allows remote reconfigurability and therefore could deal with any evolution in DC norms.

5. SECURITY ANALYSIS

In order to fairly evaluate the security of our decoder, we propose first to briefly extrapolate the four current well-known attacks of 35mm system (detailed in Subsection 2.1) to our Digital Cinema decoder:

1. Our solution does not prevent a pirate from hacking movies directly in the production chain. Additional security layers (conditional accesses, fingerprinting, ...) are thus required in production studios in order to track the piracy. This is obviously out of concern for the proposed system.

2. Concerning the robbery of distribution media in delivery processes or in projection offices, the attacker does not have a physical access to the decryption device. Therefore, the security rests on the symmetric cryptographic algorithm (AES) as well as the number of secret keys. Knowing that a two-hour movie film represents 300 GBytes of encrypted data, which corresponds to less than 2^{35} ciphertexts, an AES encryption with a single secret key K_{dec} is theoretically secure enough. Nevertheless, it should be preferable to *regularly change this key* during the movie in order to improve the global robustness of the system. An appropriate number of keys $K_{dec(i)}$ should be between 1000 and 10000 for one movie in order to have independent encrypted movie sequences of less than eight seconds. Finding one secret key will not significantly

corrupt the global system. In addition, these secret keys must also be changed for every new film. Our AES decryption module allows all these features.

3. Attacks where the projectionists are able to duplicate the original encrypted film without any evidences of thefts are still possible. Nevertheless, if no secret keys are directly given to theater employees and directors, the system remains secure. In this thesis, we want to promote the use of *a smart card* (valid for one movie) that confidentially contains the secret keys $K_{dec(i)\_SC}$ required for decryption of the movie. It is therefore necessary to achieve a mutual authentication between the smart card and the decoder (using a challenge-response protocol based on symmetric-key or public-key techniques), before performing the secure transfer of all secret keys. In addition to the secret keys for the conditional access (K_{auth}) and secure transfer (K_{trans}), the FPGA decoder must store (at the configuration) another secret key (K_{dec_FPGA}) also required for the decryption process of movie. Indeed, we improve the security using *shared secret keys* between the smart card and the FPGA, which forces an attacker to hack both devices. The secret keys for the decryption of the movie can be thus expressed as $K_{dec(i)} = F(K_{dec\_FPGA}, K_{dec(i)\_SC})$.

4. Camcorder capture of projected movies can be also an important attack of digital systems. Projectionists as well as spectators can be responsible of such hacking. Projectionists could organize illegal and private projection session in order to perform high-quality camcorder recordings of movies. Nevertheless, thanks to the conditional access and projector monitoring, these dishonest employees will be directly spotted. Concerning unscrupulous spectators, the fingerprinting process should enable us to track illegal copies, locate the corrupted projection rooms and increase the surveillance of suspected theaters. A robustness evaluation of our fingerprinting scheme is proposed in the Appendix.

In addition to major Digital Cinema requirements, our considered reconfigurable hardware decoder proposes additional security layers. This is due to the use of FPGAs (as discussed in paper [33]):

- In comparison to current commercial solutions (mostly based on separated triple-DES and MPEG-2 chips without a fingerprinting process), the three main blocks of our decoder are implemented in one single FPGA device. Therefore, our solution prevents any "probing attacks" after decryption and/or decompression blocks because no internal data transits outside the FPGA. A fully-integrated hardware chip is an additional countermeasure that should significantly not increase the price of the complete digital projection unit but would widely increase this security.

- Our reconfigurable hardware chip enables cheap and easy renewal of the system. In order to prevent attacks under construction, our device choice enables fast periodical security renewals.

- If an attack against the cryptographic algorithm (AES) or against our fingerprinting algorithm is discovered, our system enables easy upgrades of the broken scheme.

- Readback is a feature (*e.g.* for easy debugging) that is supplied for most FPGA designers. Nevertheless, an attack can be performed using this option. It is called "Readback Attack" and consists in reading the configuration of the FPGA in order to recover secret keys or clone the decoder itself. The attacker can also try to intercept the bitstream at the configuration step. Thanks to recent FPGA families, the readback functionality can be prevented with security bits and the configuration bitstream can be encrypted (FPGA includes thus 3-DES decryptor). Obviously, we chose such an FPGA.

Currently, only meticulous side-channel attacks can be performed to recover all secret keys. As these secret keys only concern a single movie file, this film will be hacked, but the entire system will not be compromised. It is possible to raise the cost of the physical attacks by means of tamper-resistant countermeasures. As asserted above, the high cost of DC equipment as well as the small set of theaters make it possible to deploy more sophisticated security countermeasures to prevent side-channel attacks against an FPGA. A tamper-resistant AES decryptor must be therefore recommended.

6. CONCLUSION

The first contribution of this paper concerns the achievement of an image decoder designed for Digital Cinema. The proposed architecture was a trade-off between the unpublished DC drafts and our personal expertise. We proposed an efficient AES decryption module dealing with 300 Mbps in CBC mode. We also achieved JPEG 2000 decompression and fingerprinting blocks (for 2K images, 24 fps and 36 bpp). These modules perfectly meet current Digital Cinema requirements. We also evaluated the reconfigurability and security features of our approach.

The global design was implemented in one single Virtex-II® FPGA (XC2V6000-4) that is currently available for about $4,000. It is the first solution known nowadays that efficiently integrates the global design in one chip. We are currently developing a more efficient version of JPEG 2000 block that will probably reduce the cost by a factor of about 10.

7. ACKNOWLEDGMENTS

This work has been funded by the Walloon region (Belgium) through the research project TACTILS
http://www.dice.ucl.ac.be/crypto/TACTILS/T_home.html

8. REFERENCES

[1] Analog Devices, *JPEG 2000 Video CODEC (ADV202),*, Summer 2003, [Online] Available: http://www.analog.com.

[2] K. Andra, T. Acharya, and C. Chakrabarti, *A High-Performance JPEG2000 Architecture,* IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 3, pp. 209-218, March 2003.

[3] *ASPIS: An Authentication and Protection Innovative Software System for DVD and Internet*, European project, IST-1999-12554.

[4] Barco-Silex, *JPEG2000 Decoder: BA111JPEG2000D Factsheet,* October 2003, [Online] Available: http://www.barco.com.

[5] *CERTIMARK: Certification For Fingerprinting Techniques*, European project, IST-1999-10987.

[6] Digital Cinema Initiatives (DCI), *Digital Cinema System Specification (version 3)*, Confidential draft, November 2003.

[7] J.-F. Delaigle, C. De Vleeschouver, and B. Macq, *Watermarking algorithm based on a human visual model*, Signal Processing, vol. 66, n3, May 1998, pp. 319-336.

[8] D. Delannay and B. Macq, *Generalized 2-D cyclic patterns for secret watermark generation*, in the proceedings of ICIP'00, 2000.

[9] A. Descampe, F.-O. Devaux, G. Rouvroy, B. Macq, and J.-D. Legat, *An Efficient FPGA Implementation of a flexible JPEG 2000 Decoder for Digital Cinema*, in the proceedings of EUSIPCO 2004, Vienna, Austria, September 2004.

[10] K. Gaj and P. Chodowiec, *Very Compact FPGA Implementation of the AES Algorithm*, in the proceedings of CHES 2003, Lecture Notes in Computer Science, vol. 2779, pp. 319-333, Springer-Verlag.

[11] *ISO/IEC 15444-1: Information Technology-JPEG 2000 image, Part 1: Core coding system,* 2000.

[12] *ISO/IEC 15444-3: Information Technology-JPEG 2000 image coding system-Part 3: Motion JPEG 2000,* 2002.

[13] *ISO/IEC 15444-8: JPSEC, security aspects, Part 8,* 2003.

[14] D. Kirovski, M. Peinado and F.A.P. Petitcolas, *Digital rights management for digital cinema,* Invited paper in Security in Imaging: Theory and Applications, International Symposium on Optical Science and Technology. San Diego, USA, July 2001.

[15] M. Kutter and F.A.P. Petitcolas, *Fair evaluation methods for image watermarking systems,* Journal of Electronic Imaging, vol. 9, no. 4, pp. 445455, October 2000.

[16] F. Lefebvre, D. Gueluy, D. Delannay and B. Macq, *A print and scan optimized fingerprinting scheme*, in the proceedings of MMSP'01, pp. 511-516, Cannes, France, 2001.

[17] D. Marpe, V. George, H. L. Cycon and K. U. Barthel, *Performance evaluation of Motion-JPEG2000 in comparison with H.264/AVC operated in pure intra coding mode,* SPIE Conf. on Wavelet Applications in Industrial Processing, Photonics East, Rhode Island, USA, October 2003.

[18] R. Merritt, *Compression schemes take screen test for digital cinema,* EE Times, March 31, 2004.

[19] National Bureau of Standards, *FIPS 197, Advanced Encryption Standard*, Federal Information Processing Standard, NIST, U.S. Departement of Commerce, November 2001.

[20] F.A.P. Petitcolas, *Watermarking schemes evaluation,* I.E.E.E. Signal Processing, vol. 17, no. 5, pp. 58-64, September 2000.

[21] M. Rabbani and R. Joshi, *An overview of the JPEG 2000 still image compression standard,* Signal Processing: Image Communication, vol. 17, no. 1, pp. 3-48, January 2002.

[22] R.M. Rast, *SMPTE Technology Committee on Digital Cinema-DC28: A Status Report*, SMPTE Journal, vol. 110, no. 2, pp. 78-84, February 2001.

[23] G. Rouvroy, F.-X. Standaert, J.-J. Quisquater and J.-D. Legat, *Efficient Uses of FPGAs for Implementations of the DES and its Experimental Linear Cryptanalysis*, IEEE Transactions on Computers, Special Edition on Cryptographic Hardware and Embedded Systems, vol. 32, no. 4, pp. 473-482, April 2003.

[24] G. Rouvroy, F.-X. Standaert, J.-J. Quisquater and J.-D. Legat, *Design Strategies and Modified Descriptions to Optimize Cipher FPGA Implementations: Fast and Compact Results for DES and Triple-DES*, in the proceedings of FPL 2003, Lecture Notes in Computer Science, vol. 2778, pp. 181-193, Lisbon, Portugal, September 2003, Springer-Verlag.

[25] G. Rouvroy, F.-X. Standaert, J.-J. Quisquater and J.-D. Legat, *Compact and Efficient Encryption/Decryption Module for FPGA Implementation of the AES Rijndael Very Well Suited for Small Embedded Applications*, in the second proceedings of ITCC 2004, special session on embedded cryptographic hardware, pp. 583-587, USA, Las Vegas, April 2004.

[26] G. Rouvroy, F. Lefebvre, F.-X. Standaert, B. Macq, J.-J. Quisquater and J.-D. Legat, *Hardware Implementation of a Fingerprinting Algorithm Suited for Digital Cinema*, in the proceedings of EUSIPCO 2004, Vienna, Austria, September 2004.

[27] D. Santa-Cruz, R. Grosbois, and T. Ebrahimi, *JPEG 2000 performance evaluation and assessment,* Signal Processing: Image Communication, vol. 17, no. 1, pp. 113-130, January 2002.

[28] Society of Motion Picture and Television Engineers (SMPTE), *Digital Cinema Distribution Master (DCDM) Image Structure*, Confidential draft, November 2003.

[29] F.-X. Standaert, G. Rouvroy, J.-J. Quisquater and J.-D. Legat, *A Methodology to Implement Block Ciphers in Reconfigurable Hardware and its Application to Fast and Compact AES Rijndael*, in the proceedings of FPGA 2003, pp. 216-224, Monterey, California, February 2003.

[30] F.-X. Standaert, G. Rouvroy, J.-J. Quisquater and J.-D. Legat, *Efficient Implementation of Rijndael Encryption in Reconfigurable Hardware: Improvements and Design Tradeoffs*, in the proceedings of CHES 2003, Lecture Notes in Computer Science, vol. 2523, pp. 334-350, Cologne, Germany, September 2003, Springer-Verlag.

[31] D. Taubman and M. W. Marcellin, *JPEG 2000: Image Compression Fundamentals, Standards and Practice,* Kluwer Academic, Boston, MA, USA, 2002.

[32] *USC-SIPI image database*, [Online]Available: http://sipi.usc.edu/services/database/Database.html.

[33] T. Wollinger and C. Paar, *How Secure Are FPGAs in Cryptographic Applications?*, in the proceedings of FPL 2003, Lecture Notes in Computer Science, vol. 2778, pp. 91-100, Lisbon, Portugal, September 2003, Springer-Verlag.

[34] Xilinx, *Virtex-II® Field Programmable Gate Array Data Sheet*, [Online] Available: http://www.xilinx.com.

[35] Xilinx, *Spartan-3 Field Programmable Gate Arrays Data Sheet*, [Online] Available: http://www.xilinx.com.

[36] W. Yu, R. Qiu and J. Fritts, *Evaluation of Motion-JPEG2000 for Video Processing,* Department of Computer Science, Washington University in St. Louis, Technical report, November, 2001, [Online] Available: http://citeseer.ist.psu.edu/yu01evaluation.html

APPENDIX

A. ANALYSIS OF THE FINGERPRINTING ROBUSTNESS

A.1 Deliberate Software Distortions

To assess the robustness and performance of the used fingerprinting method, we test our algorithm with 40 real-world images taken from the USC-SIPI database [32].

For each of the 40 images, we embed a message with a range of six different forces (0.02,0.04,0.08,0.1,0.15,0.2). To evaluate the image processing degradation due to the fingerprinting insertion, we calculate the PSNR means for each modified image according to the force of the mark. Fig. 6 shows the resulting PSNR means. An empirical value of 40 *dB* is a very good PSNR threshold to achieve a not too visible added template.

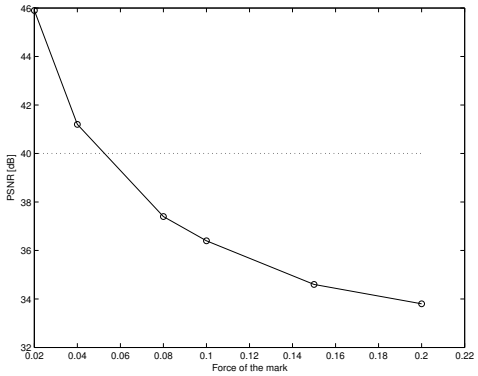

Figure 6: PSNR of 40 fingerprinted images regarding to the force of the mark

For each fingerprinted image, we consider four image processing attacks, generating $40 \times 6 \times 4 = 960$ images, named processed images. The attacks are filtering (3x3 Gaussian filtering with standard deviation of 0.5), noise (salt and pepper) and compression (JPEG compression with 80% and 60% quality factor).

The robustness results are given in Tables 7, 8, 9 and 10. The term *Extracted* represents the number of processed images where the mark is correctly detected and extracted. *Only detected* represents the number of processed images where the mark is correctly detected but too many bits are lost in the payload to compute a correct extraction. *Not detected* represents the number of processed images where the mark is not detected and thus not extracted.

Force	0.02	0.04	0.08	0.1	0.15	0.2
Extracted	29	39	40	40	40	40
Only detected	4	1	0	0	0	0
Not detected	7	0	0	0	0	0

Table 7: Gaussian attack

Force	0.02	0.04	0.08	0.1	0.15	0.2
Extracted	27	40	40	40	40	40
Only detected	4	0	0	0	0	0
Not detected	9	0	0	0	0	0

Table 8: Noise attack

Force	0.02	0.04	0.08	0.1	0.15	0.2
Extracted	30	39	40	40	40	40
Only detected	3	1	0	0	0	0
Not detected	7	0	0	0	0	0

Table 9: JPEG attack, quality=80

Force	0.02	0.04	0.08	0.1	0.15	0.2
Extracted	26	37	40	40	40	40
Only detected	3	3	0	0	0	0
Not detected	11	0	0	0	0	0

Table 10: JPEG attack, quality=60

Attacks and PSNR figures provide a good illustration of the watermarking force (close to 0.06), necessary to obtain a good trade-off robustness/visibility of the fingerprint. Nevertheless, this robustness evaluation is not fair with the real piracy act based on illegal camcorder recording. In fact, our insertions scheme is perfect for affine transforms. Nevertheless, our scheme can suffer from projective transforms. A fair evaluation of robustness should be based on papers [15, 20].

A.2 Camera Captures of Projected Fixed Images

Fig. 7 illustrates the major cinema piracy theft: the camcorder capture and duplication issues. Distortions occur in the pixel values and boundaries, and in the image geometry. The distortion of pixel values is caused by the luminance, contrast and chrominance variations. The distortion of pixel boundaries is due to the blurring of adjacent pixels. These are typical effects of projectors and camcorders, and cause perceptible changes of the visual quality to the illegal movie file. The geometric distortion of the movie comes from the shape of the theater screen and the position of the camcorder in the projection room.

In order to evaluate the proposed watermarking scheme, some tests have been performed with a projector where we intentionally limit the projective deformations. The pictures were projected using a flat screen with no deformation.

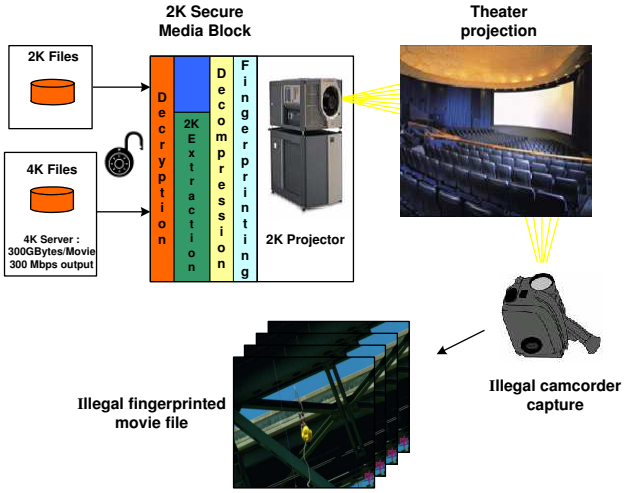

Figure 7: Digital Cinema camcorder capture and duplication issues

After some camera shots, the captured pictures are resized, cropped and manually re-distorted, using image processing softwares. Transformed images are then compressed in JPEG. The conclusion is that we mostly extract correct watermarks. Further experiments have therefore to be carried out in order to better asses the watermarking robustness with projective transformations.

As examples, next figures depicts one successful experiment of the camcorder capture. Fig. 8 and 9 respectively show the original and fingerprinted images while Fig. 10 illustrates the camcorder capture (with a good JPEG quality factor) of this projected and fingerprinted image. The conclusion for this image is that this fingerprinting process is resistant against such transformations. The invisibility of the fingerprint is also noticeable. The mark also resists a deeper JPEG compression with a 10% quality factor, as shown in Fig. 11.

Figure 8: Original image
Source: Shrek, Universal Studios, 2000

Figure 9: Fingerprinted image

Figure 10: Camcorder capture of the projected image

Figure 11: Camcorder capture compressed to a 10% quality factor