Video Watermarking For Digital Cinema Contents

Sadi Vural, Hiromi Tomii, Hironori Yamauchi
Ritsumeikan University, Department of Information Science,
1-1-1 Noji-higashi, Kusatsu-shi, Shiga-ken, Japan
Email : {svv21002,re009994 ,yamauchi}@se.ritsumei.ac.jp

Abstract— With the advent of digital cinema and digital broadcasting, copyright protection of video data has been one of the most important issues.
We present a novel method of watermarking for video image data based on the hardware and digital wavelet transform techniques and name it as "traceable watermarking" because the watermarked data is constructed before the transmission process and traced after it has been received by an authorized user.
In our method, we embed the watermark to the lowest part of each image frame in decoded video by using a hardware LSI.
Digital Cinema is an important application for traceable watermarking since digital cinema system makes use of watermarking technology during content encoding, encryption, transmission, decoding and all the intermediate process to be done in digital cinema systems.
The watermark is embedded into the randomly selected movie frames using hash functions.
Embedded watermark information can be extracted from the decoded video data. For that, there is no need to access original movie data.
Our experimental results show that proposed traceable watermarking method for digital cinema system is much better than the convenient watermarking techniques in terms of robustness, image quality, speed , simplicity and robust structure.

Keywords— Decoder, Digital content, JPEG2000 Frame, System-On-Chip, traceable watermark, Hash Function, Wavelet.

1. Introduction

WITH the rapid spread of the Digital world in the field of movie Industry, many companies are starting to develop equipments for digital cinema systems. Lately, Olympus Corp has developed digital video camera (SH-880TM) with 8Million pixels [9] and Victor Corp developed D-ILA projector (DLA-HD2K) with 8million pixels compatible [10].
In addition to two companies given above, NTT incorporated, Japan continues R&D using fiber optic networks for Digital Cinema networks and systems [11]. While companies are working on, moviemakers in Hollywood are also starting to change their current novel methods from analog tapes to digital DVDs and/or Digital Medias at the crossway to digital. Digital Cinema initiatives in US work on specifications and standardization for digital cinema [8]. In recent days the encoding specifications have been standardized as ISO/IEC 15444-1:2000 Information Technology-Jpeg2000 [4] [5].
Since far, many digital watermark techniques have been proposed for digital cinema as a protection method [1] [2] [3] and many papers have been published and researches still continue to find some security solutions for Digital cinema [6][7]. However, none of those is satisfactory for the either digital cinema content providers or digital cinema clients. It is fundamental that the watermarking be robust against to every signal processing methods and must be difficult to remove when an attack has occurred. But the current methods are fragile to attacks. Some methods are robust enough but the image is distorted by embedded watermark data.
Based on those, we propose traceable watermarking method. We embed watermark at transmitter side as well as at Receiver side and then trace the watermark to make system sync work.
In this research, we put the watermark twice to trace the video data not only during the play at projection but also during the data transmission, encoding and during the download process from Digital Cinema content server.
The brief digital cinema architecture will be discussed at [2]. The [3] gives the further details on proposed watermarking techniques including concrete design of encoder, decoder, traceable watermarking technology, consequently.
The chapter [4] gives the experimental results of our research.
The following chapter [5] will give a simple conclusion of the entire research and the last chapter is reference chapter.

2. Digital Cinema System Architecture

A. Entire Digital Cinema Stage

Digital Cinema is complete Hardware/Software systems which make its users enjoy full-length noise free moving pictures and high resolute cinema-quality in their homes using some digital technologies over the high-speed networks.
The Digital Cinema system delivers digitized, compressed, and encrypted movie contents to its users using some Electronic transmission methods. In Japan, High-bandwidth fiber optic cables for internet and cable TV are commonly used. With its use for Digital Cinema, clients can enjoy watching movie, get news from live broadcasting with high resolute view..
Security is another major issue for digital cinema systems since many problems come out while tape-based movie contents are replaced by digital-based contents.
Main security problems are such like data hacking, dubbing, reproduction of the licensed movie, external access to the client server and internal attackers. To come over those problems, we construct a total cinema system where it is formed by Data

Transmitter and Data Receiver by using hardware components as seen at Fig 1.

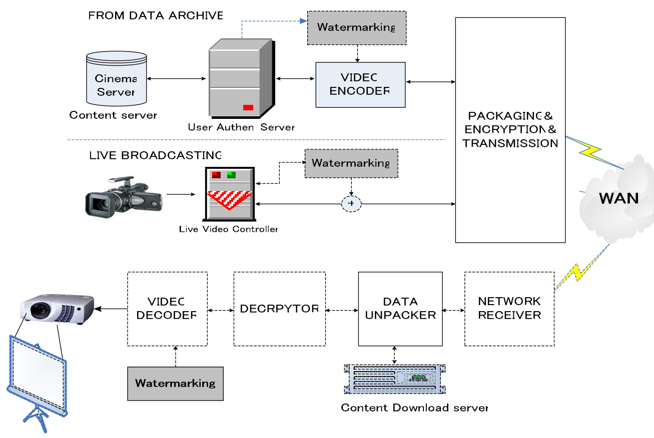


Fig 1 Digital Cinema system

As seen at Fig 1, there is a Cinema Server, where the content data is kept. This server includes a RAID system and it has some large storage where movie contents are stored. The service of Cinema Server can also be renamed as Video-On-Demand (VOD). Another service which digital cinema system provides is for live broadcasting service. For that, we need a high resolution Digital Video Camera placed which is placed outside at Fig 1 above. Using it, the broadcasting data from camera is directly transmitted to the client side. Client is the service user. The data is controlled by a digital video data controller which provides an interface between the digital camera device and encoder & transmitter interfaces as seen at Fig 1.
Authentication server connected to the Cinema server authenticates both the client who put a request to the server and the transmitter, which is responsible for requested content transmission. Authentication sever takes important role when the client use the cinema system.
The transmitter is a one-chip LSI, which is used for data encoding, embedding watermark data, encryption and any other sub-processes needed during the transmission like data packing, load balancing of the network, data protocol selection.
Likewise the transmitter, the Receiver is another one-chip LSI, which is built in receiver circuits. It decompresses, decodes, decrypts, and re-embeds the traceable watermark into a very carefully calculated position on image. Receiver operates at user side which has a direct connection to download server to save the downloaded content. Default for receiver is to transfer the data to the projector to watch.
The content data at download server is not possible to watch prior to decoding since a series of authentication, evaluation, decoding must be done before playing the content. For each play of the content from Download server, a new authentication with the server is required

3. OUR PROPOSED WATERMARKING SOLUTION

The Encoder LSI primarily handles on several works such as the embedding watermark to the encoded content, Encoding, encryption, compression, synchronization, packaging, network authentication. The watermark embedded at encoder side protects the content from the network attackers or hackers during the content transmission while the watermark embedded at Decoder side protects the media from content stealing and illegal dubbing.
Watermarking data consists of the Content Administration ID, company name of the content supplier's and the content owner. Watermark is inserted to the sub bands of the content frames using DWT. Since the watermark embed does not vary for each user, the load of encoder is light, which makes encoder LSI run quick enough.

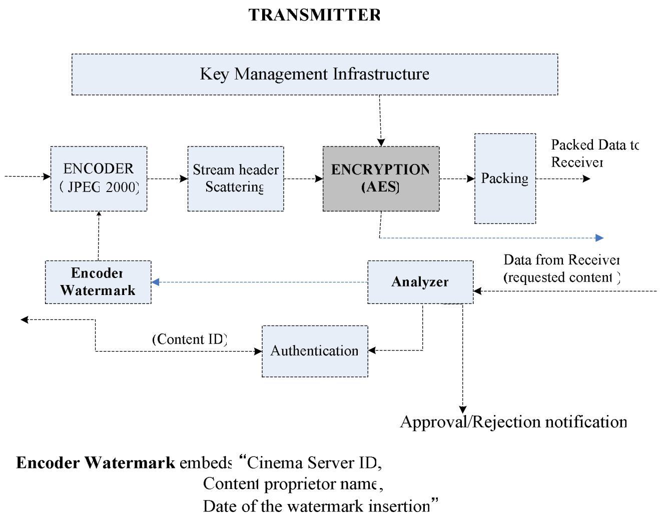


Fig 2 Transmitter LSI with encryption method

JPEG2000 compatible transmitter is responsible for inputs from both the digitalized data from the Cinema server and watermarking data at the same time. The plain content and Watermark data are added inside the Encoder by our Crc-32 traceable watermarking method, which will be further explained at chapter "3" (fig 2).
Transmitter makes an output for watermarked content. The watermarked content is made an input to a SHS (stream header scattering) so that frames are randomly distributed on the entire contents. Information for watermarking to embed at transmitter part is restricted into cinema server's identification number, Content Proprietor name, and Date of Watermarking insertion. It is possible as large as 256-byte per each frame.

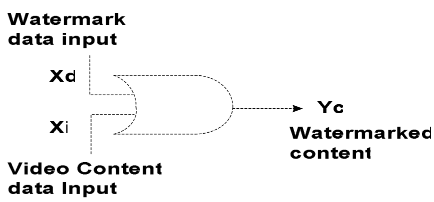


Fig 3 Logic of the Watermark embed

1 *Proposed traceable Watermarking*

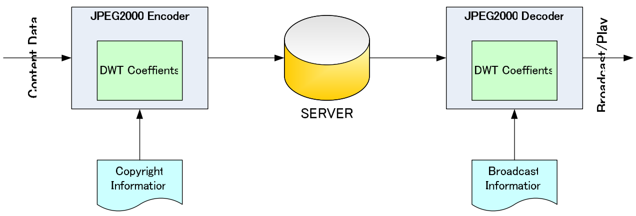


Fig 4 Traceable watermark application

The basic structure of our proposed traceable watermark is shown at Fig 4. According to the figure, the contents of watermark are the copyright information at transmitter side and the broadcast information at receiver side. It is important that constant information such as transmitter ID, GPRS information of the transmitter, content ID is embedded into the video content to keep the transmitter load light. Doing it, the watermark to be embedded does not change for each user. Assume that content information is embedded with different watermark information. Then the transmitter is heavily loaded and the data is delayed which causes a significant drop at overall system performance. However, watermark information embedded at receiver side is unique to each user. That does not affect the system since each user has one processor. The watermark information to embed into the receiver side is the broadcast information as shown at Fig 4. We embed the watermark into LL subbands and divide embedded subbands into the code blocks using the DWT at transmitter side. Receiver side is useful to embed due to the illegal recordings during play. Because data dubbing at receiver side is another problem. The basic algorithm for data embed is shown at Fig 6-(a), (b) and its embedding method by hash functions is given at Fig 5

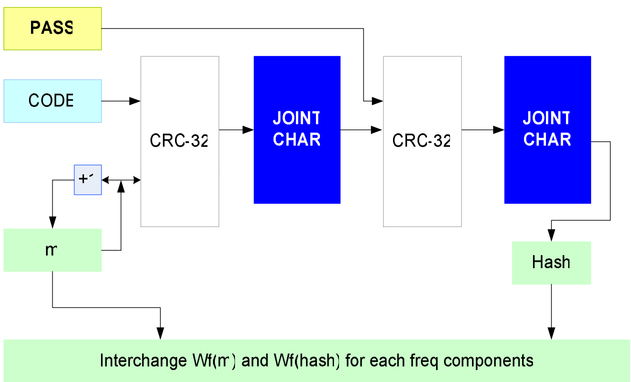


Fig 5 Transverse using CRC-32 Hash function

At Fig 5, by using the hash function, we execute the traceable watermarking. Hash Function generates constant length data from the input data. Obtaining the original data from hash data is almost impossible so showing its robustness against any attack. SHA and MD are also robust but they need a series of complicated calculations. We use CRC32 of the RFC1662. The input for CRC32 is called as "strings", which has a variable string length and generated 32-bit hash is called "CRC (string)"

2 RNG Based watermarking embedding

Fig 6-(a) gives a general representation for Motion JPEG2000 movie frames. RNG generates some random numbers for the automatic frame selection while Fig6-(b) shows the frames in terms of frame's sub-bands. We use the low frequency levels of the image where is given as LL2, LH2, HL2, and HH2.

The watermark is embedded into the image subbands after two subdivisions of image frames. The second subdivision is low frequency region. The reason to work in low frequency regions is because the low frequency levels of the image are robust against the common geometrical attacks. However it is also true that image is distorted at high frequency levels but a secure watermarking is possible. We select the frequency region so that we get no disturbance at image and robust against the attacks.

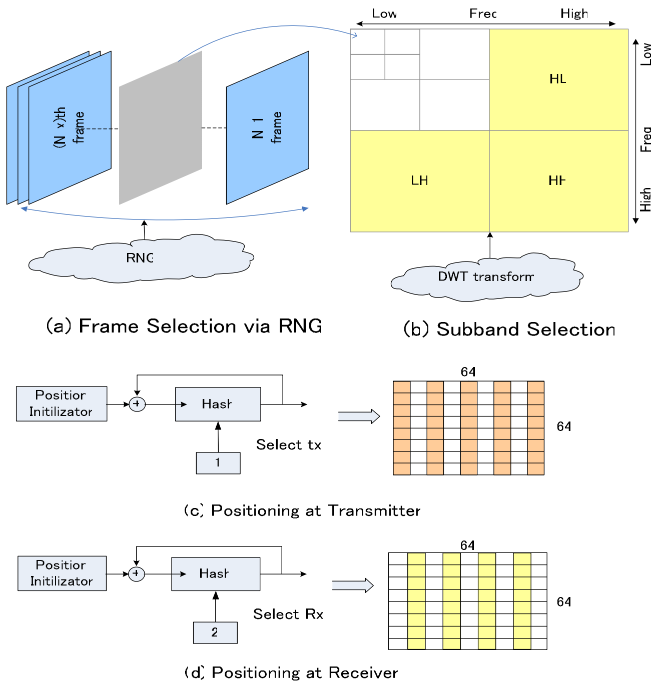


Fig 6 Watermarking Algorithm

[A] Positioning for the embedding

Fig6-(c) right side is the method of how we embed the watermark into the content. The left side of the (c) is the position of the watermark. First, a 4-16 digit Hash key is decided and its 4x4 representation is drawn as seen at Fig 6-(c) right side. For each hash key, the 4x4 data cells are interchanged so that the original location of the watermark is not determined.

At Fig 6-(d), the same procedure as given at Fig 6-(c) is done for Receiver. It is because the watermarking information embedded at transmitter side is not distorted or overwritten by the embedded watermark at receiver side. Therefore we use single blocks at transmitter and even blocks at receiver. We embed the watermark at decoder side to follow where and when the content is played and we embed it at encoder side to prevent some unexpected effects done to the decoder side and those watermarks are embedded at once and at the same time.

To recover the watermark information from image, the hash key is assigned in reverse and for each hash key, 4x4 data cells are interchanged in opposite way. At Fig 6-(c) and Fig 6- (d), position initializator determines the coordinate (xe,ye) for encoder and (xd,yd) for decoder. It is the position where the watermark information is embedded via Hash function. 64x64/2=2048 dot (256byte) can be embedded for both Decoder and Encoder. It is 128 byte for encoder and 128 byte for decoder part, which gives a total 2048 dots.

[B] Embedding Strength

Encoder is embedded into the odd numbers of the sub-band and decoder is done into the even numbers. This is given as below

$$L=(N_x \times N_y)/2^{2n},(0 \le x < N_x/2^n),(0 \le y < N_y/2^n) \quad (1)$$

Where L is the maximum number of dots to be embedded.

A simple formulation of the above hash function used for traceable watermarking is also given at 2. To compute it,
First, we have to decide the position using the threshold value T.
As a given value T, below threshold condition must be satisfied.

$$norm(m) \ge T \quad (2)$$

Where

$$norm(m) = \sqrt{W_{HL}{}^2(m) + W_{LH}{}^2(m) + W_{HH}{}^2(m)} \quad (3)$$

And using

$$tmp = (\text{int})[W_{LL}(m)/Q] \quad (4)$$

Where (int) is cut-off integer and Q is embedding intensity.
Here we use the following concept;
Set tmp "old number" if Watermark information is 0,
Set tmp "even number" if Watermark information is 1.

Then $W_{LL}(m) = tmp \times Q$ (5)

And using the equation 5 in addition to the 4,

$$m = m + Num, Count += count \quad (6)$$

Embedding string array to the frame is done as shown at Fig 6-b. By Positioning of the each component using the hash key from the reverse order of the method given at Fig 6-(d), we get the original watermarking.

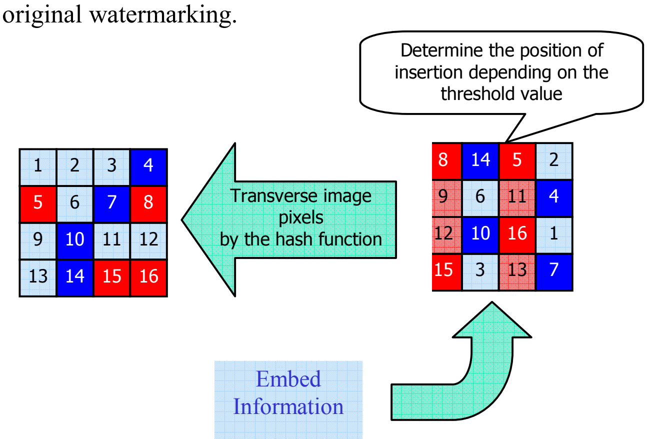


Fig 7 Watermark insertion via hash function

As an example of the watermark embed, please see the Fig 7. We first change the image into the wavelet, extend each frequency components using hash function and calculate the value from (2) and obtain the watermark.

2 *Architecture of encoder*

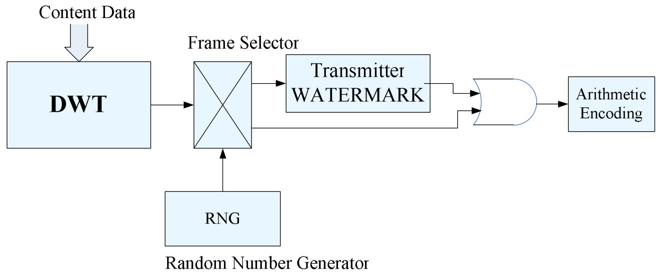


Fig 8 Watermarking at Transmitter

Fig 8 is shows encoding process, which is a part of transmitter. JPEG2000 based DWT coefficients are separated into the code blocks and each frame sub-band is divided into the same size (64x64). Multiplexer (Frame selector) simply decides the content frames whether to insert watermark. RNG decides if watermark must be put into the frame. RNG randomly generates a series numbers with its high calculation algorithms. Finally, the result is applied to the AE (arithmetic encoding).
From Fig 8, we only embed watermark to random frames using RNG information not only for playing but also for the user or client is authenticated user.

3 *Architecture of Decoder*

After the watermarked content has been downloaded, it is either saved into the user server or directly applied to the Decoder LSI for projector.

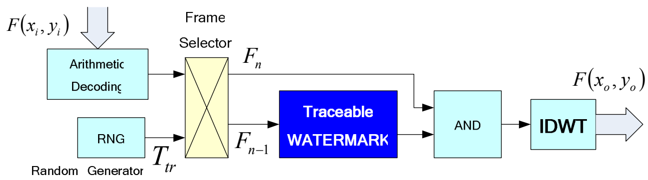


Fig 9 watermarking at Receiver

The content inputs to the Arithmetic Decoding (AD) block. RNG must be synchronized with transmitter RNG. So, we have to use a trigger for synchronization. Finally, Mux decides if frames will be watermarked. Should watermarked frames be detected, traceable watermark is inserted. If no watermarked frames are found, it is bypassed to IDWT to recover the frames.

$$\begin{cases} Hash(F(x,y) \times T_{tr} \times (n-1)) & if \ldots F_n \\ Hash(F(x,y) \times T_{tr} \times (n)) & if \ldots F_{n-1} \end{cases} \quad (7)$$

According to the 7, if it is even frame, F_n th frames are embedded with watermark. Else, watermark is embedded to the F_{n-1} th frames. Receiver LSI gets the Hash key and inserts 2nd watermark. So, embedding process is fully handled with HW implementations.

4. EXPERIMENTAL RESULTS

Experimental results show that proposed method is robust against any image processing.

We did geometrical attacks (cut, crop and trim the one part of a random selected frames, flip) and signal processing attacks (noise, hulman filtering, increase/decrease image quality, compress/decompress, apply FFT, DCT transformations).

Tile size of 2560x2048 MotionJPEG2000 is used. For the simplicity, we used 512x512 gray-scale images and divided into 5 subband levels via wavelet transform. The Lowest subband is 16x16. The total character size is 256byte to embed, which means entire subband is used. The results are shown at Fig 10-b:

Fig 10 Lena Image (512x512)

We observed the embedding intensity and the image quality and observed the changes on the image quality during our watermark insertion into the image sub bands. We learned how efficient our proposed method is during the watermark insertion and extraction. We set embedding intensity coefficient Q to 5 and we set the level to 3 and 5.

For experimental purposes, we also increased the watermark information to 512byte at level 3 and we got high BER ratios and the image was distorted with high compression rate and 512byte information which is not allowed for 512x512 images under normal conditions and QL=3 is not applicable for digital cinema images.

Table-1 BER values with Intensity

JPEG	Comp rate[%]		2	4	6	8	10	12
	(PSNR[DE])		24.37	29.23	31.77	32.84	33.64	34.41
	Q	3	46.87	25	40.62	46.87	49.21	14.06
		5	50	15.62	0	0	0	0
		7	37.5	6.25	0	0	0	0
JPEG2000	Comp rate[%]		5	7	9	11	13	15
	(PSNR[DE])		33.51	35.00	36.06	37.20	38.14	38.80
	Q	3	42.96	21.87	19.53	14.84	9.375	3.906
		5	25.06	3.906	3.125	1.562	0	0
		7	41.40	0	0	0	0	0

Above table shows the experimental results for JPEG and JPEG2000 compression in accordance with PSNR and Quantization Level (QL). It has been approved at digital cinema experiments that 5% compression rate for an image is satisfactory enough for the quality of digital cinema [12]. Hence, the results for QL≥5 satisfy the digital cinema requirements which also means that QL=3 is ignorable. Our experiments shows Jpeg2000 compression gives better results compared with JPEG images and there is almost no error for QL=5 and 7.

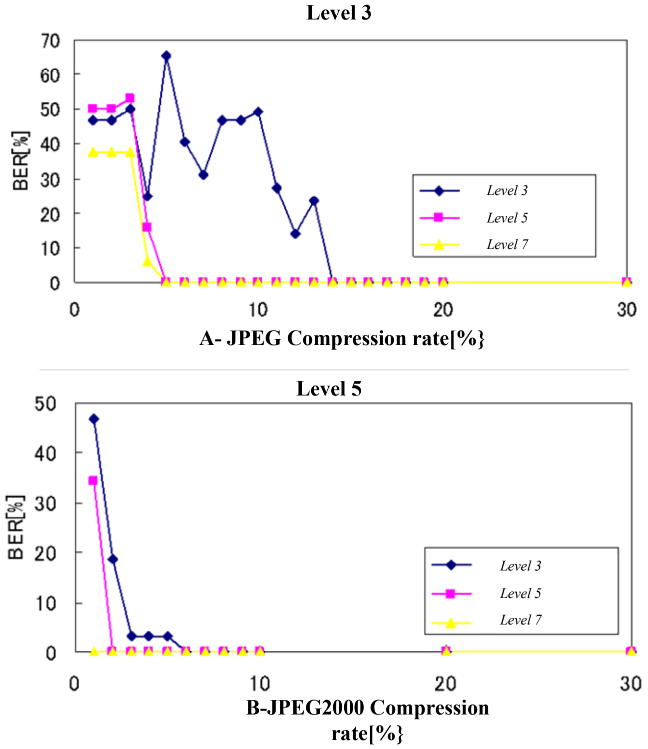


Fig 11 Embedded Data under Compression

At Fig 11 A-B, it is clear that when compression rate is increased, BER is decreased Especially for JPEG 2000 compression, the result becomes almost zero for further compression rates. Fig 11 gives that 5% of compression rate has an ignorable BER and it is feasible to make it zero by error correction. We continue tests using Stirmark and Checkmark programs to further investigate how robust our algorithm is. Some tests using Stirmark are given at Fig 12. Fig 12 (a-d) shows signal processing attacks. Images are applied some transformations based on the signal processing effects.

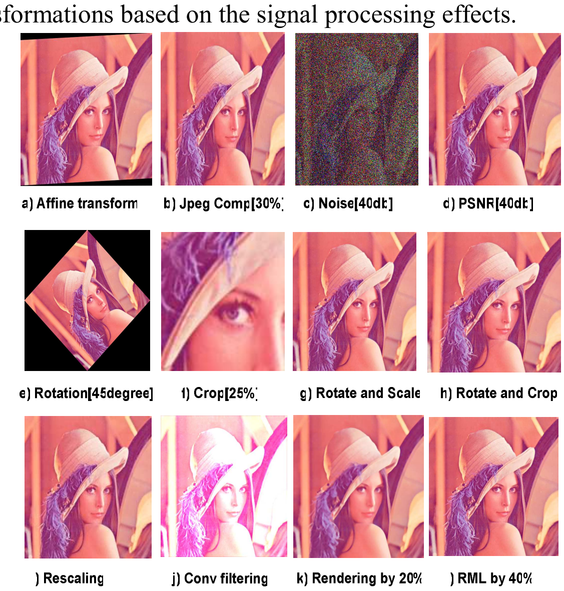
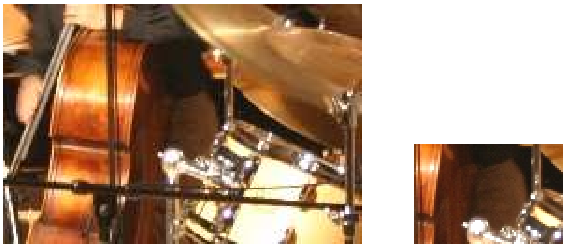


Fig 12 Stirmark test results

Fig 12 (a) is affine transform. (b) is Jpeg compression where the image is compressed by 30%. (c) is a noise addition. Here, we add noise and reduce color. Fig 12 (e-i) is geometric transform.

The target is to change the image size, rotation, crop and trim which relates of physical effects on images. The rest of the images apply special transformations.
Fig 13 is one frame image of live concert. It is watermark embedded frame. Fig 13 (a),(b) are given as a result of cropping the frames into small pieces. The watermark is kept inside. No part of watermark information is removed after cropping.

(a) Small part is cropped (b) Some part is cropped



(c) Significant part is cropped (d) almost all cropped

Fig 13 Image Crop Attack

Image is cropped more from (a) to (d). (d) is almost cropped and it is hard to recognize the image. But the watermark we embed is still visible and obtainable.

(a) Rotate by 5% (b) Rotate by 10%

(c) Rotate by 30% (d) Rotate by 90%

Fig 14 Rotation attack

Differing from Fig 13, Fig 14 gives an attack using rotation techniques. Most of watermarking technology starts failing after 30% rotation. Using our method, it is not impossible to get the watermark and distort the image. All of those tests results done as shown at Fig 11-13 show that our traced algorithm is robust enough against to signal transformations, geometric transformations and filtering effects.

5. Conclusion

In this work, we have proposed traceable watermark techniques based on the DWT for an application of digital cinema systems and confirmed that the proposed watermark method is robust enough against to signal processing attacks. The most general basic structure of Traceable watermarking is that the watermark information embedded before transmission and the watermarking information after transmission are kept synchronous and even if one side of watermarking were distorted, broken or changed, decoder LSI will never decode the content. If the watermark is attacked at receiver side, the encoder LSI will understand what has happened and stop transmission immediately.
Based on our tests and structural building of our algorithm, we can say that our watermarking method is robust and safe enough We will further expand our experiments to the digitalized high-vision movie for its further spread out in the industry and test our algorithms using the recompiled Stirmark program and Checkmark for not only JPEG2000 motion pictures but also for MPEG4 more intensively.

References

[1] Akio, Miyazaki, “Digital Watermarking for images”. IEICE Transactions. Fundamentals, Vol.E85-A,NO.3 March 2002, pp. 2.
[2] N. J. Mathai, D. Kundur and A. Sheikholeslami, "HW Implementation Perspectives of Digital Video Watermarking," IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 925-938, April 2003
[3] Hisashi. Inoue, “A Digital Watermark method using the Wavelet Transform for Video Data” , *IEICE Trans.Fundamentals*,Vol.E83-A,No.1 Jan2000.
[4] Suzuki, Junshi, “JPEG2000 Technology” by *Ohm Publishing,* Jan 2001.
[5] Rohm Corp, “Jpeg2000 Coder LSI ” http://wwww.rohm.com
[6] Xilinx Corp, “.Digital Cinema Applications” http://www.xilinx.com
[7] “Rijndale” http://www.esat.kuleuven.ac.be/~rijmen/rijndael/
[8] Digital Cinema Initiatives “ Digital Cinema System Specifications v2.0”, 2003 , http://www.dcci.com
[9] Olympus Corp, “R&D Center, IS Division Project , Planning Group”
[10] Japan Victor Corp “ILA Center Division” http://www.victor.co.jp
[11] NTT Telecommunications “Yokotsuka R&D Division” http://www.ntt.co.jp
[12] NTT Electronics "Digital Cinema quality" http://www.ntt-west.co.jp

Sadi Vural was born at Corum/Turkey and after getting his B.S degree in Istanbul University at 1997, He started to Science and Information Technology of Ritsumeikan University Kyoto/Japan. He got his M.S at 2000 and he is now studying for Ph.D Degree while working for Takumi vision Technologies, Inc,Osaka/Japan.

Hiromi Tomii has obtained her B.S from Ritsumeikan University at 2003 and continued for M.S degree in the same university. She joined at Yamauchi Research room and did researches in the field of Watermarking technology. After she obtained her M.S degree at 2005, she left University to work. She is now working for Konica Co.Inc Tokyo/Japan
Hironori Yamauchi was born at 1950 in Fukui-ken/Japan. After he obtains his M.S from Tokyo University at 1975, he started to work for NTT Corp.
He joined at Ritsumeikan University Kusatsu/Japan in 1996. He is currently a chairman of Rohm Plaza, an LSI Design cenrter.
His field covers Multimedia image, Hardware design, VLSI development and Medical imagings. He is a member of IEEE Society.