Traceable Watermarking System using SoC for Digital Cinema Delivery

Sadi Vural, Hiromi Tomii, Hironori Yamauchi

***Abstract*—**As the development of digital technology is increasing, Digital cinema is getting more spread.
However, content copy and attack against the digital cinema becomes a serious problem. To solve the above security problem, we propose “Additional Watermarking” for digital cinema delivery system. With this proposed “Additional watermarking” method, we protect content copyrights at encoder and user side information at decoder. It realizes the traceability of the watermark embedded at encoder.
The watermark is embedded into the random-selected frames using Hash function. Using it, the embedding position is distributed by Hash Function so that third parties do not break off the watermarking algorithm.
Finally, our experimental results show that proposed method is much better than the convenient watermarking techniques in terms of robustness, image quality and its simple but unbreakable algorithm.

***Keywords*—** Decoder, Digital content, JPEG2000 Frame, System-On-Chip and additional watermark.

I. INTRODUCTION

With the rapid spread and the high demand to the Digital Cinema, *Olympus Corp* developed digital video camera (SH-880TM) with 8Million pixels [9] and *Victor Corp* developed D-ILA projector (DLA-HD2K) with 8million pixel compatible [10].
On the other side Japan the biggest telecommunication company, *NTT* continues researches and experiments using fiber optic networks for the Digital Cinema networks and systems [11].
In addition, many moviemakers in Hollywood are looking for any probability of digital cinema [12] at the crossway to digital. Moreover, Digital Cinema initiatives generate specifications for digital cinema and its usage [8]. Recently the encoding specification has been decided as ISO/IEC 15444-1:2000 Information Technology-Jpeg2000, a superior algorithm [4][5]. With this rapid grow security and legal issues like the protection of the owner copyrights have become more and more important. Since far, many digital watermark techniques have been proposed for digital cinema as a protection method [1][2][3] at recent years and many papers are published as a solution of security at Digital cinema [6][7].
However, none of those methods is satisfactory for the digital cinema clients. The watermark must be robust for several common signal processing and difficult to remove for an attacker for providing a modern protection of the video content. Based on this, we propose the additional watermark method.
According to the additional watermarking method, the watermarking embedded is continuously monitored at Encoder and Decoder side so that the watermarking for both sides is strictly kept under control.
We put watermark into Encoder and Decoder separately using style will adjust your fonts and line spacing, completely new algorithm “additional watermarking”.
In this research, we put the watermark twice to protect the image not only during the play at projection but also during the data transmission and download from Digital Cinema System.
The watermark method is based on DWT (Discrete Wavelet transform), which does not require the original image for recovery process. The content is JPEG2000 compatibility.
Also, our embedding method uses CRC-32 technology. Hash function is a perfect embed method. It is because the watermark cannot be obtained from Image. However it is so simple and quick in case someone knows the hash key. The hash key is sent to the decoder side using secured and encrypted networks. So it is practically impossible to obtain from the network which is used during the media and movie content transmission.
The brief digital cinema delivery system will be discussed at [II]. The [III] gives the further details on proposed watermarking techniques including concrete design of encoder, decoder, additional watermarking technology, consequently.
The chapter [IV] gives the experimental results of our research.
The following chapter [V] will give a simple conclusion of the entire research and the last chapter is reference chapter.

S. V. is with the Science and Information Technology of Ritsumeikan University BKC Campus Kusatsu/Japan (phone: +81-90-1958-8949; fax: +81-72-675-4806; e-mail: svv21002@se.ritsumei.ac.jp).
H. T. was with Science and Information Technology of Ritsumeikan University BKC Campus Kusatsu/Japan. She now works for Konica Co. Ltd (phone: +81-775-671-1111,, email: tomii@hotmail.com.
H. Y. is with the VLSI Center of Ritsumeikan University BKC Campus Kusatsu/Japan (e-mail: yamauchi@se.ritsumei.ac.jp).
He is now the director of Rohm Plaza where LSI design and FPGA circuit design are done for educational as well as business purposes

II. DIGITAL CINEMA DELIVERY SYSTEM

A. *Entire Digital Cinema Stage*

Digital Cinema is a complete system delivery to deliver full-length noise free motion pictures, in addition to the other visual "cinema-quality" programs to users throughout the world using some digital technologies over the high-speed networks.

The Digital Cinema system delivers digital movie contents digitized, compressed, and encrypted to users via Electronic transmission methods, such as satellite, multicast methods, Fiber optics, WAN (Wide Area Networks) and LAN.

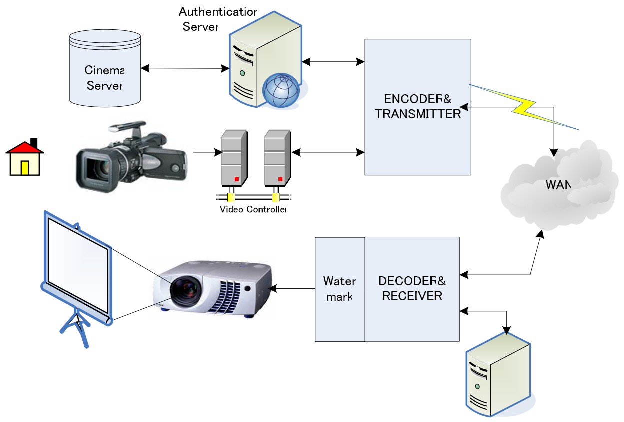

Fig 1 Digital Cinema Delivery system outline

There is a Cinema Server, which consists of the contents. This server should be provided in some amounts so that the huge amount of movie contents should be stored. The service, which is provided from Cinema Server is also knows as VOD. Another service is for live broadcasting from Digital Video. Camera. Using it, the broadcasting data from a high-resolution digital video camera is directly transmitted to the user side. The data is controlled by a video controller which provides an I/F between the digital camera and the encoder & transmitter I/F.
The File Server administrates the raw data of Cinema server. It maintains the content by indexing and reordering each content frame and makes a database with the high-speed seek features.
The authentication server in addition to the file server is a security interface between the transmitter and Cinema Server.
The transmitter is a One-chip LSI, which does encode, embed watermark, encrypt and any other sub-process for transmission.
The output terminal of the Encoder is connected to the high-speed network, which can be external gigabit WAN network, fiber-optic or an equal network for transmission.
The Receiver is another one-chip LSI, which uncompresses, decodes, decrypts, and embeds the additional watermarking. It is at the user side and directly connected to a server to save downloaded data and to the projector.

The content data at local disk is not possible to play prior to decoding. Because playing the data requires a series of authentication, evaluation, decoding. For each play of the content, a new authentication with the server has to be taken on.
The Projector to fulfill the Digital Cinema initiative's specifications is used for converting the digital data into the light. It not only displays the movie content on the screen, but also shows movie sub-titles, open captioning, user information.

III. Proposed Watermarking Technique

The Encoder SoC primarily handles on several works such like the embedding watermark to the encoded content, Encoding, encryption, compression, synchronization, packaging, network authentication. The watermark embedded in encoder side is done to protect the content from the network attackers or hackers during the content transmission to the user side.
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 operation of encoder LSI is done quickly and speedy

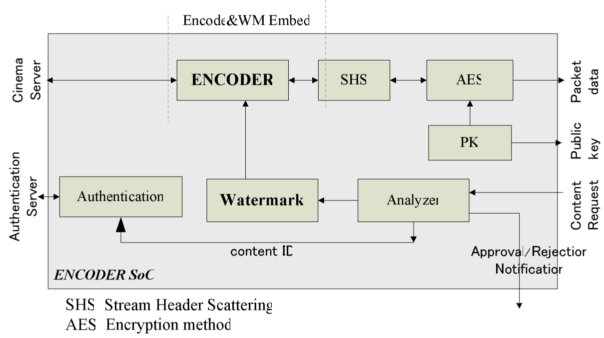

Fig 2 Encoder and Watermarking LSI with encryption method

JPEG2000 Encoder gets inputs from both the digitalized data from the Cinema server and watermarking data at the same time. The intricate Content and Watermark are added inside the Encoder by our Additional watermarking method, which will be further explained at chapter "3").
Encoder outputs a watermarked content and it is applied to a SHS (stream header scattering) so that frames are randomly distributed over. It is then encrypted by AES with 256bits.

Watermark information to embed at encoder side is Cinema Server ID, Content Proprietor name, and Date of Watermarking insertion. It is possible as large as 256-byte per each frame.

1 *Proposed Additional Watermarking*

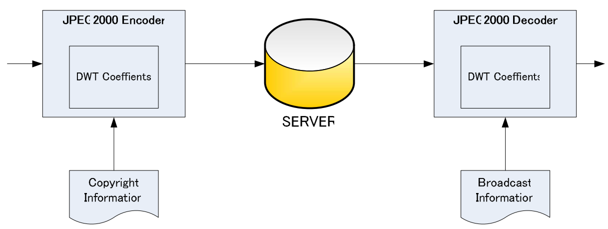

Fig 3 Additional Watermark based digital cinema delivery

The basic structure of our proposed additional watermarking at digital cinema delivery system is shown above at Fig 3. Here, The watermark is copyright information at encoder and broadcast information at decoder. We embed the watermark into the frame LL sub bands and then divide embedded sub bands into the code blocks using the DWT at both encoder and decoder. The basic algorithm for embedding it is shown at Fig

5-(a), (b) and its embedding method is given as below at Fig 4

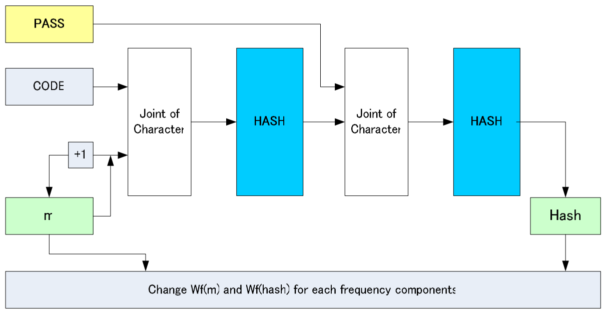

Fig 4 Methodology of Additional watermarking using Hash

At Fig 4, by using the hash function, we execute the additional watermarking. Hash Function generates constant length data from the input data. Since obtaining the original data from hash-generated data by arithmetic calculations is almost impossible so showing its robustness against any attack. SHA and MD are also powerful methods but they need a series of complicated calculations, which makes entire process slow. As Hash Function, we used CRC32 of the RFC1662 FCS. The input for CRC32 is called as "strings", which has a variable string length and generated 32-bit hash is called "CRC (string)".

1.1 Watermarking Algorithm

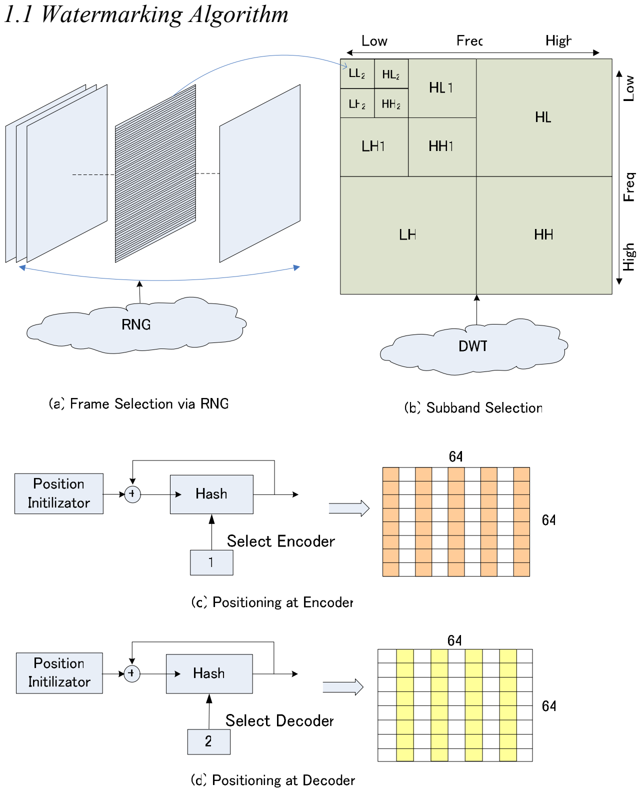

Fig 5 Watermarking Algorithm

[A] Positioning for the embedding

At Fig5-(a) an RNG generates random numbers to be a basis of automatic frame selection while Fig5-(b) shows the frame in terms of sub-band position. The frame is embedded after its 2nd division into the sub-bands. The second level is LL_2, LH_2, HL_2, and HH_2 as seen at the top. Fig5-(c) right side is the method of embedding watermark into the content. The left side of the (c) is the position of the watermark. We decide a Hash key and re-draw the left box in one-dimension like 4x4 representation of the box. For each hash key, the 4x4 data cell is interchanged. Finally, watermark is embedded in random order. To recover it, the hash key is assigned in reverse so that data is feed-backed. At above, position initializator determines the coordinate (x_e,y_e) for encoder and (x_d,y_d) for decoder. It is the position of where to embed the first data at content frame depending on the Hash function. For encoder 64x64/2=2048 dot can be embedded. This is approximately equal to 256byte for both Dec and Enc.

[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

$$L = (N_x \times N_y)/2^{2n} \qquad (1)$$

Where L is the maximum number of dots to be embedded.
A simple formulation of the above hash function used for additional 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.

$$norm(m) \geq T \qquad (2)$$

Where

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

And using

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

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),

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

Embedding string array to the frame is done as shown at Fig5-b. Following the opposite way of the Positioning of the each component using the hash key from the reverse order of the method given at Fig 5-(d), we get the original watermarking.
At fig 5-d, position initializator extracts the exact location for new watermark-embed. Hash calculates a new key and loops the values.
The block "2" shows the watermarking-embed is used for decoder side. Hence watermark-location embedded at encoder side is protected and new location is allocated for decoder.

2 *Concrete design of encoder*

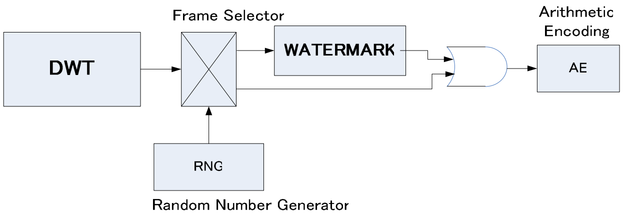

Fig 6 JPEG2000 Encoding with watermark

Fig 6 is encoding part compound from JPEG2000 DWT and AE (arithmetic encoding) with watermarking using RNG.
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. The condition of putting watermark into the frame is created by RNG. For example, if RNG output is 1, put watermark and if it is 0, do not apply watermark. RNG randomly generates a series numbers with its high calculation algorithms. Finally, the result is applied to the AE (arithmetic encoding). It is the function of the JPEG2000 and will not discuss here.
As understood from Fig 6, we only embed watermark to random-determined frames using RNG information not only for playing but also for proving that the user is authenticated user using the information such like client specific ID number, Movie content ID, client GPS information.

3 *Concrete design of Decoder*

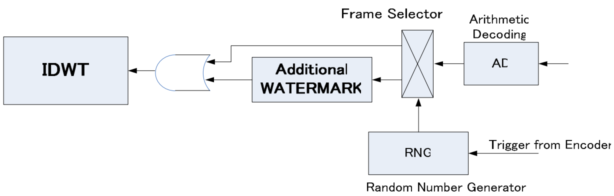

Fig 7 JPEG2000 Decoding with watermark

After the watermarked content has been downloaded, it is either saved into the user server or directly applied to the Decoder LSI for projector. The downloaded content is applied into the JPEG2000-based AD block. The output of the AD is applied to the multiplexer. Mux gives outputs according to the RNG output. RNG at decoder must be synchronized on accordance with RNG at encoder. Therefore, we use a trigger signal for synchronization. The output of the Mux decides either frames are watermarked or not. If the watermarked frames are detected, then additional watermark is added in addition to the existing watermark. If no watermarked frames are found, it is bypassed directly to the IDWT to inverse the Wavelet transformed data.

Decoder LSI gets the Hash key and inserts watermark to the image. So, embedding process is fully handled with HW implementations which make robust watermarking, even then the hash key might have been obtained.

IV. Experimental Results

Experimental results show that proposed method is robust against any image processing.
Experimental robustly tests are done for JPEG and JPEG 2000 images.
Tile size of 2048x2048 Digital Cinema is used. For the simplicity, we used 512x512 image and divided into 5 subband levels via DWT. The Lowest subband is 16x16. The total character size is 256byte to embed, which means entire subband is used. The resulted image is shown in Fig 8-b:

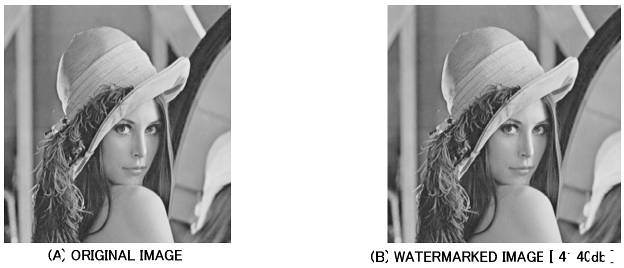

Fig 8 Lena Image (512x512)

Fig 8(a) is the original Lena image and it does not contain any watermarking data.
Fig 8(b) is the Lena image which is watermark-embedded.
The watermark has energy at 41.40db. Other energy levels are given at Table 1 for both Jpeg and Jjpeg2000 images .

Table-1 BER values with Intensity

JPEG	Comp rate[%] (PSNR[DB])		10 (34.93)	9 (34.56)	7 (33.66)	5 (32.23)	3 (29)
	Q	3	0	0	0.781	7.03	35.94
		5	0	0	0	1.56	48.44
		7	0	0	0	0	45.31
JPEG2000	Comp rate[%] (PSNR[DB])		10 (36.47)	9 (36.11)	7 (35.33)	5 (34.16)	3 (32.25)
	Q	3	0	0	0.781	4.68	14.06
		5	0	0	0	0.78	5.47
		7	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 [11]. Hence, the results for QL≥5 satisfy the digital cinema requirements. Our experiments shows Jpeg2000 compression gives better results and there is almost no error for QL=5 and 7. For little error rate that QL=3 gives out, BER is used for QL=3 errors to eliminate the little errors.

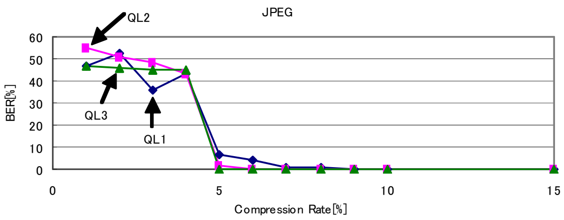

Fig 9 Bit Error Rate under JPEG Compression

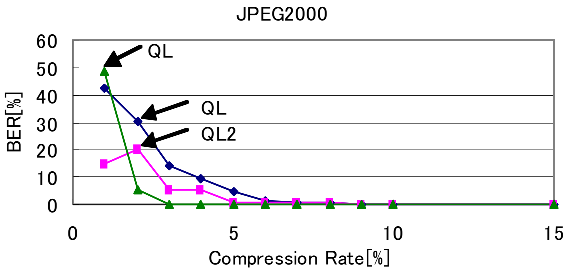

Fig 10 Bit Error Rate under JPEG2000 Compression

At Fig 9-10, it is clear that when compression rate is increased, the less BER is obtained. It means watermarking data is fully obtained with no BER Especially for JPEG 2000 compression, the result becomes almost zero for further compression rates. Fig 9-10 shows that 5% of compression rate has an ignorable BER and it is feasible to make it zero by error correction..

V. Conclusion

In this work, we proposed additional watermarking for digital cinema delivery. Our experimental results show 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.

References

[1] Akio, Miyazaki, Digital Watermarking for images.IEEE Trans. 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

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 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 Kusatsuy/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.