JPEG 2000 Wireless Image Transmission System using Encryption Domain Authentication

Ryo Ito*, Muneaki Matsuo*, Yuya Miyaoka*, Koji Inoue**, Shoma Eguchi**,

Masayuki Kurosaki*, Hiroshi Ochi*, Yoshimitsu Kuroki**, Akio Miyazaki***

* Department of Computer Science and Electronics, Kyushu Institute of Technology

Kawazu 680-4 Iizuka, Fukuoka, Japan

** Department of Control and Information Systems Eng., Kurume National College of Technology

Komorino 1-1-1 Kurume, Fukuoka, Japan

*** Department of Social Information System, Kyushu Sangyo University

Matsukadai 2-3-1 Fukuoka Higashi-ku, Fukuoka, Japan

***{ito, mnmatsuo, miyaoka}@dsp.cse.kyutech.ac.jp, {kurosaki,ochi}@cse.kyutech.ac.jp**

****{s46206ki, s46208se}@std.kurume-nct.ac.jp, kuroki@kurume-nct.ac.jp**

*****miyazaki@is.kyusan-u.ac.jp**

***Abstract*— In this paper, we propose a wireless high resolution video transmission system with encryption and authentication. The proposed system is implemented by JPEG 2000 coding. We implement JPEG 2000 coder by GPU in CUDA which is an integrated development environment for GPU, or by JPEG 2000 codec LSI. Moreover, the authentication system can check the user information in encrypted domain using Paillier encryption. Therefore, this system is more secure than conventional systems. We show that the proposed system can achieve 4K size coding by 2.34fps with CUDA, and HD size coding by 29.98 fps with LSI codec. In addition, we demonstrate that the authentication using Paillier encryption is successful.**

***Keywords*— JPEG 2000, Paillier encryption, GPGPU, Image transmission, Digital cinema**

I. INTRODUCTION

In recent years, frame size of the TV that is popular in each household (1920 × 1080 pixels) is the mainstream full HD. However, there is a growing demand for high-definition that exceeds the quality of full HD video in applications including movies and medical.

Digital cinema is an application of digital technology for storage, distribution and projection of motion pictures [1]. This technology is also expected to be used in home theaters in the near future and promise much better image quality than high definition (HD) televisions. In addition, the size of 4K (4096 × 2160 pixel) TV that has a resolution that is more than four times the full HD which has been commercially available, expected to spread.

When using a projector to view high definition television (HDTV) content as well as digital cinema, wireless technology has become necessary because of the complexity of wiring. Wireless transmission systems for HD content are being researched and developed such as home theater system, Wireless HD (WiHD) [2, 3], UWB(Ultra wide band)[4, 5] and wireless home digital interface (WHDI) [6]. Additionally, 4K video has variety of benefits including remote medical diagnosis using a high-definition video.

In case that uncompressed 4K size image is transmitted, the throughput needed is over 6Gbps. Recently, since wireless LAN technology is developing rapidly, next generation wireless LAN standard IEEE 802.11ac can achieve a maximum of 6.9Gbps in physical layer. However, 4K size image is needed to be compressed for transmission to account for protocol overhead in upper layer.

In addition, content security for protecting copyright becomes important. Commonly-used authentication system has risk because the authentication identifier is checked after decryption. If the decrypted data is sniffed, the wiretapper can get content data perfectly.

JPEG 2000 coding is appropriate compression technology for wireless transmission [7]. JPEG 2000 is successor standard of JPEG, and used for digital cinema. The image deterioration for high compression rate is prevented more than JPEG. Additionally, rate control is easy, and error resilience can be used. In this report, we propose wireless transmission system platform for JPEG 2000 with authentication using encryption domain. The proposed system can achieve real time processing and secure transmission for high-definition image.

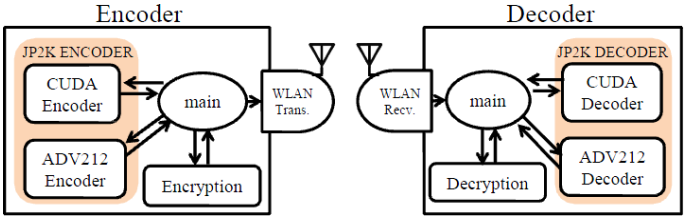

Figure 1. The proposed image transmission system

II. JPEG 2000 IMAGE TRANSMISSION SYSTEM

The proposed image transmission platform is shown in Figure 1. The rest of the paper is organized as follows: Section 3 and 4 describe JPEG 2000 codec implementations with codec LSI and CUDA. Section 5 states encryption and authentication algorithms. Section 6 shows the implementation results of the proposed system. Finally, the paper is concluded with Section 7. This platform is implemented based on "main" application with JPEG 2000 codec and the authentication system. These functions are provided as Dynamic Link Library (DLL).

III. IMPLEMENTATION WITH JPEG 2000 CODEC LSI

We have implemented JPEG 2000 codec DLL using "ADV212" JPEG2000-compatible video LSI codec produced by Analog Devides [8]. ADV212 can real-time JPEG 2000 encode/decode of HD resolution uncompressed video. ADV212 evaluation board has Serial Digital Interface (SDI) for uncompressed image input/output.

The architectures of JPEG 2000 encoder and decoder using ADV212 are shown in Figure 2 and 3, respectively. The proposed system controls ADV212 with DirectShow which is a multimedia framework and API produced by Microsoft [9]. DirectShow generates processes for JPEG 2000 encoding/decoding with ADV212 independently from "main" application and other functions. Therefore, this architecture can process real-time JPEG 2000 coding with low latency. A picture of the proposed system using ADV212 is shown in Figure 4.

IV. IMPLEMENTATION OF JPEG 2000 CODEC WITH CUDA

In this implementation, the goal is to playback the images at a frame rate of 30fps (frame per sec.) 4K image size. For speeding up image of JPEG 2000 codec 4K image size, implemented using CUDA(Compute Unified Device Architecture). The block diagram of a JPEG 2000 encoder is shown in Figure 5. In the proposed codec with CUDA, the processing speed is improved by using split tiles and parallel codeblocks.

A. CUDA

CUDA produced by NVIDIA is an environment of general purpose computing on graphics processing units (GPGPU) [10]. CUDA is parallel computing architecture that enables dramatic increases in computing performance by harnessing the power of the GPU. GPU cannot operate alone. GPU can operate on instruction from the CPU. A CUDA architecture are shown in Figure 6. Inside the GPU, there is a kind of memory Shared memory and Register, such as the Global memory. Access time to the memory space of each is different from the thread.

B. Split Tiles for parallel coding

In this paper, we show a JPEG 2000 parallel processing algorithm using tile process. After split tiles, each image is encoded by JPEG 2000.

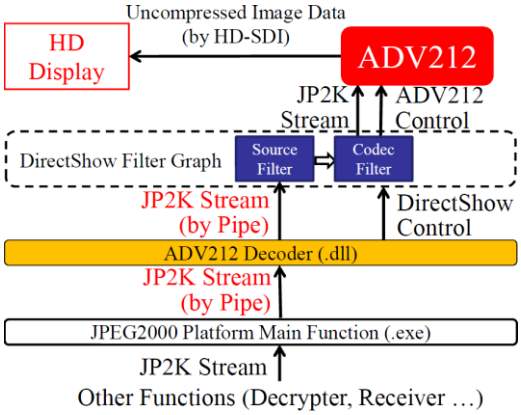

Figure 2. The architecture of ADV212 Decoder

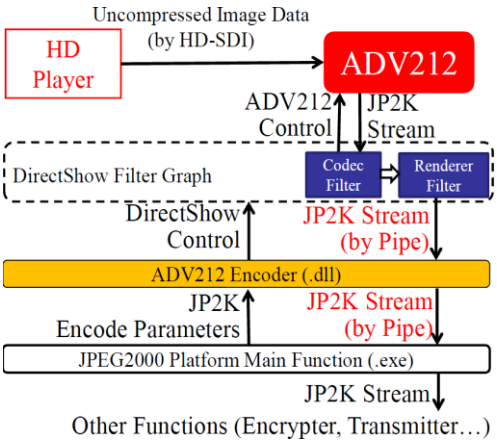

Figure 3. The architecture of ADV212 Encoder

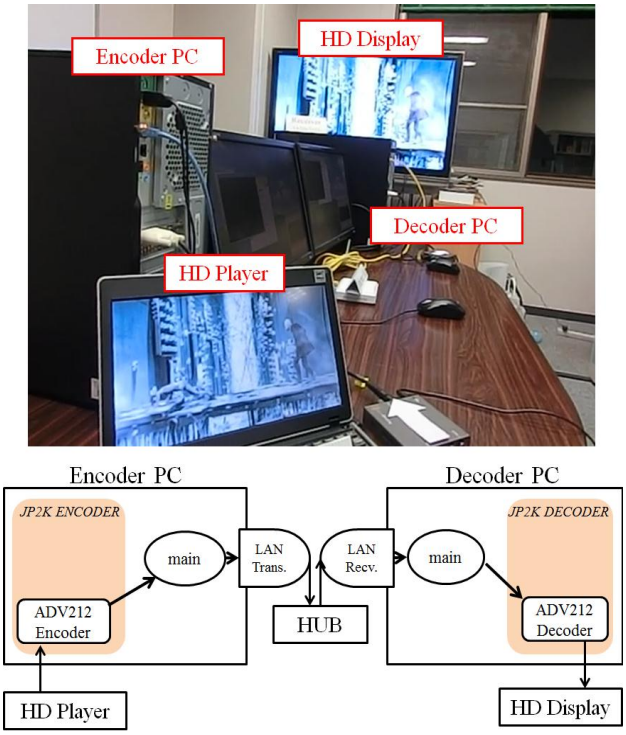

Figure 4. A picture of the proposed system using ADV212

C. Parallel codeblocks

In EBCOT each sub-band is partitioned into rectangular blocks (e.g., 64 × 64) called "code-blocks," which form the independent input to the coefficient bit modeling based on bit-plane and arithmetic coding. However, in JPEG 2000, one side of code block is defined by a minimum of 4pixel. Each code block is independent of each other, the code does not affect the other blocks. Processed in parallel by each code block, we parallelize the coefficient bit modeling.

V. Encryption and Authentication System

The encryption and an authentication system are based on Paillier encryption [11]. Paillier encryption is one of the public key cryptosystems and consists of three parts, generation of key, encryption, and decryption.

A. Additive Homomorphism

Outline of homomorphism is shown in Figure 8. Homomorphism consists following properties.

- Elements A and B are in set S, and an operator $\oplus$ is closed under set S. Result that elements A and B are calculated by operator $\oplus$ is expressed as $A \oplus B$.
- A set that elements A and B are mapped by function f is denote by T, and the elements are $f(A)$ and $f(B)$. An operator $\otimes$ is closed under set T.
- Element $f(A \oplus B)$ that element $A \oplus B$ is mapped by function f is equal to $f(A) \otimes f(B)$ that elements $f(A)$ and $f(B)$ are calculated by operator $\otimes$.

Additive homomorphism has following relationship.

$$f(A) \times f(B) = f(A + B). \tag{1}$$

Equation (1) denotes that mapping $A + B$ can be gotten by multiplying mapping A and mapping B.

B. Paillier Encryption

1) Generation of Key

The public key is denoted as N and g, and the secret key is denoted as μ and λ. The function L is defined by

$$L(x) = \frac{x-1}{N}. \tag{2}$$

First, N and λ are expressed respectively with two great prime numbers p and q as

$$N = p \times q, \quad \lambda = \mathrm{lcm}(p-1, q-1). \tag{3}$$

Here, function $\mathrm{lcm}(x, y)$ derives lowest common multiple between x and y.

Next, g is selected with following conditions.

$$g \in Z^*_{N^2}, \quad \gcd(L(g^\lambda \bmod N^2), N) = 1, \tag{4}$$

where function $\gcd(x, y)$ derives the greatest common divisor between x and y.

Finally, μ is given by

$$\mu = (L(g^\lambda \bmod N^2) \bmod N)^{-1}. \tag{5}$$

2) Encryption

The plaintext written in numbers is denoted as m. The ciphertext c is expressed with N, g ,r and m by

$$c = g^m r^N \bmod N^2, \tag{6}$$

where r is selected with conditions that $r \in Z^*_{N^2}$. Z is integer set, and r is the parameter to map ciphertext in random order for encryption and decided by encryption side. The random nature strengthens security.

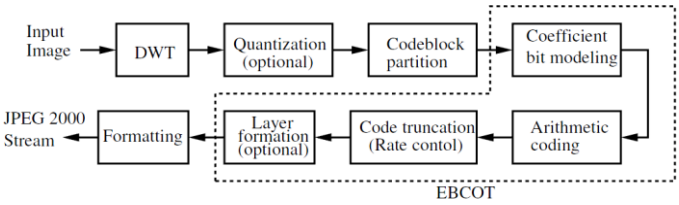

Figure 5. JPEG 2000 encoder block diagram

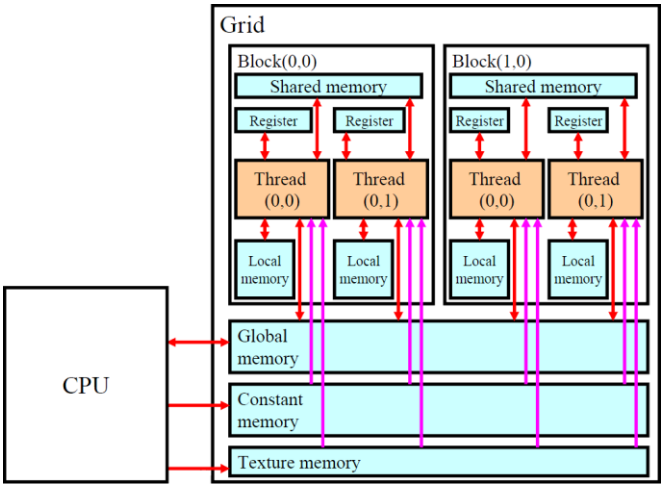

Figure 6. CUDA Architecture

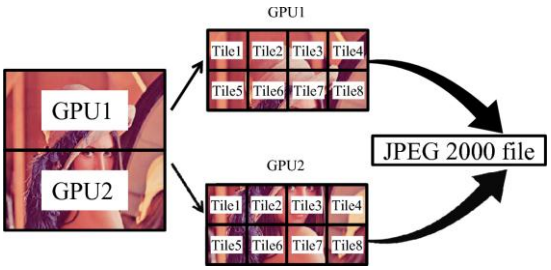

Figure 7. Split Tiles for parallel processing

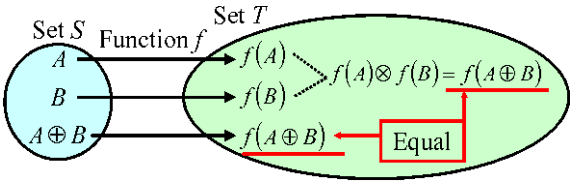

Figure 8. Outline of homomorphism

3) Decryption

The plaintext m can be decrypted from c. Here, m is given by

$$m = \mu \times L(c^{\lambda} \bmod N^2) \bmod N. \quad (7)$$

C. Proposed System

Authentication system is implemented by additive homomorphism of Paillier encryption, and the identifier is embedded in video image with encryption [12].

(i) Authentication Identifier Embedding

As authentication identifier, ID that is allocated for each projector is added to moving picture image data m in encryption processing.

In case that $m > ID$,

$$c = g^{m-ID} r^N \bmod N^2. \quad (8)$$

In case that $m < ID$,

$$c = g^{m+N-ID} r^N \bmod N^2. \quad (9)$$

(ii) Authentication Identifier Removing

The Encryption data is multiplied with a parameter d in projector for decrypting. Here, d is given by

$$d = g^{ID} r^N \bmod N^2. \quad (10)$$

This parameter can be generated by projector that knows the ID. When encryption data is transmitted to projector from server, the ID can removed by

$$\begin{aligned} c \times d &= (g^{m-ID} r^N \bmod N^2) \times (g^{ID} r^N \bmod N^2) \\ &= g^{m-ID+ID} r^N \bmod N^2 \\ &= g^m r^N \bmod N^2. \end{aligned} \quad (11)$$

The encrypt domain is the header that has the most important data. Since operation results affect all images, the content is kept secret.

VI. Implementation Results

The implementation results of the proposed system are shown in Table 1 and 2. From Table 1, the proposed system can transmit 4K images by 2.34fps (Frame per Second). In addition, from Table 2, the proposed system achieves real-time HD image transmission (29.98fps) with ADV212 codec LSI.

We have also validated the encryption and authentication function of the proposed system. Figure 10 and 11 illustrate a comparison of the decryption images with correct/incorrect ID by the proposed system. From these figures, the proposed system can protect images against a third party.

VII. Conclusion

In this paper, we proposed JPEG 2000 image transmission system with the authentication system. The proposed system can process 4K images by 2.34fps, and HD images by 29.98fps with the encryption and authentication function. In future work, we will implement real-time 4K image transmission systems by improving coding speed of CUDA.

Acknowledgment

This work was partly supported by a grant of Regional Innovation Cluster Program by Ministry of Education, Culture, Sports, Science and Technology (MEXT) and Grants-in-Aid for Scientific Research (KAKENHI) Grant Number 22760279, 21656099.

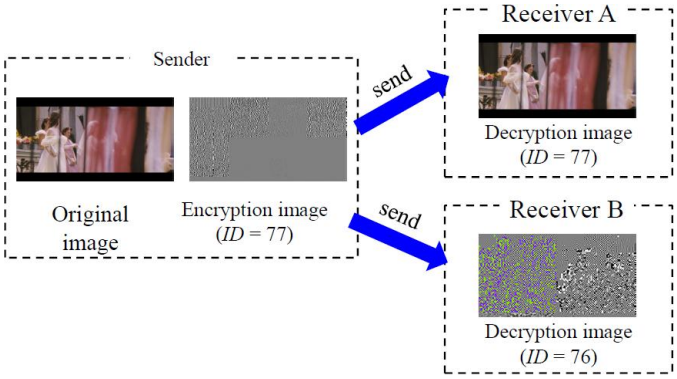

Figure 9. The impelemtation results of the authentication system

TABLE 1. The implemantation results of CUDA

	Encoder	Decoder
Resolution [pixel]	4096 x 2160 (4K)	
Coding speed [FPS]	2.34	2.51

TABLE 2. The implemantation results of ADV212

	Encoder	Decoder
Resolution [pixel]	1280 x 720 (HD)	
Coding speed [FPS]	29.98	30.00

Figure 10. The decryption images with correct ID

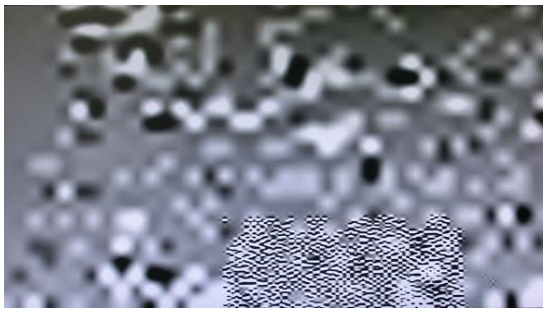

Figure 11. The decryption images with incorrect ID

REFERENCES

[1] Digital Cinema Initiatives, Digital cinema system specification, [Online] Available: http://www.dcimovies.com, Sep. 2012.

[2] Wireless HD, WirelessHD Specification, [Online] Available: http://www.wirelesshd.org/about/specification-summary/, May, 2010.

[3] J. M. Gilbert, C. H. Doan, S. Emami, and C. B. Shung, "4-Gbps uncompressed wireless HD A/V transceiver chipset," *IEEE Micro*, vol.28, issue 2, pp. 56--64, Mar. 2008.

[4] R. Krishnamoorthy, "High definition, any-where: How ultra wideband makes wireless HDMI possible," in *Proc. CCNC 2007*, 2007, pp. 395--399.

[5] S. S. Lee, C. W. Kim, B. H. Park, S. S. Choi, and K. R. Cho, "A wimedia UWB transceiver for 4-HD channel streaming," *IEEE Trans. Consumer Electronics*, vol. 53, no. 2, pp.782--787, May 2007.

[6] AMIMON, High-Definition Wireless. AMIMON - WHDI Technology Overview, [Online] Available: http://www.amimon.com/Technology, Sep. 2012.

[7] ISO/IEC, "Information technology - JPEG 2000 image coding system - Part1:Core coding system," ISO/IEC 15444-1, 2000.

[8] Analog Devices, ADV212: JPEG 2000 VIDEO CODEC, [Online] Available: http://www.analog.com/en/audiovideo-products/video-compression/adv212/products/product.html, Sep. 2012.

[9] Microsoft, Microsoft Developer Network: DirectShow, [Online] Available: http://msdn.microsoft.com/en-us/library/dd375454.aspx, Sep. 2012.

[10] NVIDIA, Parallel Programming and Computing Platform | CUDA, [Online] Available: http://www.nvidia.com/object/cuda_home_new.html, Sep. 2012.

[11] Muneaki Matsuo, Masayuki Kurosaki, Akio Miyazaki, and Hiroshi Ochi, "Image Transmission using Encryption Domain Authentication for Mesh Network," *2011 International Workshop on Smart Info-Media Systems in Asia (SISA2011)*, 2011, pp.57--60.

[12] Pascal Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," *EUROCRYPT'99*, 1999, pp. 223--238.