논문 2009-46CI-3-7

멀티미디어 핑거프린트에 의한 DRM 구현

(DRM Implementation by Multimedia Fingerprint)

이 강 현*

(Kang Hyeon RHEE)

요 약

최근에, 다양한 멀티미디어 콘텐츠 제작에 따라, 불법복제, 불법배포 및 저작권 침해 등과 같은 문제들이 야기되고 있다. 이러한 문제를 해결하기 위하여, 콘텐츠에 저적권 정보를 삽입하는 워터마킹과 RSA를 이용하여 불법복제를 방지하는 DRM에 인증을 위한 암호화하는 방법들이 제안되었다. 본 논문에서는, BIBD코드 기반의 멀티미디어 핑거프린트를 RSA의 DRM을 위하여 영상콘텐츠의 비트플랜에 삽입하고, 디코딩 처리에서 영상전송과 변환을 고려하여 실험을 하였다. 실험결과, Stirmark 공격의 PSNR 30, 40, 70 그리고 80에서, 영상에 삽입된 멀티미디어 핑거프린트 코드가 AWGN 7dB에서 60% 이상 검출되었으며, AWGN 10dB 이상에서는 100%의 완전함을 확인하였다.

Abstract

Recently, according to the product variety of multimedia content, some problems are occurred as like an illegal copying, an illegal distribution and a copyright infringement etc. So, for the solution of these problems, some methods were proposed as like watermarking which inserts the information of copyright to the content and the cipher for authentication to DRM which prevents an illegal copying using RSA. In this paper, the multimedia fingerprint based on BIBD code is inserted to the bit-plane of the image content for DRM with RSA, and while the decoding processing. The experiment is operated with the consideration of the image transmission and the transformation. As a result, it confirmed that the multimedia fingerprint code inserted in image is detected 60% upper at AWGN 7dB and detected completely 100% at AWGN 10dB upper on PSNR 30, 40, 70 and 80 of Stirmark attacks.

Keywords: Multimedia fingerprint(MF), DRM, RSA, BIBD code, Watermarking.

I. Introduction

For the recent days, digital technologies are used in so many place that we could not have imagined in the past. Contents producers are now able to make audio and video file with high quality and the technical development in internet and communication make it possible to connect all the network of the world. It became easier to produce and distributes digital contents[1~4].

These methods are publishing key encryption algorithm, time stamp and checksum for the integrity of the certification and data with watermarking which has been present as copyright. Also there is DRM(Digital Right Management) that prevents from illegal copy[5].

Using DRM technology for encryption algorithm, it is categorized into two encryption methods, such as symmetric encipherment algorithm and asymmetrical encipherment algorithm whether encryption key and decryption key are identical or not identical. The typical symmetric encipherment algorithms are DES[6] and AES, and asymmetric encipherment algorithms

* 평생회원, 조선대학교 전자정보공과대학 전자공학과
(Chosun University, Electronics & Information Engineering College, Dept. of Electronics Eng.)

※ This study was supported by research funds from Chosun University, 2008.
접수일자: 2009년3월27일, 수정완료일: 2009년5월4일

are El-Gaml, RSA, ECC(Elliptic Curve Cryptography)[7].

RSA(Rivest, Shamir and Adleman) method is based on the difficulties of factorization and difficult problem to factor the big number, and it became the most frequently using public key algorithm in the world today. And RSA used in electronic signature algorithm combined with various messages compressing algorithm and use to be the safe transmission of symmetrical key in the encryption format.

There are several algorithm types for encryption. To prevent from the copyright infringement and illegal distribution during the contents distribution, DRM is used in representation of information of copyright with digital watermarking and multimedia fingerprint(MF).

In this paper, multimedia fingerprint based on BIBD(Balanced Incomplete Block Designs) code is inserted to the bit-plane of image for DRM with RSA which is the public key. Among the decryption proceeding, the proposed algorithm is experimented with the consideration of image transmission and transformation.

The rest of thesis is organized as follows: it will briefly review the theoretical background of DRM and RSA in Section Ⅱ, Section Ⅲ explains our encryption realization by using RSA and multimedia fingerprint for DRM system. Furthermore, it implements the proposed algorithm and analyzes the experimental results. Finally, the conclusion is drawn in Section Ⅳ.

Ⅱ. Theoretical Background

2.1 DRM and Watermarking

DRM is the copyright protection system for the distribution management of digital contents with safe and trustable method and enable for certified user to use the signified contents to protect the rights and benefit[8]. The methods to prevent from illegal reproduction and distribution are categorized into two ways. The one enable authorized users to use and transmit within a boundary of admitted limitation, and another is to trace how people reproduce and distribute contents illegally, when they are found to be illicit contact with the unauthorized content[9].

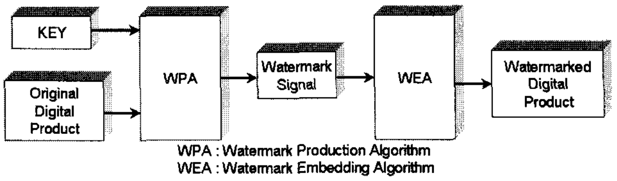

KEY
Original Digital Product
WPA
Watermark Signal
WEA
Watermarked Digital Product
WPA : Watermark Production Algorithm
WEA : Watermark Embedding Algorithm

그림 1. 워터마크 삽입
Fig. 1. Watermark insertion.

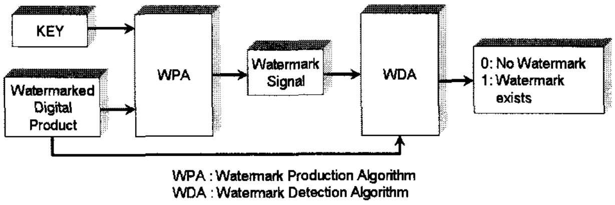

KEY
Watermarked Digital Product
WPA
Watermark Signal
WDA
0: No Watermark
1: Watermark exists
WPA : Watermark Production Algorithm
WDA : Watermark Detection Algorithm

그림 2. 워터마크 검출
Fig. 2. Watermark detection.

Digital watermarking method that indicates the copyright by inserting the provider's information directly on digital contents. This orientation of technology comes from the intention to protect the copyright because digital contents on web are easy to reproduce. Fig. 1 and 2 shows the watermark insertion and watermark detection.

When the copyright infringement has been occurred, copyrighters can choose to insert the watermark into their content to acknowledge who is responsible for the original contents.

2.2 Multimedia Fingerprinting

Multimedia fingerprinting is contents security technology based on watermarking technology. To improve the weak point that illegal production circulation process remains unknown, fingerprinting technology has been being researched[10]. Fingerprinting watermark insertion and detection algorithm can protect Intellectual Property Rights(IPR) by inserting Unique Digital Signature on every single digital content. BIBD code was used for multimedia fingerprint. Compounding a problem of

BIBD code is using a matrix model to produce code satisfied with constraints[11].

v: number of processed.

b: number of blocks.

r: (k<v) number of repetition of each processing.

k: number of processing contained in one block.

λ: number of blocks that each processed pair appears in.

5 parameters are satisfying following two limitation conditions.

$$vr = bk \tag{1}$$

$$r(k-1) = \lambda(v-1) \tag{2}$$

BIBD is simply able to expressed with (v, k, λ).

$$b = \frac{v(v-1)\lambda}{k(k-1)} \tag{3}$$

$$r = \frac{\lambda(v-1)}{k-1} \tag{4}$$

b=v or r=k then BIBD is symmetrical.

If $X = \{X_i\}_{i=1}^{v}$ and $A = \{A_j\}_{j=1}^{b}$, then BIBD's frequency matrix becomes matrix M as Eq. (5).

$$m_{ij} = \begin{cases} 1 & \text{if } x_i \in A_j \\ 0 & otherwise. \end{cases} \tag{5}$$

Therefore M satisfy Eq. (6).

$$MM^t = (r-\lambda)I + \lambda J \tag{6}$$

All row vectors of frequency matrix M in BIBD becomes multimedia fingerprint code and authorizes then to users. This M can be used like anti-collusion code. Vector becomes 1 or k-1 when many users execute OR's logical collusion attack.

BIBD code for multimedia fingerprint is are appeared in Fig. 3 when {v, k, λ } are {7,3,1}.

M=

m_{ij}	b_1	b_2	b_3	b_4	b_5	b_6	b_7
v_1	0	1	0	1	0	1	0
v_2	1	0	0	1	1	0	0
v_3	0	0	1	1	0	0	1
V_4	0	1	0	0	1	0	1
v_5	1	1	1	0	0	0	0
v_6	1	0	0	0	0	1	1
v_7	0	0	1	0	1	1	0

그림 3. 멀티미디어 핑거프린트를 위한 {7,3,1} BIBD 코드

Fig. 3. {7,3,1} BIBD code for multimedia fingerprint.

2.3 RSA Algorithm

RSA public-key cryptography has been developed by Rivest, Adi Shamir and Adleman from MIT mathematics major in 1978, which is known for fully reflected the public-key cryptography system suggested by Diffe and Hellman in 1976[12].

This algorithm use two prime number. These two prime numbers generate public-key by adjusting themselves and personal keys are generated by using existing public-key. It is the RSA that encode and decode with public-key and private-key.

Fig. 4 shows how RSA cryptography system works. Where M is message and C is the encrypted code and e is public-key and d is private-key and N is modulus.

At this time N is determined by two prime number. If this two prime number is called p and q, N and key are determined following equations.

$$N = p \cdot q \tag{7}$$

$$\begin{aligned} &\gcd(e, \phi(N)) = 1, \\ &where\ \phi(N) = (p-1)(q-1) \\ &1 < e < \phi(N) \end{aligned} \tag{8}$$

$$d = e^{-1} \mathrm{mod}\ ((N)) \tag{9}$$

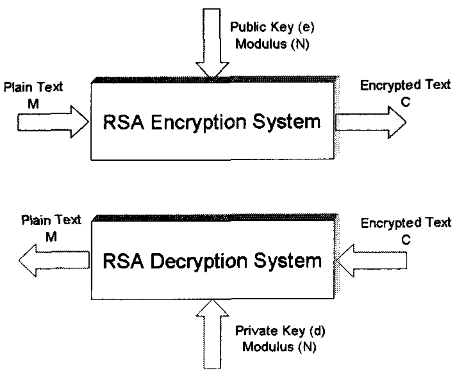


그림 4. RSA 암·복호 시스템

Fig. 4. RSA encryption, decryption system.

표 1. RSA 연산 과정
Table 1. RSA operation processing.

Operation	Algorithm
Prime number	$p,\ q$
Modulus	$N=p \cdot q$
Public Key	$gcd(e,\ \phi(N))=1$ where $\phi(N)=(p-1)(q-1)$ $1<e<\phi(N)$
Private Key	$d=e^{-1}\ mod(\phi(N))$
Cipher	$C=M^{e}\ mod\ (N)$
Decipher	$M=C^{d}\ mod\ (N)$

On encryption and decryption using modulus, public-key and private-key determined by Eq. (7), (8) and (9) leads to Eq. (10) and (11).

$$C = M^{e} \bmod N \tag{10}$$

$$M = C^{d} \bmod N \tag{11}$$

The process followed has "Cipher" and "Decipher" in Table 1.

Ⅲ. Implementation of the proposed algorithm and Analysis of the experimental result

The proposed DRM system is shown in Fig 5. It composed with BIBD code and RSA.

Multimedia fingerprint based on BIBD code is inserted into original content then encryption is operated, and multimedia fingerprint is detected from decrypted content. It decides final multimedia fingerprint throughout the correlation with the inserted multimedia fingerprint.

Multimedia fingerprint was inserted into LSB(Least Significant Bit) after decompose image into each bit-plane. Because insertion of multimedia fingerprint into MSB could be relatively easily noticed changes of image quality, insertion to LSB is intended for difficulty of notification. Using two prime numbers of BIBD code in the process of insertion of multimedia fingerprint, combination of the row and column would determine the place for multimedia fingerprint to be inserted. LSB 7 bit of 7 pixels of determined place and multimedia fingerprint are operated on logically EXOR. Fig. 6 shows the proceeding for insertion of multimedia fingerprint into its content.

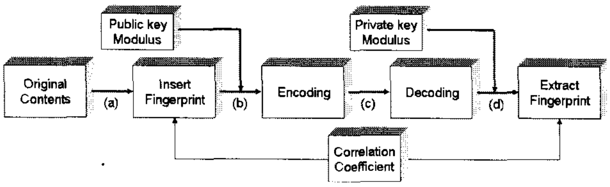
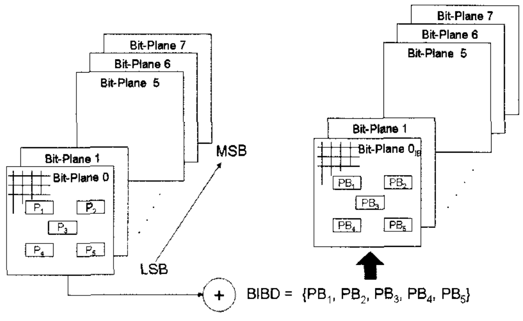


그림 5. 제안된 DRM 시스템의 블럭도
Fig. 5. The block diagram of the proposed DRM system.

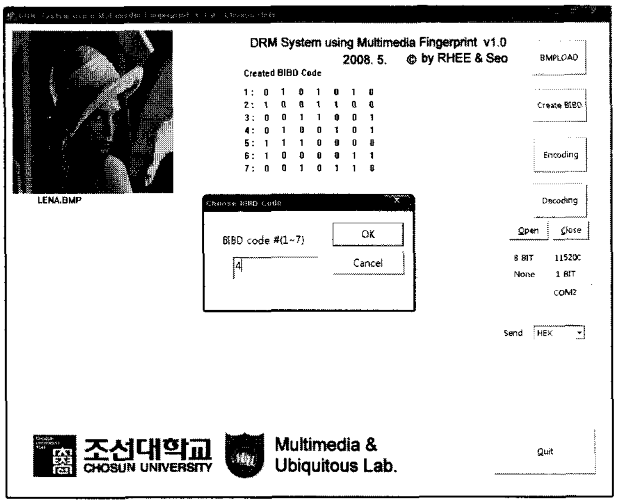


(a) Original Image
(b) MF Added Image

그림 6. 멀티미디어 핑거프린트 삽입과정
Fig. 6. The multimedia fingerprint insertion proceeding.

To experiment on the proposed algorithm, Visual C++, Matlab and Maple are used for the implementation and the application program of GUI environment is shown in Fig. 7.

In Application program, encrypted contents were decrypted with private-key and multimedia finger


DRM System using Multimedia Fingerprint v1.0
2008. 5. © by RHEE & Seo

Created BIBD Code

```
1: 0 1 0 1 0 1 0
2: 1 0 0 1 1 0 0
3: 0 0 1 1 0 0 1
4: 0 1 0 0 1 0 1
5: 1 1 1 0 0 0 0
6: 1 0 0 0 0 1 1
7: 0 0 1 0 1 1 0
```

BIBD code #(1~7) 4

그림 7. 멀티미디어 핑거프린트를 삽입하기 위한 과정
Fig. 7. The proceeding for inserting multimedia fingerprint.

print is detected from the decrypted data.

The prime numbers composed with combination of each column bit in Fig. 3 are used to create public key. Showing columns v4 and v6 in combination of bits is following

$$v4 = 0100101_{(2)} = 37$$
$$v6 = 1000011_{(2)} = 67$$

Column v4 and v6 are used as prime number to create public key of RSA to encryption. The place for MF(Multimedia Fingerprint) to be inserted can be determined by adjusting two prime numbers above and each place denoted as P is same as P_1=(37, 37), P_2=(37, 67), P_3=(52, 52), P_4=(67, 37) and P_5=(67, 67).

Fig. 8 shows each bit-plane image of LENA, which is the previous process for MF to be inserted in LSB in Fig. 6.

Fig. 9 shows the process of inserting MF code(01010101) onto P_1 of bit-plane which is LSB of LENA image, and other positions of MF are inserted in this method. Let original pixel be M, MF code be B and pixel inserted with MF be MB, to extract the inserted MF, like Eq. 12. MF inserted image MB and original image M are calculated with ExOR together to extract MF and then determine MF by using the correlation with original MF.

$$M \oplus B = M_B$$
$$M_B \otimes M = B \tag{12}$$

Fig. 10 shows each image that are both original and MF-inserted. When MFs are inserted to 5 specific points, PSNR between a point (a) and (b) in Fig. 5 appears to be 85.4dB. The reason why 5 points are inserted with MF is to determine MF with estimating that extracting MF is more than 3/5, when AWGN noise and distorted MF code by Stirmark.

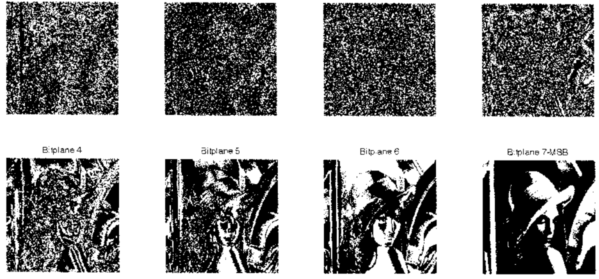
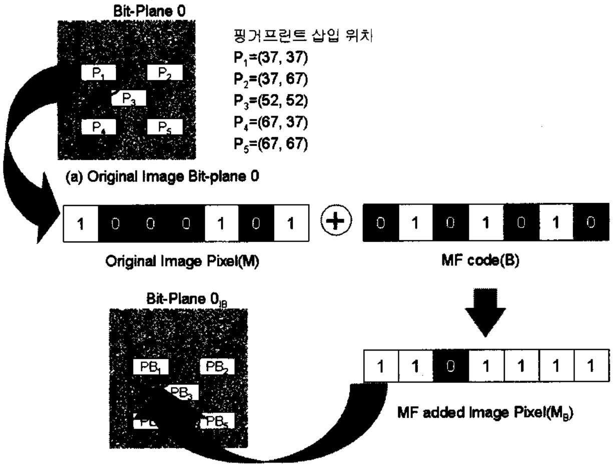


그림 8. LENA 영상의 각 bit-plane 영상
Fig. 8. Each bit-plane images of the LENA image.



(a) Original Image Bit-plane 0

(b) MF added Image Bit-plane 0

그림 9. LSB Bit-plane의 첫 번째 멀티미디어 핑거프린트 코드 삽입을 위한 연산과정
Fig. 9. The processing for insertion of the 1st multimedia fingerprint code of LSB bit-plane.

(a) Original Image (b) MF Added Image

그림 10. 원 영상과 멀티미디어 핑거프린트가 삽입된 영상
Fig. 10. Original and multimedia fingerprint added image.

For encrypted data, AWGN was measured the error bit from 0dB to 60dB at a point (c) in Fig. 5 to measure the effect of noise in transferring line. As a result shown Fig. 11 and Table 2, when AWGN equals to 0dB, maximum possibility of error is 60 percent and when it equals to 20dB, possibility of error is 0%.

When more than 20dB of gaussian white noise is applied, decryption works perfectly. In each BIBD

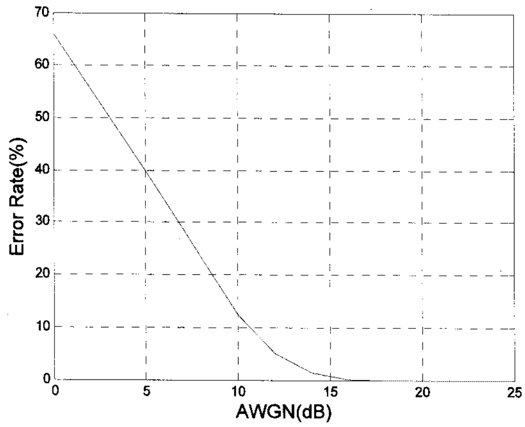
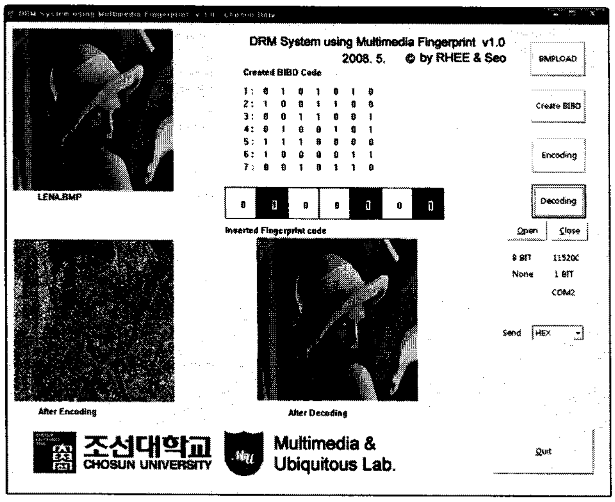


그림 11. AWGN(dB)에 따른 에러율
Fig. 11. The error rate according to AWGN(dB).

표 2. AWGN(dB)에 따른 에러 비트 및 에러율
Table 2. Error bit and error rate according to AWGN(dB).

AWGN (dB)	0	5	10	12	14	16	18	20	25
Error Bit	346,395	209,998	65,152	26,262	6,919	898	33	0	0
Error Rate(%)	66	40	12.4	5	1.3	0.1	0	0	0


DRM System using Multimedia Fingerprint v1.0
2008. 5. © by RHEE & Seo

Created BIBD Code

```
1: 0 1 0 1 0 1 0
2: 1 0 0 1 1 0 0
3: 0 0 1 1 0 0 1
4: 0 1 0 0 1 0 1
5: 1 1 1 0 0 0 0
6: 1 0 0 0 0 1 1
7: 0 0 1 0 1 1 0
```

Inserted Fingerprint code: 0 1 0 0 1 0 1

그림 12. GUI 환경의 응용프로그램
Fig. 12. The application program with GUI environment.

code, there was experiment to research the consistency about MF noise with two BIBD code that has most net change. In the experiment, when AWGN noise occurs at a point (c) in Fig. 5, MF in point (d) was extracted. To acknowledge average extraction rate, experiment was executed in different points inserted with MF.

MF for each places inserted with MF. As a result, MF code is extracted 100% in v1 and v4 in more than 10dB, and 60% in v1 and v4 in more 7dB.

To measure the efficiency of extracting for BIBD code depending on Stirmark attack, Benchmark(Ver. 4.0) was used[13].

As a result, the detected number of MF in PSNR 30, 40, 70 and 80 Stirmark attack has a strong resistance showing 60% detection rate, however, has a less resistance in CONV, JPEG, MEDIAN and NOISE showing less than 50% Stirmark.

The result of encryption and decryption, inserting MF from image and creating MF based on BIBD in GUI environment is shown in Fig. 12.

Ⅳ. Conclusion

In this paper, DRM system using MF to prevent the illegal use of contents is designed and multimedia fingerprint code based on BIBD code is inserted to image. The place of image to insert is determined by selecting prime number among the BIBD code value. RSA block is realized with two prime numbers which are used to create public key of RSA.

To estimate the resistance for Stirmark attack of MF, Stirmark Benchmark was used for a decrypted image after adding AWGN of 7dB. In measuring interrelationship, 7dB results 60% of BIBD code and is determined as MF code. As a result, when more than 20dB of AWGN was added, it does not affect on data. However, when it is less, it damages so much that decryption does not work properly.

Therefore, it requires powerful method to transfer the data for the case of noise and method to correct the errors when data were damaged from noise and external attack.

참 고 문 헌

[1] S H Seo "Implementation on FPGA of DRM using Multimedia Fingerprint," M.Eng. Degree Thesis, Chosun Univ., Graduate School, 2008.8

[2] J S Noh and K H Rhee "Detection of colluded multimedia fingerprint by neural network," 대한

전자공학회 논문지, 2006-43CI-4-10, pp.80~87, July 2006.

[3] K H Rhee "Detection of colluded multimedia fingerprint using LDPC and BIBD," 대한전자공학회 논문지, 2006-43CI-5-8, pp.68~75, Sep. 2006.

[4] B L Cho, I Y Chung, C G Park, K H Rhee "A Study on the Digital Audio Watermarking for a High Quality Audio," 대한전자공학회 논문지, Vol. 39-CI, NO. 3, pp. 62-70, May 2002.

[5] 최동현, 이병희, 김승주, 원동호, "DRM(Digital Rights Management) 기술," 정보과학회지 제25권 제5호, 5. 2007.

[6] Federal Information Processing Standards Publication 197 November 26, 2001.

[7] V. Miller, "Use of elliptic curves in cryptography", CRYPTO 85, 1985

[8] DRM포럼, "http://drm.or.kr/spb3/index.php"

[9] Ju-Young Moon, "Design of DRM System for Contents Redistribution in Home Domain", 한국컴퓨터 정보학회 논문지, 7. 2007.

[10] K.J.Ray Liu, Wade Trappe, Z.Jane Wang, Min Wu, and Hong Zhao "Multimedia Fingerprinting Forensics for Traitor Tracing," EURASIP Book Series on Signal Processign and Communications, Volume4.

[11] Shashanka, D.; Bora, P.K. "Collusion Secure Scalable Video Fingerprinting Scheme," ADCOM 2007. International Conference, 18-21 Page(s):641 - 647, Dec. 2007.

[12] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, Vol. 21 (2), pp. 120-126, 1978.

[13] http://www.petitcolas.net/fabien/watermarking/stirmark/

저자소개

이 강 현(평생회원)-교신저자

1979년, 1981년 조선대학교 전자공학과 공학사 및 석사
1991년 아주대학교대학원 공학박사
1977년~현재: 조선대학교 교수
1991년, 1994년 미 스탠포드대 CRC 협동연구원.
1996년 호주시드니대 SEDAL 객원교수
2000년~현재 한국 멀티미디어 기술사협회 이사
2000년~현재 아시아태평양 Silicon Sea Belt 위원
2002년 영국 런던대 객원교수
2002년 대한전자공학회 멀티미디어연구회전문위원장
2003년 한국 인터넷 방송/TV 학회 수석부회장
2003년~현재 대한전자공학회 이사
2005년~2008년 :조선대학교 RIS지원 사업단장
<주관심분야 : 멀티미디어 시스템 설계, Ubiquitous convergence, 디지털 시네마 DRM>