논문 2010-47CI-1-2

유비쿼터스 네트워크 환경의 멀티미디어 콘텐츠 보호를 위한 공모공격 방지 임베디드 시스템 설계

(An Embedded System Design of Collusion Attack Prevention for Multimedia Content Protection on Ubiquitous Network Environment)

이 강 현*

(Kang Hyeon RHEE)

요 약

본 논문은 비디오 콘텐츠가 P2P 환경에서 배포될 때, 멀티미디어 핑거프린팅 코드를 삽입하는 알고리즘을 제안하고 공모공격 방지를 위한 공모 코드북 SRP(Small RISC Processor) 임베디드 시스템을 설계한다.

구현된 시스템에서는 웹서버에 업로드를 요청하는 클라이언트 사용자의 비디오 콘텐츠에 삽입된 핑거프린팅 코드를 검출하여 인증된 콘텐츠이면 스트리밍 서버로 전송을 하여 P2P 네트워크에 배포를 허락하고, 공모코드가 검출되면 스트리밍 서버로 비디오 콘텐츠의 전송을 차단하여 P2P 네트워크에 배포를 중지시키고, 또한 공모코드에 가담한 공모자를 추적한다.

BIBD 코드 v의 10%를 공모자로 하여 평균화공격의 공모코드를 생성하였다. 이를 기반으로 공모공격 방지의 코드북이 설계되었다. 비디오 콘텐츠의 온라인 스트리밍 서비스 ASF와 오프라인 제공 MP4의 비디오 압축에서는 I-프레임의 휘도성분 Y의 비트플랜 0~3에 핑거프린팅 코드의 삽입량이 0.15% 이상에서 삽입된 원코드와 검출된 코드의 상관계수는 0.15 이상이었다. 상관계수 0.1 이상에서 공모코드 검출율은 38% 그리고 상관계수 0.2 이상에서 공모자 추적율은 20%임을 확인하였다.

Abstract

This paper proposes the multimedia fingerprinting code insertion algorithm when video content is distributed in P2P environment, and designs the collusion codebook SRP(Small RISC Processor) embedded system for the collusion attack prevention.

In the implemented system, it is detecting the fingerprinting code inserted in the video content of the client user in which it requests an upload to the web server and in which if it is certified content then transmitted to the streaming server then the implemented system allowed to distribute in P2P network. On the contrary, if it detects the collusion code, than the implemented system blocks to transmit the video content to the streaming server and discontinues to distribute in P2P network. And also it traces the colluders who generate the collusion code and participates in the collusion attack.

The collusion code of the averaging attack is generated with 10% of BIBD code v. Based on the generated collusion code, the codebook is designed. As a result, when the insert quantity of the fingerprinting code is 0.15% upper in bitplane 0~3 of the Y(luminance) element of I-frame at the video compression of ASF for a streaming service and MP4 for an offline offer of video content, the correlation coefficient of the inserted original code and the detected code is above 0.15. At the correlation coefficient is above 0.1 then the detection ratio of the collusion code is 38%, and is above 0.2 then the trace ratio of the colluder is 20%.

Keywords: Multimedia fingerprinting code, BIBD code, (n,k) code, LDPC code, P2P, DRM, SRP.

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

※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 일반연구자 지원사업(2009-0073050)임

접수일자: 2009년12월16일, 수정완료일: 2010년1월11일

Ⅰ. 서 론

무선 인터넷, 핸드헬드 모바일 단말기, 스트리밍 전송기술 그리고 압축기법의 최근 진보는 디지털 음악, 이미지, 비디오와 같은 멀티미디어 콘텐츠를 인터넷을

통해 광대역 배포를 가능하게 했다. 이러한 멀티미디어 콘텐츠는 CD나 DVD와 같은 물리적 매체 형식과 유, 무선 네트워크를 통하여 디지털 미디어 포맷으로 배포가 되는데 관리와 인증과정 없이, 멀티미디어 콘텐츠는 불법으로 변경되고, 권한이 없는 사용자에게 복사되고 배포가 된다. 이러한 저작권 위반은 멀티미디콘텐츠 생산 업체의 수익에 영향을 미친다[1~2].

이에 따라 멀티미디어 핑거프린팅 기술이 대두되었고, 핑거프린팅 코드를 멀티미디어 콘텐츠에 삽입하는 방법도 다양하게 연구되었다. 핑거프린팅 코드를 콘텐츠에 삽입할 때, 직교변조 기술은 공모자들의 평균화공격에 대하여 강인성이 제한적이나, 코드변조 기술은 평균화 공격에 대하여 강인성을 갖고 있으며 균형불완비 블럭코드(BIBD: Balnced Incomplete Block Design)에서 파생된 탄력적 코드를 핑거프린팅 코드로 이용한다[3]. 또한 [3]에서 평균화 공격에 사용된 공모코드를 배포된 콘텐츠로부터 검출하는데 공모자의 수에 따라 임계값의 설정이 바뀌므로 임계값을 결정하기가 어려운 문제점도 있다[4].

본 논문에서는 유비쿼터스 네트워크 환경의 멀티미디어 콘텐츠 보호를 위한 공모공격 방지 임베디드 시스템 을 설계한다. P2P 환경에서 스트리밍 서버를 통하여 비디오 콘텐츠가 배포되는데, BIBD 기반의 멀티미디어 핑거프린팅 코드와 이의 (n,k) 확장코드와 LDPC 응용코드를 생성하여 비디오 콘텐츠에 삽입하는 알고리즘을 제안한다. 또한 클라이언트 사용자가 배포할 콘텐츠를 웹 서버에 업로드하기 위한 요청단계에서 콘텐츠에 삽입된 핑거프린팅 코드를 검출하여 인증된 콘텐츠는 스트리밍 서버로 전송하고, 공모코드가 검출되면 스트리밍 서버에 콘텐츠 전송을 차단하면서, 불법공모자를 추적한다. 그리고 공모코드에 의한 공모공격 방지를 위하여 공모코드 북의 SRP(Small RISC Processor) 임베디드 시스템을 설계하고 P2P 환경의 웹서버와 연동하여 동작한다.

제Ⅱ장에서는 P2P 웹서버에서 스트리밍 서버로 콘텐츠를 전송하는데 삽입되는 멀티미디어 핑거프린팅 생성과 공모공격 방지를 위한 공모코드 북 SRP 임베디드 시스템을 설계하고, 제Ⅲ장에서는 P2P 네트워크 환경에서 제안된 알고리즘의 비디오 콘텐츠에 적용하여 실험과 결과고찰을 통하여 제Ⅳ장에서 결론을 맺는다.

Ⅱ. P2P 웹서버와 스트리밍 서버의 공모공격 방지 임베디드 시스템 설계

멀티미디어 핑거프린팅 코드 설계에서 중요한 요소는 평균내성과 코드 효율성 2가지이다. 이를 위하여 본 논문에서는 BIBD 기반으로 생성된 핑거프린팅 코드[3, 5]와 이를 [6]에서 다룬 (n,k) 코드로 확장하고 또한 [7]에서 다룬 LDPC 코드로 표 1과 같이 확장한다. 이 3가지의 코드는 비디오의 압축과정에서 I-프레임의 Y, Cb, Cr 성분의 비트플랜에 그림 1과 같이 각각 삽입한다.

이렇게 3가지로 생성된 코드를 [8]에서 다룬 공모자의 추적 알고리즘과 통합하여 그림 2와 같이 P2P 환경에서 실시간 온라인 스트리밍 배포(LDPC 응용코드 적용)와 오프라인 구매에 적용((n,k) 확장코드 적용)하고 불법 공모자의 공모공격을 방지하고 또한 공모자의 추

표 1. 콘텐츠 영상의 Y, Cb, Cr 성분에 삽입하는 핑거프린팅 코드의 확장

Table 1. The extending of the fingerprinting code into Y, Cb and Cr elements of the content image.

BIBD 코드 (7,4,1)	Y 성분 BIBD 기반 핑거프린팅 코드	Cb 성분 (n,k) 핑거프린팅 코드	Cr 성분 LDPC 핑거프린팅 코드
0101010	0101010	0100101110	01101010101010
1001100	1001100	1010110100	00001101001100
0011001	0011001	0011100011	11011100011001
1110000	1110000	1100010000	00011001110000
0100101	0100101	0101000111	11001000100101
1000011	1000011	1011011101	10101111000011
0010110	0010110	0010001010	01111110010110

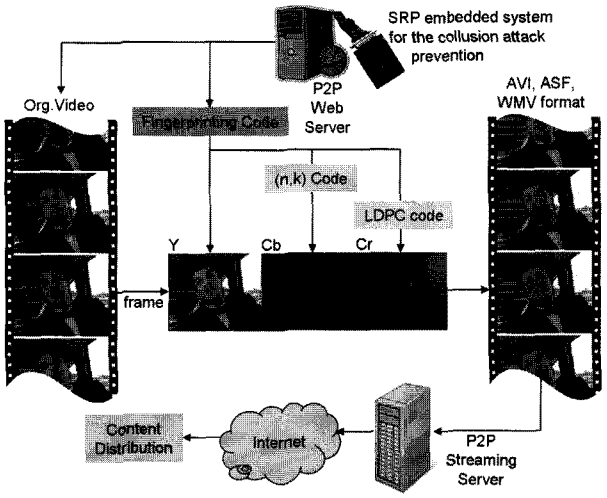

그림 1. 웹 서버에서 스트리밍 서버에 제공하는 콘텐츠의 핑거프린팅 코드 삽입

Fig. 1. Insertion fingerprinting code of the provided content to Streaming server from Web server.

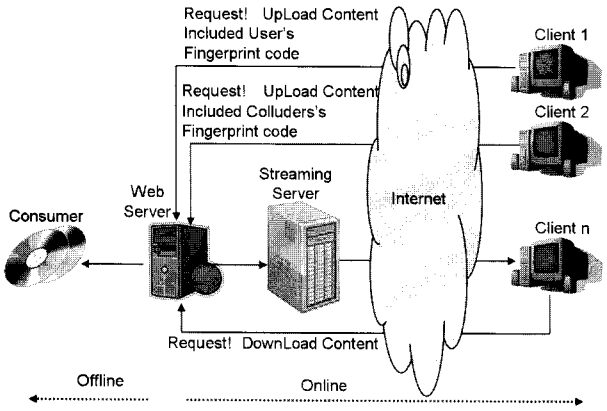

그림 2. 클라이언트에서 콘텐츠의 스트리밍 서비스의 업로드 및 다운로드 요청처리

Fig. 2. For streaming service, the request processing of the content Up/Download from Client.

적이 가능한 알고리즘을 제안한다.

그림 2에서 클라이언트 1은 정상 User가 자신의 핑거프린팅 코드가 삽입된 콘텐츠를 업로드 요청을 한다. 웹서버는 콘텐츠에 삽입된 핑거프린팅 코드가 코드북에 등록된 코드인지를 확인하면 배포 가능 콘텐츠로 분류하여 스트리밍 서버로 전송하여 P2P 네트워크 환경에서 배포할 수 있게 한다. 클라이언트 2에서 공모코드를 삽입하여 웹서버에 업로드 요청을 하면 웹서버는 콘텐츠에 삽입된 핑거프린팅 코드가 공모코드인지 검사하여 공모자 추적을 시작한다.

그리고 클라이언트 n이 요청한 콘텐츠가 정상적으로 배포 가능한 콘텐츠이면 스트리밍 다운로드 서비스를 받을 수 있다. 또한 웹서버는 오프라인에서도 콘텐츠 배포를 위한 CD 또는 DVD 등의 매체 제작을 준비하게 된다.

그림 3에서 P2P 클라이언트에서 업로드를 위하여 요청한 비디오 콘텐츠의 I-프레임 Y, Cb, Cr 성분의 비트플랜으로 부터 웹 서버는 그림 3과 같이 Y 성분에서 핑거프린팅 코드를, Cb 성분에서 (n,k) 코드를 그리고 Cr 성분에서 LDPC 코드를 검출한다. 검출된 (n,k) 코드와 LDPC 코드로 부터 핑거프린팅 코드를 복호하여 각각 원 핑거프린트와의 상관계수들을 구한다. 이들 3개의 상관계수 중 2개가 임계치 이상이거나, 또한 3개의 상관계수들의 평균값이 임계치 이상이면 업로드 할 비디오 콘텐츠는 인증이 된 정상 콘텐츠로 판정한다. 만약 여기에서 불법 콘텐츠로 판정이 되면 검출된 공모코드는 공모자 추적을 통하여 공모에 가담한 User들을 색출한다.

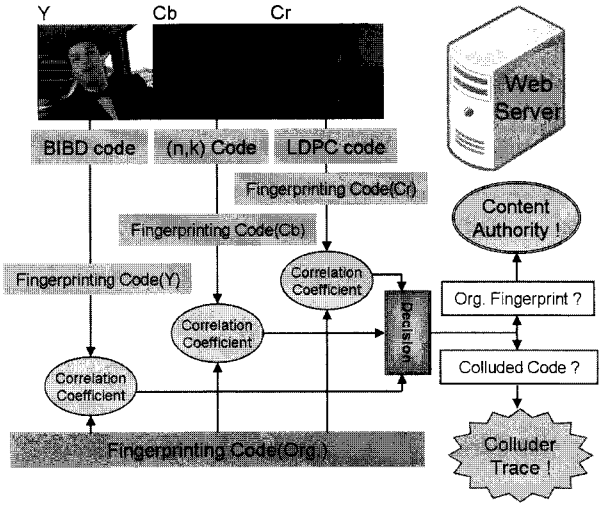

그림 3. 웹 서버에서 스트리밍 서버에 콘텐츠 등록과 공모자 추적의 결정

Fig. 3. Decision of the content registration to the Streaming server or the colluder trace in Web server.

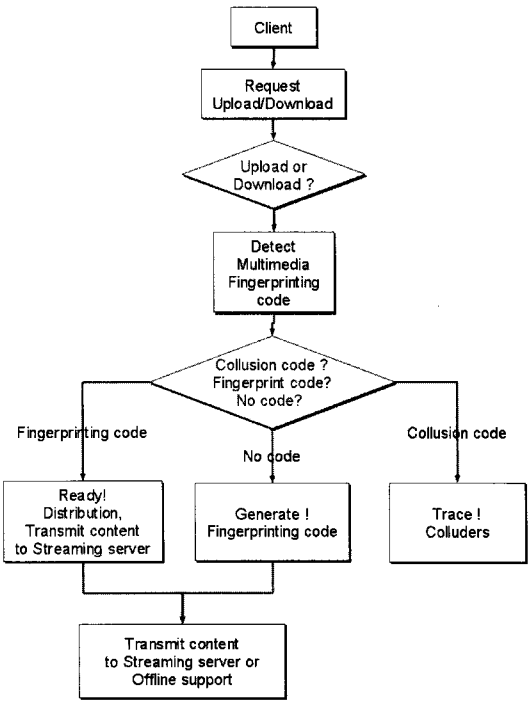

그림 4. 웹 서버에서 스트리밍 서버에 제공하는 콘텐츠의 핑거프린팅 코드 삽입

Fig. 4. Inserting fingerprinting code of the content which would be provided to Streaming server from Web server.

그림 3의 제안하는 알고리즘을 이용하여 공모공격 방지를 위한 유비쿼터스 네트워크 환경의 비디오 콘텐츠 보호를 위한 멀티미디어 핑거프린팅 코드 삽입의 플로우 챠트는 그림 4와 같다.

Ⅲ. 실험결과 및 고찰

제안된 알고리즘의 구현을 위하여 웹서버와 스트리밍 서버의 OS는 Windows Server 2003 R2이다. 그림 5는 P2P 환경에서 클라이언트 User가 웹서버에 콘텐츠의 업로드 및 다운로드 그리고 콘텐츠 배포를 요청하는 응용프로그램으로 Visual C++로 구현하였다.

웹서버는 그림 4의 플로우 챠트에 따라서 그림 3과 같이 콘텐츠의 핑거프린트의 검사 및 삽입을 통하여 인증관계를 정의하고 그림 6와 같이 스트리밍서버의 Publishing Point 디렉토리에 콘텐츠 파일을 등록한다.

그림 5의 과정과 그림 6의 과정 사이에서 본 논문에

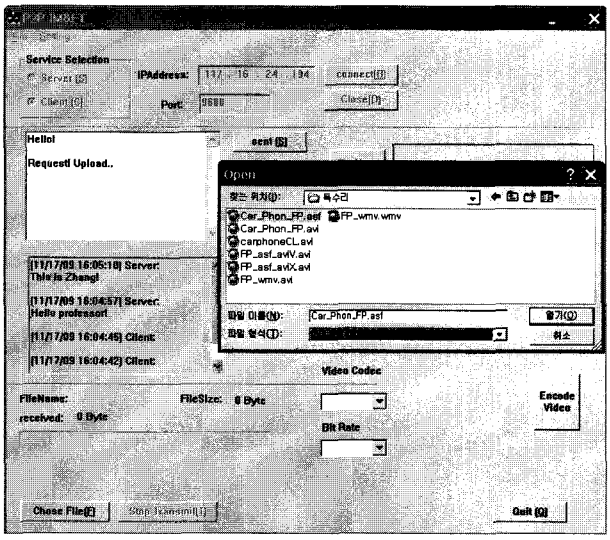

그림 5. 클라이언트 User의 비디오 콘텐츠 업로드 요청
Fig. 5. Request for upload of the video content from the client User.

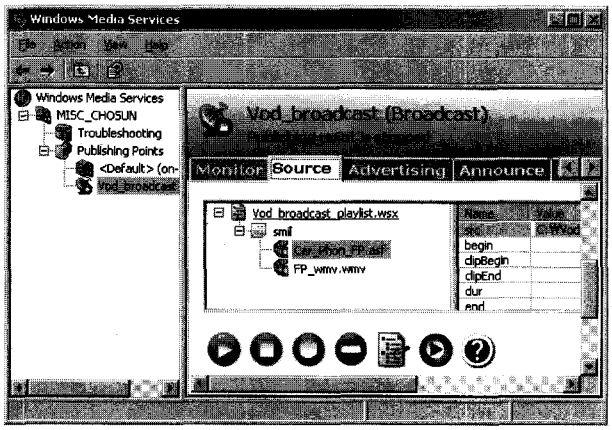

그림 6. 스트리밍 서버의 퍼블리싱 포인트 디렉토리에 등록된 인증된 비디오 콘텐츠 파일
Fig. 6. The authorized video content files is registered in Publishing Point of the streaming server.

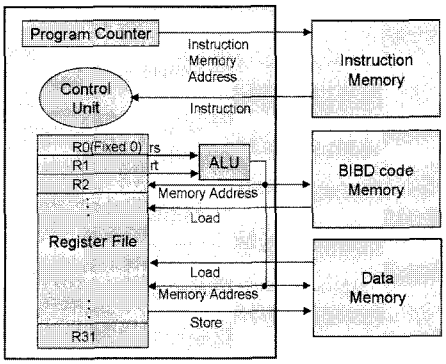

그림 7. 제안된 SRP 구조
Fig. 7. The proposed SRP architecture.

표 2. 공모공격 방지를 위한 SRP 임베디드 명령어
Table 2. SRP embedded instructions for the prevention of the collusion attack.

Category	Instruction	Operation	Comment
Multimedia Fingerprinting Code	BIBD	R1<=Memory[R2+100]	BIBD Code
	NK	R1<=Mod(Conv(Memory[R2+100],R3),2	Extension Code
	LDPC	R1<=Mod(R3*Trans(Memory[R2+100])),2	Application Code
Collusion Attack Code	AND	R1<=R2 · R3	Logical Operation
	OR	R1<=R2+R3	
	EXOR	R1<=R2⊕R3	
	AVR	R1<=R2/R3	Average Operation
Data Transfer Operation	LOAD	R1<=Memory[R2+200]	Data Memory to RF
	STR	Memory[R2+200]<=R1	RF to Data Memory

서 제안된 유비쿼터스 네트워크 환경의 멀티미디어 콘텐츠 보호를 위한 공모공격 방지의 공모 코드북 SRP 임베디드 시스템은 웹서버와 연동하여 동작되며, 명령어 구성은 표 2와 같고, 그림 7은 [9,10]을 기반으로 하여 멀티미디어 핑가프린팅 코드 생성의 "BIBD code Memory"를 추가하여 제안된 본 논문의 SRP 구조이다.

제안된 SRP 임베디드 시스템에서 표 2의 "Category"에 따라 핑거프린팅 코드는 BIBD 코드, (n,k) 확장코드, 그리고 LDPC 응용코드 세 가지로 생성되며, 공모공격 코드는 AND, OR, EXOR 그리고 AVR 연산으로 네 가지가 생성된다. 이 공모공격 코드는 의심되는 핑거프린팅 코드의 공모자를 추적하기 위해 사용된다. "Data Memory"에는 매크로 동작의 중간 값, 네 가지의 공모 연산결과의 코드 값, (n,k) 코드 연산에 사용되는 Gx 생성코드 값 그리고 LDPC 코드의 생성을 위한 [H] 메트릭스 값이 있다.

그림 7의 제안된 공모공격 방지의 SRP 임베디드 시스템은 Xilinx ISE Design Suite[TM] 환경에서 VHDL

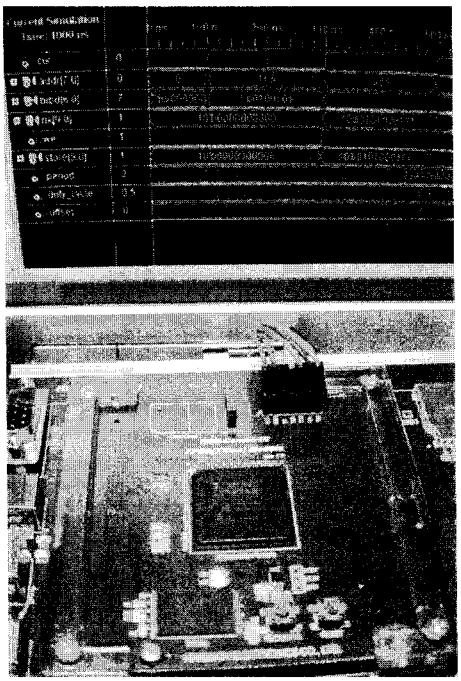

그림 8. 구현된 공모공격 방지의 SRP 임베디드 시스템과 실행 파형

Fig. 8. Implemented SRP embedded system for the prevention of the collusion attack and the executed waveform.

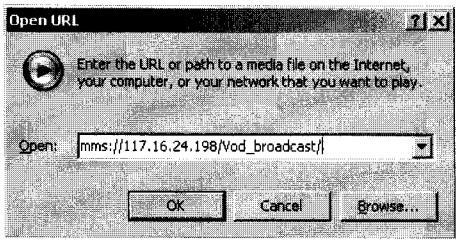

그림 9. 스트리밍 서버에 클라이언트 User의 VoD 서비스 요청

Fig. 9. VoD service request of the client' User to Streaming server.

코딩을 통하여 그림 8과 같이 Spartan XC3SD1800A [TM] FPGA에 구현되었으며, 실행파형은 "BIBD code Memory" $105의 BIBD 코드 '0100101'을 NK 명령어에 의하여 '0101000111'으로 생성된 (n,k) 확장코드를 "Data Memory" $205에 저장한다.

그림 9는 클라이언트 User가 스트리밍 서버에 핑거프린팅 코드가 처리된 인증 콘텐츠를 Widows Media Player[TM]를 통하여 서비스를 요청하는 단계이다. 그리고 실험에 사용된 비디오는 그림 10과 같이 carphone, foreman, suzie로 영상크기는 176×144(qcif)이다.

MS사의 스트리밍 미디어 형식인 ASF (Encoder: MSMPEGV3, Bit rate: 2,500Kbps) 및 MP4 (H.264/

(a) carphone (b) foreman (c) suzie

그림 10. 실험에 사용된 비디오 콘텐츠

Fig. 10. Video contents used in experiment.

그림 11. Windows Media Player에서 인증된 비디오 콘텐츠(Car_Phon_FP.asf)의 스트리밍 서비스

Fig. 11. Streaming service of the authorized video content (Car_Phon_FP.asf) on Windows Media Player.

MPEG4-AVC) 파일의 비디오 압축에서 핑거프린팅 코드의 보존을 극대화하기 위하여, 핑거프린팅 코드는 비디오 콘텐츠의 I-프레임 영상의 spatial 4:4:4 표본화 형식에서 Y, Cb, Cr 요소에 표 1의 3가지 코드를 각각 삽입하였다. 인간시각이 휘도영역 Y에 민감하기 때문에 코드길이가 짧은 BIBD 코드 자체인 멀티미디어 핑거프린팅 코드를 삽입하고, 시각의 민감성이 둔한 색채영역 Cb와 Cr에 BIBD 코드의 확장으로 생성된 (n,k) 확장코드와 LDPC 응용코드를 각각 삽입한다. Cb 성분에 삽입되는 (n,k) 코드의 생성 다항식 Gx의 차수는 round(n/2)이며, Cr 성분에 삽입된 LDPC 응용코드의 BER(Bit Error Ratio)는 AWGN -5dB~5dB까지 적용하였다. 그림 11은 그림 3의 알고리즘으로 처리가 완료되어 그림 5의 인증된 비디오 콘텐츠의 스트리밍 서비스로 디스플레이 되는 것을 보여주고 있다.

3가지 비디오 영상의 carphone, foreman, suzie의 각 I-프레임의 Y 성분의 비트플랜 0~3까지에 63, 127, 255, 511, 1023비트의 BIBD 기반 멀티미디어 핑거프린트 코드를, Cb 성분의 비트플랜 0~3까지에 94, 190,

표 3. 비디오 콘텐츠의 I-프레임 Y, Cb, Cr 성분의 비트플레인(3~0)에 삽입하는 핑거프린팅 코드길이에 따른 PSNR

Table 3. PSNR according to the fingerprinting code length is inserted in the bit plane(0~3) of the I-frame's Y, Cb and Cr components of the video content.

Finger-printing Code	Bitplane		0	0~1	0~2	0~3
1	63bits (BIBD Based)	Y	78	69	61	56
	94bits ((n,k) code Extension)	Cb	76	67	58	54
	126bits LDPC code Appl.	Cr	74	59	49	43
2	127bits (BIBD Based)	Y	74	66	57	52
	190bits ((n,k) code Extension)	Cb	72	64	56	51
	254bits LDPC code Appl.	Cr	71	56	47	41
3	255bits(BIBD Based)	Y	71	63	55	49
	382bits ((n,k) code Extension)	Cb	69	61	52	48
	510bits LDPC code Appl.	Cr	68	55	46	40
4	511bits(BIBD Based)	Y	68	60	52	46
	766bits ((n,k) code Extension)	Cb	66	58	50	45
	1,022bits LDPC code Appl.	Cr	66	51	42	36
5	1,023bits(BIBD Based)	Y	65	57	49	43
	1,534bits ((n,k) code Extension)	Cb	63	55	47	42
	2,046bits LDPC code Appl.	Cr	63	48	39	33

(삽입량 0.11%) (삽입량 : 2.43%)
(Insert ratio : 0.11%) (Insert ratio : 2.43%)

그림 12. 핑거프린팅 코드의 삽입량과 표출

Fig. 12. The insertion ratio and the expression of the fingerprinting code.

382, 766, 1534비트의 (n,k) 확장코드를, Cr성분의 비트플랜 0~3까지에 126, 254, 510, 1022, 2046bits의 LDPC 응용코드를 각각 삽입하여 측정된 평균 PSNR은 표 3과 같다.

그리고 멀티미디어 핑거프린팅 코드의 삽입량이 0.1%를 넘으면 그림 12와 같이 영상 프레임에 핑거프린팅 코드가 표출되기 시작한다.

핑거프린팅 코드가 삽입된 프레임은 다시 AVI 파일 포맷의 비디오 콘텐츠 파일로 재생성한 후, 스트리밍 서비스로 배포할 ASF와 오프라인 배포용 MP4 파일형식으로 압축하여 제공되는 과정에서 사용한 툴은 Picture2avi[TM][TM], iSkysoft Video Converter[TM] 그리고 Xilisoft Video Converter Ultimate[TM]이다.

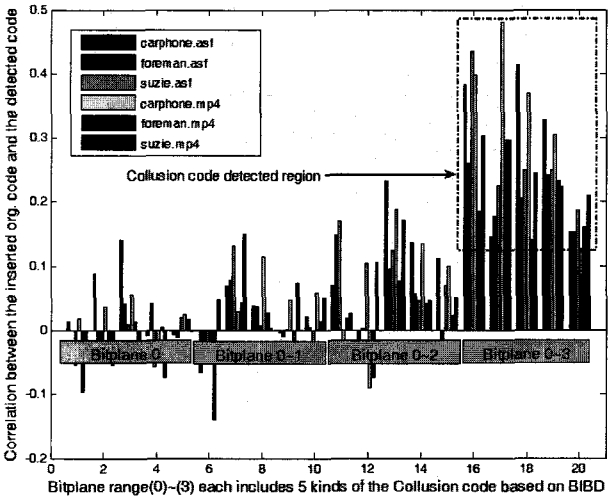

그림 13. Y 성분의 비트플레인에 삽입된 코드와 검출된 코드와의 상관계수

Fig. 13. Correlation coefficient between the inserted original code and the detected code on the bitplane of Y element.

표 4. 공모코드의 검출율과 공모자의 추적율

Table 4. The detection ratio of the collusion code and the trace ratio of the colluder.

비디오 포맷		공모코드의 검출율					공모자의 추적율				
		공모코드 비트					공모코드 비트				
		63	127	255	511	1,023	63	127	255	511	1,023
AVI	Y	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
	Cb	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
	Cr	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
ASF	Y	0.42	0.42	0.50	0.33	0.33	0.25	0.08	0.33	0.25	0.17
	Cb	0.17	0.08	0.08	0	0	0	0	0	0	0
	Cr	0.17	0.08	0	0.08	0.25	0	0	0	0	0
MP4	Y	0.25	0.42	0.50	0.33	0.25	0.17	0.25	0.17	0.25	0.08
	Cb	0.17	0	0	0	0	0.08	0	0	0	0
	Cr	0.17	0.58	0.17	0	0.17	0	0	0.08	0	0

공모공격 실험을 위하여 BIBD 코드 v의 10%로 공모자 수를 정해서 평균화공격을 위한 공모코드를 생성하여 (n,k) 확장코드 및 LDPC 응용코드로 확장하였다. 생성된 공모코드는 그림 10의 3가지 비디오 콘텐츠에 2가지 비디오 압축방식에서, 4가지의 bitplane 범위(0, 0~1, 0~2, 0~3)에 삽입되었다.

그림 13에서 Y 성분의 bitplane 0~3에 삽입된 원코드의 길이가 63, 127, 255, 511, 1023bits 5가지일 때, 검출된 코드와의 상관계수가 0.15 이상으로 높았다. 그리고 비디오 콘텐츠에 공모코드를 삽입하여 AVI 변환 및 ASF 그리고 MP4의 비디오 압축방법을 통하여 공모코

드의 검출율과 공모자의 추적율은 표 4와 같이 측정되었다. AVI 비디오 포맷에서는 Y, Cb, Cr 성분에서 공모코드의 검출율과 공모자의 추적율은 100%이었으나, ASF 및 MP4 비디오 압축에서 상관계수 0.1 이상에서, Y 성분에 삽입되는 코드의 검출율은 평균 38%이며, 0.2 이상에서 공모자 추적율은 평균 20%이었다. 이는 Cb와 Cr 성분에 삽입되는 (n,k) 확장코드와 LDPC 응용코드는 비디오의 압축을 통하여 심하게 변형됨을 알 수 있으며, (n,k) 확장코드에서 k는 n의 1/2 이상에서, LDPC 응용코드에서는 AWGN의 변화에 따른 외부잡음 첨가에 대해서는 0dB 이상에서 공모코드의 검출율과 공모자의 추적율을 높일 수 있다.

IV. 결 론

이상으로 본 논문에서 제안된 유비쿼터스 네트워크 환경의 멀티미디어 콘텐츠 보호를 위한 공모공격 방지 임베디드 시스템을 설계하였다. 공모공격 방지를 위한 공모코드의 코드북 SRP 임베디드 시스템이 최대 동작 주파수 25MHz로 구현되어 웹서버와 연동하여 동작되었다. 구현된 시스템으로 부터, P2P 환경에서 웹서버는 클라이언트 User들의 비디오 콘텐츠의 Up/Download 요청에서 멀티미디어 핑거프린팅 코드에 따라 온라인의 스트리밍 서비스와 오프라인 서비스 제공, 불법 콘텐츠의 공모코드 검출과 공모자를 추적한다. 실험을 통하여 비디오 콘텐츠의 압축에서 I-프레임의 휘도성분 Y에 삽입되는 핑거프린팅 코드의 높은 보존성이 있으나, Cb와 Cr 성분에 삽입되는 코드는 심하게 변형되었다.

DRM 기술이 콘텐츠의 유통시장에서 크게 요구됨에 따라 본 논문에서 제안된 알고리즘과 구현된 시스템이 광범위하게 응용될 것으로 기대된다.

표절논문 인용주의

{"유비쿼터스 네트워크 시스템에서의 미디어 보안에 관한 연구," 한국사이버테러정보전학회, [7권 1호-04], pp. 29-34, 2007.3}은 참고문헌 [6]을 표절한 논문으로 이를 인용할 시에 주의를 요합니다.
참조: http://paper.chosun.ac.kr (원저자 및 선임변호사)

참 고 문 헌

[1] Chu, C-C, Su, X., Prabhu, B.S., Gadh, R., Kurup, S., Sridhar, G., Sridhar, V., "Mobile DRM for Multimedia Content Commerce in P2P Networks," Consumer Comm. and Networking Conf., CCNC 2006 3rd IEEE, Vol. 2, 8-10 pp.1119-1123, Jan. 2006.

[2] Simon Byers, Lorrie Cranor, Dave Korman, Patrick McDaniel, Eric Cronin, "Analysis of Security Vulnerabilities in the Movie Production and Distribution Process," ACM Workshop DRM'03, Oct. 27, 2003, Washington, DC, USA.

[3] Wade Trappe, Min Wu, Jane Wang and K.J. Ray Liu "Anti-collusion Fingerprinting for Multimedia," IEEE Tran. on Signal Processing, Vol.51, No.4, pp.1069-1087, April 2003.

[4] In Koo Kang, Choong-Hoon Lee, Hae-Yeoun Lee, Jong-Tae Kim, Heung-Kyu Lee, "Averaging attack resilient video fingerprinting," IEEE Int'l Symposium on Circuits and Systems, ISCAS 2005, Vol. 6, pp.5529-5532, 23-26 May 2005.

[5] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," IEEE Trans. On Information Theory, 44(5):1897-1905, Sep. 1998.

[6] 노진수, 이강현 "신경회로망에 의한 공모된 멀티미디어 핑거프린트의 검출" 전자공학회논문지, 제43권 CI편 제4호, pp.80-87, 2006. 7.

[7] K.H. Rhee, "Detection of Colluded Multimedia fingerprint using LDPC and BIBD," IEEK Computer Society, Vol.43, No.5, pp.68-75, Sept. 2006.

[8] 이강현, "BIBD 기반의 멀티미디어 핑거프린팅 코드의 공모코드들에 대한 공모자 추적," 전자공학회 논문지, 제46권 CI편 제6호, pp.79-86, 2009. 11.

[9] 송상섭, 조태원, 이강현, "컴퓨터구조의 설계," Part III, 대영사, 1998. 3.

[10] http://www.lsi-contest.com/2009/siyou-1.html and http://www.radrix.com/

저 자 소 개

이 강 현(평생회원)-교신저자
대한전자공학회논문지,
제46권 CI편 제3호 참조