Journal of Korea Multimedia Society Vol. 7, No. 9, September 2004(pp. 1263-1272)

시간축 웨이블릿 변환을 이용한 블라인드 비디오 핑거프린팅

강현호[†], 박지환[††], 이혜주[†††], 홍진우[††††]

요 약

본 논문에서는 불법으로 복제된 컨텐츠의 근원지를 확인할 수 있는 핑거프린팅 기법을 제안하고 있다. 판매자와 구매자의 키로 만들어진 균일 랜덤 신호를 시간축 웨이블릿 변환에 의해 얻어진 계수 중에서 배포받을 사용자의 영역에 삽입하여 핑거프린팅을 수행하게 된다. 제안기법은 핑거프린팅된 컨텐츠에 대한 공모공격과 MPEG2 압축에도 유일한 핑거프린팅 정보를 감지할 수 있다. 특히, 핑거프린팅 정보를 삽입할 사용자의 영역 지정을 위해서 시간축 웨이블릿 변환의 특성을 이용한다. 실험에서는 비디오 컨텐츠의 불법 배포를 추적할 수 있음을 보이고, 다양한 공모공격과 MPEG2 압축에 대해 강인(robustness)함을 보인다.

Blind Video Fingerprinting Using Temporal Wavelet Transform

Hyun-Ho Kang[†], Ji-Hwan Park[††], Hye-Joo Lee[†††], Jin-Woo Hong[††††]

ABSTRACT

In this paper, we present a novel video fingerprinting implementation method to identify the source of illegal copies. The video fingerprinting is achieved by the insertion of uniform distributed random number - is made by seller and buyer's identification key - in the video wavelet coefficients by their temporal wavelet transform. The proposed fingerprinting is able to detect unique fingerprint of video contents even if they have been distorted by collusion attacks and MPEG2 compression. Especially, we use characteristics of the temporal wavelet transform to assign user's embedding area. Experimental results show the traceability of unauthorized distribution of video contents and its robustness to various collusion attacks and MPEG2 compression.

Key words: Temporal Wavelet Transform(시간축 웨이블릿 변환), Video Fingerprinting

1. 서 론

인터넷의 활성화로 다양한 디지털 컨텐츠가 쉽게 유통이 되지만 이에 따른 저작권 침해의 문제가 생겨나게 되었다. 이러한 컨텐츠의 저작권 침해를 방지 및 억제하기 위한 방법으로 디지털 워터마킹 기법이 연구되고 있다. 이러한 워터마킹 기술을 응용함에 있어서 소유자 정보와 구매자 정보를 함께 포함하는 핑거프린팅 정보를 삽입하여 불법 배포자를 추적할 수 있는 방안으로 디지털 핑거프린팅 기술이 대두되고 있다. 워터마킹 기술과의 차이는 서로 다른 구매자 정보를 삽입하기 때문에 핑거프린팅된 컨텐츠도 서로 조금씩 다르게 된다는 점이다.

디지털 핑거프린팅 기술은 식별 정보의 노출수준

※ 교신저자(Corresponding Author) : 강현호, 주소 : 부산시 남구 대연3동 부경대학교 5214A, 전화 : 051)620-6392, FAX : 051)620-6390, E-mail : hhkang@shannon.pknu.ac.kr
접수일 : 2003년 12월 31일, 완료일 : 2004년 3월 19일
[†] 준회원, 부경대학교 대학원 전자계산학과
[††] 종신회원, 부경대학교 전자컴퓨터정보통신공학부
(E-mail : jpark@pknu.ac.kr)
[†††] 준회원, 한국전자통신연구원 방송미디어연구그룹 선임연구원
(E-mail : hyejoo@etri.re.kr)
[††††] 한국전자통신연구원 방송콘텐츠연구팀장
(E-mail : jwhong@etri.re.kr)

에 따라 대칭형 핑거프린팅[1,2]과 비대칭형 핑거프린팅[3]으로 연구되었다. 대칭형 핑거프린팅(symmetric fingerprinting)은 판매자와 구매자 둘 다 핑거프린팅된 컨텐츠를 알 수 있으므로 불법적 행위시 책임 소재가 불명확하다. 이 문제를 해결하기 위한 비대칭형 핑거프린팅(asymmetric fingerprinting)은 오직 구매자만이 핑거프린팅된 컨텐츠를 알 수 있기 때문에 책임소재를 명확히 할 수 있다. 만약 판매자가 불법적인 재분배를 확인하였을 경우에 판매자는 불법 구매자를 검출하고 신뢰기관에게 이를 증명할 수 있다.

그 후 인터넷에서 디지털 컨텐츠 거래를 활성화하는데 긍정적 영향을 줄 수 있는 익명 핑거프린팅(anonymous fingerprinting)[4]에 대한 연구가 진행되었다. 익명 핑거프린팅은 비대칭형 핑거프린팅의 개념을 포함하는 프로토콜로서 판매자는 구매자에게 컨텐츠를 판매하지만 프로토콜 진행과정에서 구매자의 신원을 알지 못하도록 하는 프로토콜이다. 핑거프린팅의 경우에는 구매자마다 삽입정보가 달라지기 때문에 임의의 구매자가 인터넷상으로 판매자의 서버에 접속하여 실시간으로 핑거프린팅 프로토콜을 거치며 판매가 이루어져야만 한다. 그러나 이 방법은 높은 계산 복잡도가 필요하여 실제 구현에 불합리한 단점이 있다. 또한 식별 단계에서 등록 센터가 소수이고 판매자는 다수일 때, 등록 센터가 처리할 일이 많아진다. Domingo[5]는 식별단계에서 등록 센터의 도움을 받지 않고 판매자가 스스로 재분배자를 찾아낼 수 있게 하였지만, 식별단계에서의 공개키 디렉토리를 검색하는데 드는 비용을 고려하면 매우 비효율적임을 알 수 있다. 그 후 Pfitzmann[6]은 전자화폐를 기반으로 하여 사용자 등록 및 식별단계의 계산적 복잡도를 낮추었고, Domingo[7]는 COT(Committed Oblivious Transfer)[8]를 사용하여 컨텐츠에 정보를 삽입하는 단계에서 시간적 복잡도를 실제적으로 낮추었다. 그러나 디지털 컨텐츠 자체에 대한 공격으로 인한 핑거프린팅 정보가 손상되는 것에 대해서는 적극적인 고려가 부족하다고 할 수 있다[9].

이와 같이 핑거프린팅 프로토콜에 대한 연구는 일반적으로 디지털 컨텐츠들의 실제적인 구조에 의존적인 워터마킹 기법과는 다른 암호학적인 프로토콜의 차원에서 연구되어지는 경우가 많다. 이것은 핑거프린팅에서는 암호학적인 프로토콜 자체가 차지하는 비중이 크기 때문일 것이다. 또한, 암호학적인 프로토콜만 완성되면 실제의 구현에 있어서는 기존에 연구되어진 디지털 워터마킹 기술을 그대로 핑거프린팅에도 적용할 수 있을 것으로 생각하기 때문이다.

본 논문에서는 암호학적인 프로토콜 차원의 연구가 아닌 Wang[10]의 논문에서와 같이 임의의 컨텐츠 배포경로를 트리로 만들고, 실제 핑거프린팅 정보 삽입을 위한 비디오 컨텐츠에 대한 구조 접근은 시간축 웨이블릿 루틴을 사용하기로 한다[11]. 구현결과를 보이기 위해서 임의의 트리를 정해놓았지만 실제 응용에서는 배포되는 경로가 동적으로 할당이 되어도 문제없이 수행될 수 있다. 또한 핑거프린팅된 컨텐츠가 배포된 후 판매자가 접근할 수 없도록 자동 삭제함으로써 비대칭형 핑거프린팅 프로토콜 방식을 따를 수 있다. 이를 위해 핑거프린팅 정보를 확인할 때 판매자 컨텐츠(원본 컨텐츠)의 참조가 필요 없는 블라인드 방식을 제안하였다.

본 논문의 구성은 2장에서 비디오 프레임에 대한 삽입과정과 추출과정을 제안하고, 3장에서 실험을 통해 얻은 결과를 분석한다. 4장에서 비디오 핑거프린팅 기법에 취해 질 수 있는 각 공격들에 대한 실험결과를 보이고, 5장에 결론을 맺는다.

2. 비디오 핑거프린팅

2.1 컨텐츠 배포경로 및 삽입영역

비디오 컨텐츠가 한번 배포될 때마다 판매자와 구매자의 정보로 구성된 핑거프린팅 정보는 시간축 웨이블릿 변환에 의해 할당되어진 각 사용자의 주파수 영역에 삽입되게 된다. 즉, 판매자와 구매자 사이에는 유일한 경로가 존재한다는 것을 알 수 있고, 이 경로를 구별하기 위한 유일한 정보를 그림 1에서 숫자로 표시하였다. 예를 들면, 그림 1에서 판매자A 트리의 *node* - A_0에서 *node* - A_1으로 갈 때 컨텐츠내의 User(1), User(2), User(3)의 영역에 핑거프린팅 정보 I_1이 삽입되고, *node* - A_1에서 *node* - A_2로 갈 때 User(1), User(2)의 영역에 핑거프린팅 정보 I_2가 삽입된다. *node* - A_2에서 *node* - A_3로 갈 때는 User(1), User(2)의 영역에 핑거프린팅 정보 I_3이 삽입되고, 마지막으로 *node* - A_3에서 *node* - A_4로 갈 때는 User(1)의 영역에만 핑거프린팅 정보 I_4가 삽입되게 된다. 여기서 한번 배포될 때 마다 판매자와 구매자

가 달라지므로 다른 핑거프린팅 정보가 생성되게 된다. 최종적으로 User(1)이 구매한 컨텐츠에는 4가지의 서로 다른 핑거프린팅 정보가 삽입된다.

나머지의 경우도 동일한 방법으로 구성하면 그림 1과 같은 형태로 5명의 최종 구매자가 있는 경우에는 14개의 서로 다른 핑거프린팅 정보를 가진 경로가 존재하게 된다. 그림 1에서 핑거프린팅 정보를 나타내는 각 번호(k)는 경로를 추적하기 위한 것으로 각 유저에게 할당하여 배포 트리를 작성하게 된다. 즉, User(1)에게는 I_1부터 I_{14}까지의 14개 번호, User(2)에게는 I_{15}부터 I_{28}까지의 14개 번호, User(3)에게는 I_{29}부터 I_{42}까지의 14개 번호, User(4)에게는 I_{43}에서 I_{56}까지의 14개 번호, User(5)에게는 I_{57}에서 I_{70}까지의 14개 번호가 할당된다. 추후 불법 컨텐츠에 대해서 총70회의 핑거프린팅 정보의 존재유무를 확인하면 불법적으로 배포한 사용자를 추적할 수 있게 된다. 비디오 프레임에서 핑거프린팅 정보(I_k)를 삽입하기 위한 방법은 시간축 웨이블릿 변환[11]을 사용하여 각각의 최종 구매자 영역을 정하게 된다. 실험에서 사용된 프레임 영역은 32프레임을 두번 시간축 웨이블릿 하여 만들어진 LH(Low High)영역의 8개 프레임중에서 순서대로 5개를 선정하였다.

5명의 최종 구매자가 각각 갖고 있는 비디오컨텐츠에 삽입되어진 핑거프린팅 정보를 표 1~5에 나타내었다. 표에서 원본 비디오 컨텐츠는 최종 구매자의 수만큼 영역이 할당되어지고, 그림 1과 같은 배포경로에 따라 각 영역에 핑거프린팅 정보가 삽입되는 것이다. 각 표의 구성은 최종 구매자의 5명 각각의 영역에 대해서 한번 배포에 따라 레벨이 한 단계 올라가면서 삽입되어진 핑거프린팅 정보의 인덱스를

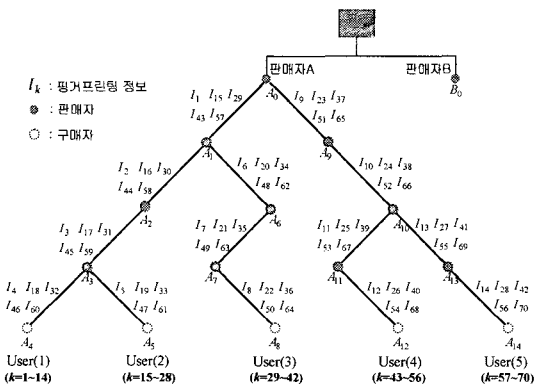


그림 1. 컨텐츠 배포 경로

표 1. User1 컨텐츠의 핑거프린팅 정보

Level	User1 Area	User2 Area	User3 Area	User4 Area	User5 Area
1	I_1	I_1	I_1		
2	I_2	I_2			
3	I_3	I_3			
4	I_4				

표 2. User2 컨텐츠의 핑거프린팅 정보

Level	User1 Area	User2 Area	User3 Area	User4 Area	User5 Area
1	I_{15}	I_{15}	I_{15}		
2	I_{16}	I_{16}			
3	I_{17}	I_{17}			
4		I_{19}			

표 3. User3 컨텐츠의 핑거프린팅 정보

Level	User1 Area	User2 Area	User3 Area	User4 Area	User5 Area
1	I_{29}	I_{29}	I_{29}		
2			I_{34}		
3			I_{35}		
4			I_{36}		

표 4. User4 컨텐츠의 핑거프린팅 정보

Level	User1 Area	User2 Area	User3 Area	User4 Area	User5 Area
1				I_{51}	I_{51}
2				I_{52}	I_{52}
3				I_{53}	
4				I_{54}	

표 5. User5 컨텐츠의 핑거프린팅 정보

Level	User1 Area	User2 Area	User3 Area	User4 Area	User5 Area
1				I_{65}	I_{65}
2				I_{66}	I_{66}
3					I_{69}
4					I_{70}

나타낸 것이다.

2.2 핑거프린팅 정보 삽입

비디오 컨텐츠에 대한 시간축 웨이블릿 변환, 최종 사용자의 영역 설정, 판매자와 구매자의 정보로 구성된 핑거프린팅 정보의 삽입을 통해 최종적으로 배포되는 비디오 컨텐츠의 과정을 그림 2에 보인다.

핑거프린팅 정보는 구매자와 판매자의 정보가 함

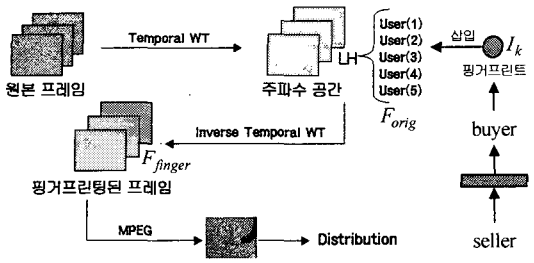


그림 2. 핑거프린팅 정보 삽입

께 포함 되어야 한다. 실험에 사용한 핑거프린팅 정보는 식(1)의 I_k 이며, 판매자가 생성한 랜덤 시퀀스에 구매자의 정보를 이용하여 재배열함으로써 생성하게 된다.

예를 들면, 핑거프린팅 정보 I_1의 생성과정을 아래에 간단히 요약한다. 단, 그림 1에서 $node-A_0$의 판매자 고유 ID는 123, $node-A_1$의 구매자 고유ID는 456, 비디오 프레임의 크기는 $m\times n$, 판매자가 되는 $node$ 값은 -1~1 사이의 실수 값, 구매자가 되는 $node$ 값은 $1\sim m\times n$ 사이의 정수 값으로 구성된다.

$$A_{0,key=123}=[A_0(1),A_0(2),\ldots,A_0(m\times n)]$$
$$A_{1,key=456}=[A_1(1),A_1(2),\ldots,A_1(m\times n)]$$
$$I_1=[A_0(A_1(1)),A_0(A_1(2)),\cdots,A_0(A_1(m\times n))]$$

실제 실험에서는 $m\times n$ 크기의 랜덤 시퀀스가 사용이 되지만, 간단히 6개의 시퀀스는 아래와 같은 *MATLAB* 코드로 구성될 수 있고 실제 생성된 값을 박스 안에 나타내었다.

```
rand('state',123)
A0 = 2*rand(1,6)-1
rand('state',456)
A1 = randperm(6)
I1 = A0(A1)
```

$$A_0=[-0.8607,\ -0.5335,\ 0.4749,\ 0.5157,\ 0.2737,\ 0.2257]$$
$$A_1=[4,2,3,5,6,1]$$
$$I_1=[0.5157,\ -0.5335,\ 0.4749,\ 0.2737,\ 0.2257,\ -0.8607]$$

핑거프린팅된 비디오 프레임을 얻기 위해서 식(1)의 삽입과정을 거친다. 그림 1에서 판매자 $node-A_k$에서 구매자 $node-A_{k+1}$로 한번 배포 될 때 마다 식(1)의 삽입과정이 수행된다. 삽입강도와 핑거프린팅 정보의 범위는 임의로 설정할 수 있으나, 본 구현에서는 삽입강도 0.5, 핑거프린팅 정보의 범위는 -1에서 1까지로 하였다.

$$F_{finger}=F_{orig}+\alpha\cdot F_{orig}\cdot I_k \quad (1)$$

F_{finger}: *fingerprinted frames*
F_{orig}: *original frames*
α: *strength*
I_k: *fingerprinting information* (*k user's path ID* $\in$ *dex*)

삽입과정은 웨이블릿 변환된 계수에 대해서 행해지고 있으며 이해를 돕기 위해 식(1)에 사용된 계수를 그림 2에 표시하였다.

2.3 핑거프린팅 정보 추출

배포되는 비디오 컨텐츠에 대한 핑거프린팅 정보의 추출 및 14개 경로로 나타내어지는 핑거프린팅 정보와의 상관도 값을 통해 불법배포를 검사하는 과정을 그림 3에 보인다.

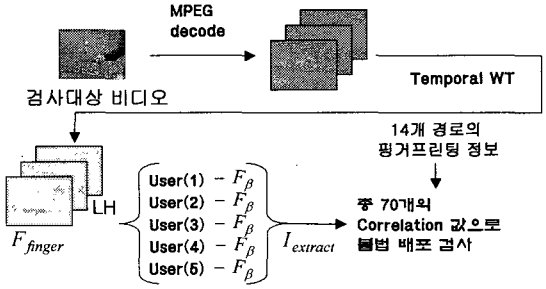


그림 3. 핑거프린팅 정보 추출

주목할 점은 핑거프린팅 정보를 추출하는데 있어서 원본 비디오 컨텐츠가 필요 없는 블라인드 기법을 구현하였다. 그림 3에서 얻어진 각각의 최종 사용자 영역 프레임(User(1), User(2), User(3), User(4), User(5))에는 원래의 비디오 신호와 핑거프린팅 정보가 섞여 있게 된다. 이러한 두 신호의 혼선을 줄이기 위해 F_β 라는 프레임을 식(2)와 같이 정의한다. F_β 프레임은 저주파 성분 프레임(LL성분)과 최종 사용자 영역 프레임(LH성분의 각 사용자 영역)을 제외한 임의의 프레임으로 정의한다. 본 정의에서는 고주파 성분(HH성분)의 첫 번째 프레임을 사용하는 것이 가장 좋은 성능을 보였음을 실험을 통해 확인하였다. 따라서 본 논문의 구현에서는 HH성분의 첫 번째 프레임을 F_β로 사용하여 실험을 하였다.

$$I_{extract}=F_{finger}-F_\beta \quad (2)$$

$I_{extract}$: *extracted fingerprinting information*

F_{finger} ; *fingerprinted frame*

F_{β} : $F_{finger}[LL], F_{finger}[LH(User(1), User(2), User(3), User(4), User(5))]$

을 제외한 frames

추출과정은 웨이블릿 변환된 계수에 대해서 행해지고 있으며 이해를 돕기 위해 식(2)에 사용된 계수를 그림 3에 표시하였다.

비디오 컨텐츠(예: 32개 프레임)에 대한 시간축 웨이블릿 변환, 최종 사용자(예: 5명)의 프레임 장소, F_{β} 프레임으로 사용할 수 있는 프레임을 그림 4에 나타내었다.

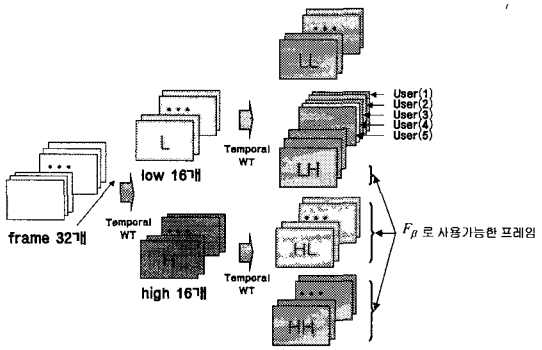


그림 4. 시간축 웨이블릿 변환 후 최종 사용자 프레임과 F_{β} 프레임

상관도 계산은 식(3)과 같은 linear correlation을 사용하였다. Linear correlation은 additive white Gaussian noise의 혼재에 있어서 신호를 감지할 수 있는 최적의 상관도로 알려져 있다. 본 논문에서는 핑거프린팅 정보를 추출하기 위하여 원본 비디오 컨텐츠를 사용하지 않고 F_{β} 프레임을 사용하였다. 이 F_{β} 프레임과의 차분을 구하는데 있어서 additive white Gaussian noise 형태의 잡음이 섞이게 되고, 이러한 환경에 가장 적절한 상관도는 linear correlation임을 실험을 통해서 확인하였다.

$$Cor=\frac{1}{N}\sum I_{original}\cdot I_{extract} \qquad (3)$$

(*N*: *frame size*)

$I_{original}$: *origianl fingerprinted information*

3. 실험 및 결과

사용한 비디오는 table-tennis(240*360) 32개 프레임이고, MATLAB 프로그램에 의해 실험을 수행하였다. 그림 5의 상관도 계산 결과를 분석하기 위하여 그림 1의 컨텐츠 배포경로를 참조하여야 한다. 그림 5의 User(1) 영역을 보면 핑거프린팅 정보 $I_1 \rightarrow I_2 \rightarrow I_3 \rightarrow I_4$에서 높은 상관도 값을 얻었다. 이 경로를 그림 1의 컨텐츠 배포경로에 대응시키면 최종 구매자 User(1) 에게 배포된 것을 알 수 있다. 마찬가지로 User(2) 영역을 보면 핑거프린팅 정보 $I_{15} \rightarrow I_{16} \rightarrow I_{17}$에서 높은 상관도 값을 얻었다. 이 경로를 그림 1의 컨텐츠 배포경로에 대응시키면 *node* - A_3까지 배포된 것을 알 수 있다. User(3) 영역을 보면 핑거프린팅 정보 I_{29}에서 높은 상관도 값을 얻었다. 이 경로를 그림 1의 컨텐츠 배포경로에 대응시키면 *node* - A_1까지 배포된 것을 알 수 있다. 즉, 그림 5로부터 최종 비디오 컨텐츠의 구매자는 User(1)임을 알 수 있다. 이와 같은 형태로 분석하면 불법 컨텐츠 배포자의 추적을 수행할 수 있다.

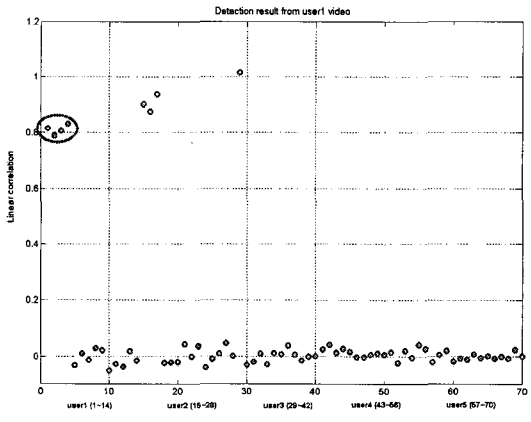


그림 5. User(1) 컨텐츠의 핑거프린팅 정보 검사

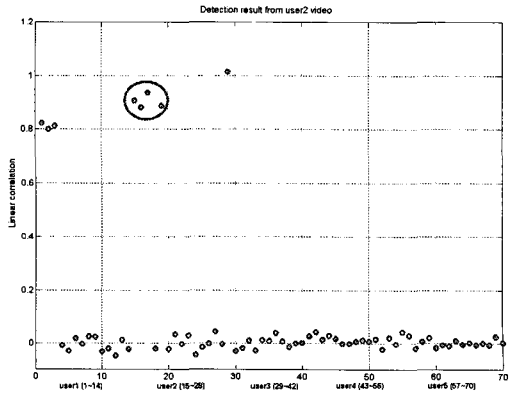


그림 6. User(2) 컨텐츠의 핑거프린팅 정보 검사

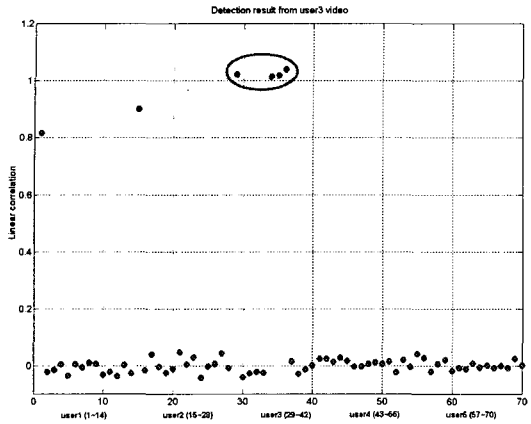


그림 7. User(3) 컨텐츠의 핑거프린팅 정보 검사

위와 같은 방식으로 그림 1의 컨텐츠 배포경로를 참고로 분석하면 이후의 결과에 대해서도 마찬가지의 결론을 얻을 수 있다. 즉, 그림 6의 경우 User(2) 영역의 $I_{15} \rightarrow I_{16} \rightarrow I_{17} \rightarrow I_{19}$에서 높은 상관도 값을 얻었고, 그림 7의 경우 User(3) 영역의 $I_{29} \rightarrow I_{34} \rightarrow I_{35} \rightarrow I_{36}$에서 높은 상관도 값을 얻었다. 그림 8의 경우 User(4) 영역의 $I_{51} \rightarrow I_{52} \rightarrow I_{53} \rightarrow I_{54}$에서 높은 상관도 값을 얻었고, 그림 9의 경우 User(5) 영역의 $I_{65} \rightarrow I_{66} \rightarrow I_{69} \rightarrow I_{70}$에서 높은 상관도 값을 얻었다.

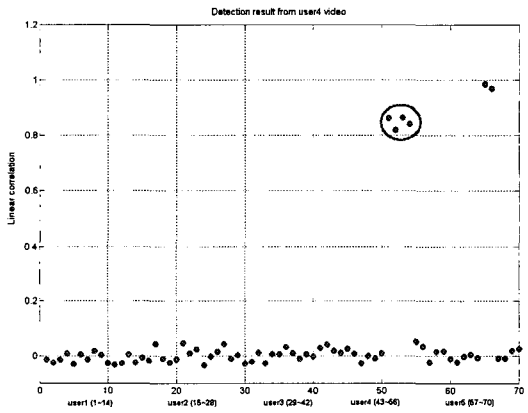


그림 8. User(4) 컨텐츠의 핑거프린팅 정보 검사

4. 각 공격에 대한 견고성

본 논문에서 다루어진 공격 실험은 크게 두 가지이다. 첫째는 핑거프린팅의 요구사항에서 중요하게 다루어지는 공모공격에 대한 것이고, 둘째는 컨텐츠

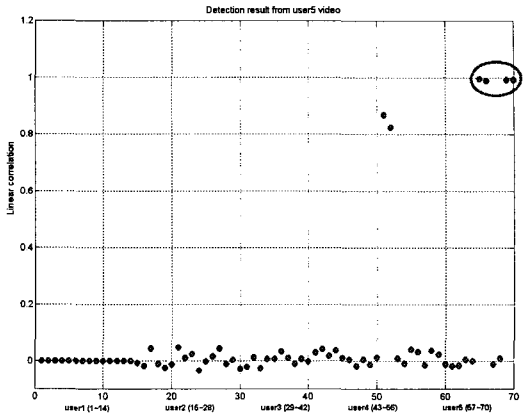


그림 9. User(5) 컨텐츠의 핑거프린팅 정보 검사

가 MPEG2의 압축을 통해 배포되는 것이 일반적이므로 이에 대한 견고성 실험이다.

4.1 공모공격

본 논문에서 구현된 각종 공모공격은 문헌[14]에 기반하여 수행하였다.

4.1.1 평균화 공모공격(Averaging Collusion Attack)

평균화 공모공격은 Cox[12]의 논문에 의해 소개되었는데 핑거프린팅된 다수의 컨텐츠를 서로 평균하여 새로운 컨텐츠를 생성하는 공격법이다. 본 실험에서는 User(1), User(2), User(3)이 갖고 있는 비디오 컨텐츠에 대한 평균화 공모공격을 실험한다. 실험결과에 있어서 주목할 점은 누가 서로 공모하였는가에 초점을 맞추어야 할 것이다. 그림 10의 경우, 그림 1의 컨텐츠 배포경로를 참조하면 User(1), User(2), User(3)의 핑거프린팅 정보가 다른 값에 비하여 상관도가 크므로 User(1), User(2), User(3)이 공모하였음을 알 수 있다.

4.1.2 최대 최소 공모공격(Maximum-Minimum Collusion Attack)

더욱 강력한 공모공격이 Stone[13]의 논문에 의해 소개되었는데 공모 처리된 비디오 컨텐츠는 실제 평균값 대신에 최대 값과 최소 값 사이의 중간 값을 얻게 된다. 결과적으로 공격된 워터마크 시퀀스는 실제 워터마크 신호를 덜 포함하게 되고, 이로 인해 상

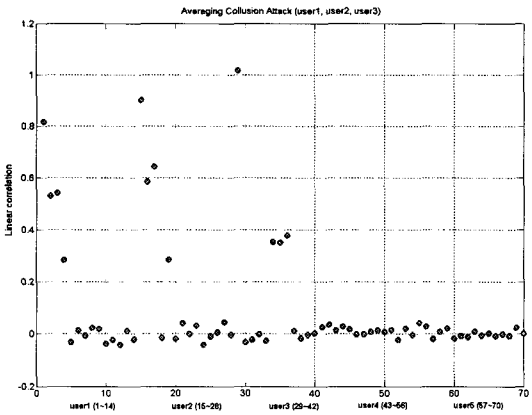


그림 10. 평균화 공격 후 핑거프린팅 정보 검사 (User(1), User(2), User(3))

관도 값은 낮아지게 된다. 그림 11의 경우도 User(1), User(2), User(3)의 상관도 값이 높기 때문에 이들이 공모했음을 알 수 있다.

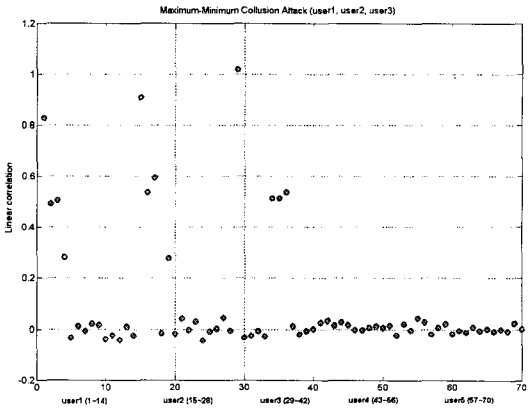


그림 11. 최대 최소 공격 후 핑거프린팅 정보 검사 (User(1), User(2), User(3))

4.1.3 상관계수 음수화 공모공격(Negative-Correlation Collusion Attack)

상관계수 음수화 공모공격은 상관계수를 이용하여 핑거프린팅 정보를 추출할 경우, 상관계수의 값을 음수로 만들어 공모자의 추출을 어렵게 만드는 공격법이다[13]. 그림 12의 경우, 그림 1의 컨텐츠 배포 경로를 참조하면 User(1), User(2), User(3)의 핑거프린팅 정보가 다른 값에 비하여 상관도가 크므로 User(1), User(2), User(3)이 공모했음을 알 수 있다.

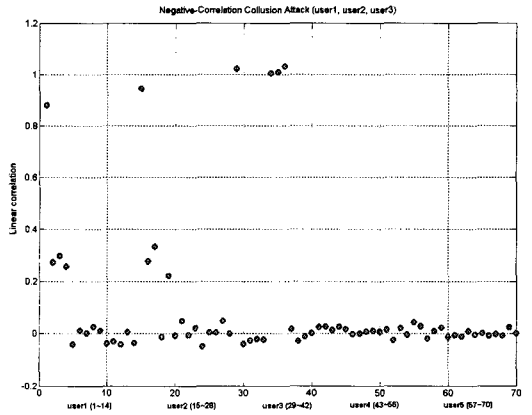


그림 12. 상관계수 음수화 공격 후 핑거프린팅 정보 검사 (User(1), User(2), User(3))

4.1.4 상관계수 제로화 공격(Zero-Correlation Collusion Attack)

상관계수 제로화 공격은 상관계수를 제로에 가깝게 유도하여 핑거프린팅 정보의 검출이 불가능하도록 만드는 공격법이다[14]. 그림 13의 경우 그림 1의 컨텐츠 배포경로를 참조하면 User(1), User(2), User(3)의 핑거프린팅 정보가 다른 값에 비하여 상관도가 크므로 User(1), User(2), User(3)가 공모했음을 알 수 있다.

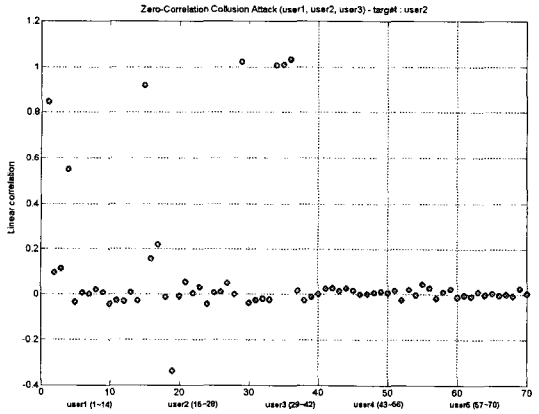


그림 13. 상관계수 제로화 공격 후 핑거프린팅 정보 검사 (User(1), User(2), User(3))

4.2 MPEG2 압축에 대한 견고성[15]

일반적으로 MPEG2에서는 4~10 Mbits/s정도의 화질을 사용하고 있으므로 본 실험에서는 4Mbits/s

에서 수행하였다. 본 논문에 그림으로 제시를 하지는 않았지만 2Mbits/s의 화질에서도 핑거프린팅 정보를 모두 추출하여 배포경로를 알 수가 있었음을 밝혀둔다. 이후의 그림에서는 전체적으로 공격이 없을 때보다 상관도 값이 낮아졌지만 핑거프린팅 정보를 확인할 수 있는 충분한 상관도 값을 보여준다.

3장에서 분석한 방법으로 살펴보면 다음과 같다. 그림 14의 User(1) 영역을 보면, 핑거프린팅 정보 $I_1 \rightarrow I_2 \rightarrow I_3 \rightarrow I_4$에서 높은 상관도 값을 얻었다. 이 경로를 그림 1의 컨텐츠 배포경로에 대응시키면 최종 구매자 User(1) 에게 배포된 것을 알 수 있다. 마찬가지로 User(2) 영역을 보면, 핑거프린팅 정보 $I_5 \rightarrow I_6 \rightarrow I_7$에서 높은 상관도 값을 얻었다. 이 경로를 그림 1의 컨텐츠 배포경로에 매치시키면 *node* - A_3까지 배포된 것을 알 수 있다. User(3) 영역을 보면, 핑거프린팅 정보 I_{29}에서 높은 상관도 값을 얻었다. 이 경로를 그림 1의 컨텐츠 배포경로에 매치시키면 *node* - A_1까지 배포된 것을 알 수 있다. 즉, 그림 14로부터 최종 비디오 컨텐츠의 구매자는 User(1)임을 알 수 있다.

그림 15의 경우도 위에서 분석한 방법에 따르면 최종 비디오 컨텐츠의 구매자는 User(5)임을 알 수 있고 나머지 경우도 같은 방법에 의해 최종 비디오 컨텐츠의 구매자를 확인할 수 있다.

MPEG2 압축에 대한 강인성은 디지털 컨텐츠 핑거프린팅 구현에 있어서 필수적인 요소라고 할 수 있다. 본 논문의 실험에서는 간단한 비디오 프레임에

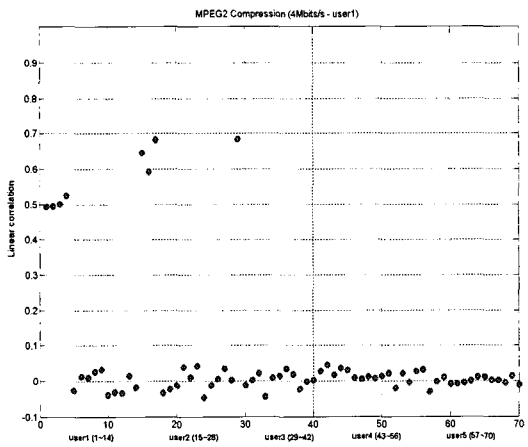


그림 14. MPEG2 압축후 핑거프린팅 정보 검사 (4Mbits/ s) ← User(1)

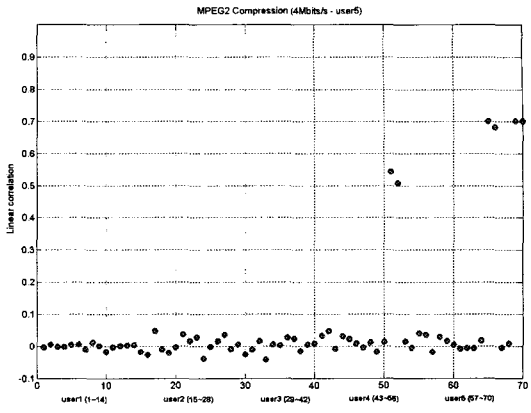


그림 15. MPEG2 압축후 핑거프린팅 정보 검사 (4Mbits/s) ← User(5)

대한 적용이지만 실제 방송국에서 보유하고 있는 방송 컨텐츠의 배포에 있어서 충분히 고려해서 적용할 수 있을 것이다.

5. 결 론

핑거프린팅 기법에 대한 대부분의 연구는 디지털 컨텐츠들의 실제 구조 차원과는 독립적으로 암호학적인 프로토콜의 차원에서 연구되어 지고 있다. 암호학적인 프로토콜만 완성되면 실제 정보 삽입의 구현은 기존 워터마킹 기술을 그대로 적용하면 되기 때문이다. 그러나 기존의 암호학적 프로토콜에 대한 연구는 디지털 컨텐츠 자체에 대한 공격으로 인해 핑거프린팅 정보가 손상되는 것에 대해서는 적극적으로 고려하지 않는 문제점이 있다. 효율적인 핑거프린팅 프로토콜이 실효를 거두기 위해서는 컨텐츠에 대한 공격을 고려하는 프로토콜로 발전되어야 할 것이다.

본 논문에서는 이러한 접근을 기존의 암호 알고리즘이나 보안코드 개발의 측면이 아닌 워터마킹 기술을 이용한 실제 구현의 측면에서 접근하였다. 특히, 비디오 프레임에 대한 삽입방법에 있어서 시간축 웨이블릿 변환을 활용함으로써 다양한 공격에 강인하게 할 수 있었다.

구현된 시스템의 성능평가를 위해 가장 중요하다고 할 수 있는 공모공격과 MPEG2 압축에 대한 실험을 하여 만족할 만한 강인성을 얻을 수 있었다. 추후, 효율적인 암호학적 핑거프린팅 프로토콜과의 접목을 통한 보다 안전한 시스템의 개발을 고려할 예정이다.

참 고 문 헌

[1] N. R. Wagner, "Fingerprinting," *Proc. IEEE Symposium on Security and Privacy*, pp. 18-22, 1983.

[2] G. R. Blakely, C. Meadows, and G. B. Purdy, "Fingerprinting long forgiving messages," *in Advances in Cryptology, Proc. of CRYPTO'85*, vol.218 of Lecture Notes in Computer Science, Springer Verlag, pp. 87-119, 1987.

[3] B. Pfitzmann, M. Schunter, "Asymmetric Fingerprinting," in *Advances in Cryptology, Proc. of EUROCRYPT'96*, vol.1070 of Lecture Notes in Computer Science, Springer Verlag, pp. 84-95, 1996.

[4] B. Pfitzmann, M. Waidner, "Anonymous Fingerprinting," in *Advances in Cryptology, Proc of EUROCRYPT'97*, vol.1233 of Lecture Notes in Computer Science, Springer-Verlag, pp. 88-102, 1997.

[5] J. Domingo-Ferrer, "Anonymous Fingerprinting of Electronic Information with Automatic Identification of Redistributors," *IEE Electronics Letters*, vol.34, no.13, pp. 1303-1304, 1998.

[6] B. Pfitzmann, A. Sadeghi, "Coin-Based Anonymous Fingerprinting," in *Advances in Cryptology, Proc of EUROCRYPT'99*, vol.1592 of Lecture Notes in Computer Science, Springer-Verlag, pp. 150-164, 1999.

[7] J. Domingo-Ferrer, "Anonymous Fingerprinting Based on Committed Oblivious Transfer," Second International Workshop on Practice and Theory in Public Key Cryptography, *Proc of PKC'99*, vol.1560 of Lecture Notes in Computer Science, Springer-Verlag, pp. 43-52, 1999.

[8] C. Crepeau, J. van de Graaf, and A. Tapp, "Committed Oblivious Transfer and Private Multi-party Computation," in *Advances in Cryptology, Proc of CRYPTo'95*, vol.963 of Lecture Notes in Computer Science, Springer-Verlag, pp. 110-123, 1995.

[9] 여상수, 윤훈기, 김성권, "디지털 컨텐츠의 지적 재산권 보호를 위한 익명 핑거프린팅의 연구 동향," 한국정보보호학회지, 제11권, 제3호, 2001. 6.

[10] Y. Wang, J. Doherty, and R. V. Dyck, "A Watermarking Algorithm for Fingerprinting Intelligence Images," *2001 Conference on Information Sciences and Systems*, The Johns Hopkins University, Mar. 2001.

[11] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution Scene-based Video Watermarking using Perceptual Models," *IEEE Journal on Selected Areas in Comm.*, vol.16, no.4, pp. 540-550, May 1998.

[12] I. J. Cox, J. Kilian, T. Leighton, and T. Shanmoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Trans. on Image Processing*, vol.6, no.12, pp. 1673-1687, 1997.

[13] H. Stone, "Analysis of Attacks on Image Watermarks with Randomized Coefficients," *NEC Technical Report*, 1996.

[14] V. Wahadaniah, Y. L. Guan, and H. C. Chua, "A New Collusion Attack and Its Performance Evaluation," *Digital Watermarking First International Workshop, IWDW2002*, vol.2613 of Lecture Notes in Computer Science, Springer Verlag, pp. 64-80, Aug. 2003.

[15] http://www.mpeg.org

강 현 호

1999년 동의대학교 컴퓨터공학과 졸업(공학사)
2001년 부경대학교 대학원 전자계산학과 졸업(이학석사)
2002년~현재 부경대학교 대학원 전자계산학과 박사과정

관심분야 : 디지털 워터마킹, 신호처리

박 지 환

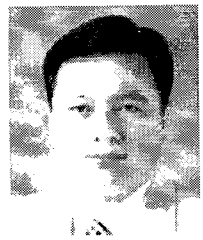
1984년 경희대학교 전자공학과 (공학사)
1987년 일본 국립 전기통신대학 정보공학과(공학석사)
1990년 일본 요코하마국립대학 전자정보 공학과(공학박사)
1990년~현재 부경대학교 전자컴퓨터정보통신공학부 교수
1996년~현재 동경대학 생산기술연구소 협력연구원
1997년~현재 한국정보보호학회 이사
1998년~현재 한국멀티미디어학회 운영위원 및 논문지 편집위원
1999년~현재 한국정보처리학회 논문지 편집위원
2002년~현재 한국정보보호학회 영남지부장 및 논문지 편집위원

관심분야 : 멀티미디어 컨텐츠 보호 및 응용, 암호학

이 혜 주

1994년 2월 부경대학교 전자계산학과 학사
1997년 2월 부경대학교 대학원 전자계산학과 석사
2000년 2월 부경대학교 대학원 전자계산학과 박사
2000년 6월~2001년 2월 한국정보통신대학원대학교 박사후연구과정생
2001년 3월~현재 한국전자통신연구원 방송미디어연구그룹 선임연구원

관심분야 : 디지털 비디오 신호처리 및 부호화, 디지털 워터마킹



홍 진 우

1982년 2월 광운대학교 응용전자공학과 학사
1984년 2월 광운대학교 대학원 전자공학과 석사
1993년 8월 광운대학교 대학원 전자계산기공학과 박사
1998년~1999년 독일 프라운호퍼 연구소(교환연구원)
1984년 3월~현재 한국전자통신연구원 방송콘텐츠연구팀장(책임연구원)

관심분야 : 오디오 신호처리 및 부호화, 디지털 콘텐츠 보호 및 관리, 디지털 오디오 방송