

시간축 웨이블릿 변환에 의한 비디오 핑거프린팅

강현호*, 박지환**, 이해주***, 홍진우***

*부경대학교 대학원 전자계산학과

**부경대학교 전자컴퓨터정보통신공학부

***ETRI 전파방송연구소 방송미디어부

Video Fingerprinting based on the Temporal Wavelet Transform

Hyun-Ho Kang*, Ji-Hwan Park**, Hye-Joo Lee***, Jin-Woo Hong***

*Department of Computer Science, Pukyong National University

**Div. of Electronic, Computer & Telecom. Eng., Pukyong National University

***Broadcasting Media Department, Radio and Broadcasting Laboratories, ETRI

요약

본 논문에서는 비디오 콘텐츠 내에 소유자와 구매자 정보를 함께 포함하는 핑거프린팅 정보를 삽입하여 불법으로 배포된 핑거프린팅 콘텐츠로부터 배포자가 누구인지를 추적할 수 있는 기법을 보인다. 특히, 문헌[1]에서 제시된 시간축 웨이블릿 변환을 이용하여 핑거프린팅 정보가 삽입될 영역을 분리해 주고, 역 변환을 통해 전 영역의 비디오 프레임에 정보가 삽입되게 된다. 이로 인해 핑거프린팅된 콘텐츠의 상이성을 이용한 기존의 여러 공모공격에도 강인함을 보이고 있다. 또한, 비디오 콘텐츠의 특성상 MPEG2의 압축에도 불법 배포자를 추적할 수 있는 강인함을 보인다.

1. 서론

인터넷의 활성화로 다양한 디지털 콘텐츠가 쉽게 유통이 되지만 이에 따른 저작권 침해의 문제가 생겨나게 되었다. 이러한 콘텐츠의 저작권 침해를 방지 및 억제하기 위한 방법으로 디지털워터마킹 기법이 연구되고 있다. 콘텐츠의 소유권을 확인하는 이러한 워터마킹의 기술에 불법 배포자를 역추적할 수 있는 방안으로 소유자 정보와 구매자 정보를 함께 포함하는 핑거프린팅 정보를 삽입하여 해결할 수 있다.

핑거프린팅 기술은 암호학적 방식을 이용할 때 대칭형 핑거프린팅 기법[2]과 불법 유통시킨 주체를 명확히 하기 위한 비대칭형 핑거프린팅 기법[3]으로 연구되었다. 최근은 비대칭성과 익명성을 효율적으로 충족시키기 위한 방향의 연구가 진행되고 있다. 듀얼 워터마킹 방식을 이용할 때는 기존 워터마킹 시스템의 보안성을 보완하고 여기에 핑거프린팅 기능까지 포함시켜 MS사의 미디어 플레이어 플랫폼에 구현된 연구가 있다[4]. 또한, 핑거프린팅된 콘텐츠의 상이성을 이용한 공모공격에 강인하기 위한 보안코드의 연구도 진행되고 있다[5].

본 논문은 Wang[6]의 논문에서와 같은 임의의 콘텐츠 배포경로를 트리로 만들고 비디오 콘텐츠에 대한 접근은 문헌[1]에서 구현된 시간축 웨이블릿 루틴을 사용하기로 한다. 구현결과를 보이기 위해서 임의의 트리를 정해놓았지만 실제응용에서는 배포되는 경로가 동적으로 할당이 되어도 문제없이 수행될 수 있다.

본 논문의 구성은 2장에서 비디오 프레임에 대한 삽입과정과 추출과정을 다루고, 3장에서 실험을 통한 결과 분석을 다룬다. 4장에서는 비디오 핑거프린팅 기법에 있어서 다루어 질 수 있는 공격들에 대한 실험 결과를 보이고 결론을 맺는다.

2. 제안방법

2.1 콘텐츠 배포경로 및 삽입영역

콘텐츠가 한번 배포될 때 판매자와 구매자의 정보로 구성된 핑거프린팅 정보가 각 유저의 콘텐츠 영역에 삽입되게 된다. 예를 들면 그림1에서 간선 I로 갈 때 user1, user2, user3의 영역에 핑거프린팅 정보가 삽입되고, 간선 II로 갈 때 user1, user2의 영역에 핑거프린팅 정보가 삽입된다. 간선 III경로로 갈 때는 user1, user2의 영역에 핑거프린팅 정보가 삽입되고, 마지막으로 간선 IV로 갈 때는 user1 영역에만 핑거프

※ 본 연구는 ETRI 지원으로 수행되었음

린팅 정보가 삽입되게 된다. 여기서 한번 배포될 때마다 구매자와 판매자가 달라지므로 다른 핑거프린팅 정보가 생성되게 된다. 최종적으로 user1이 갖고 있는 콘텐츠에는 4가지의 서로 다른 핑거프린팅 정보가 user1 영역, user2 영역, user3 영역에 나누어져 삽입되어 있는 것이다. 나머지 경우도 동일한 방법으로 구성하면 아래와 같은 배포경로의 경우에는 14개의 서로 다른 핑거프린팅 정보가 존재하게 된다. 그림1의 번호는 경로를 추적하기 위해 각 유저에게 할당하여 배포트리를 작성한 것이다. 즉, user1에게는 (1)부터 (14)까지의 14개 번호, user2에게는 (15)부터 (28)까지의 14개 번호, user3에게는 (29)부터 (42)까지의 14개 번호, user4에게는 (43)에서 (56)까지의 14개 번호, user5에게는 (57)에서 (70)까지의 14개 번호가 할당된다. 추후 불법 콘텐츠에 대해서 총70회의 핑거프린팅 정보의 존재유무를 확인하면 불법적으로 배포한 사용자를 추적할 수 있게 된다.

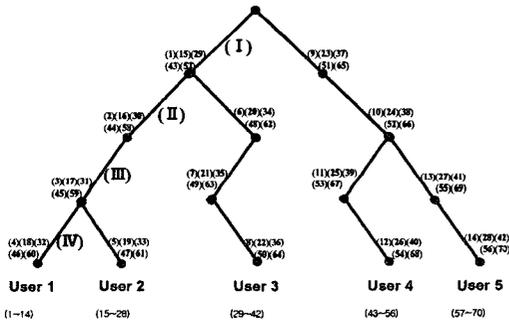


그림 1. 콘텐츠 배포경로

비디오 프레임에서 핑거프린팅 정보를 삽입하기 위한 방법은 문헌[1]에서 구현된 시간축 웨이블릿 변환 루틴을 사용하여 그림2와 같은 각각의 유저 영역을 정하게 된다. 실험에서 사용된 프레임 영역은 32프레임을 두번 시간축 웨이블릿 하여 만들어진 LH(Low High)영역의 8개 프레임중에서 순서대로 5개를 선정하였다.

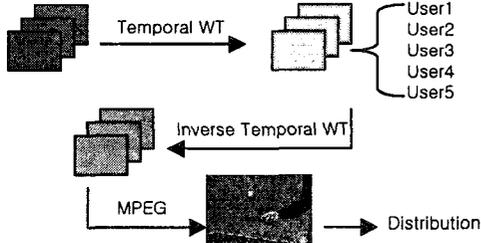


그림 2. 비디오 프레임에서 삽입영역

2.2 핑거프린팅 정보 삽입

핑거프린팅 정보는 구매자와 판매자의 정보가 함께

포함 되어야 한다. 실험에서 핑거프린팅 정보는 식(1)에서 M이 되는데 판매자가 생성한 랜덤 시퀀스에 구매자의 정보를 이용하여 재배열 함으로써 핑거프린팅 정보를 생성하게 된다.

$$F_{new} = F_{old} + \alpha \cdot F_{old} \quad (1)$$

F_{new} : fingerprinted frame

F_{old} : original frame

α : strength

M : uniformly distributed

random number(-1 ~ 1)

핑거프린팅된 프레임은 식1과 같은 과정을 거쳐서 그림2에서 보듯이 역 시간축 웨이블릿 변환을 거치게 된다.

2.3 핑거프린팅 정보 추출

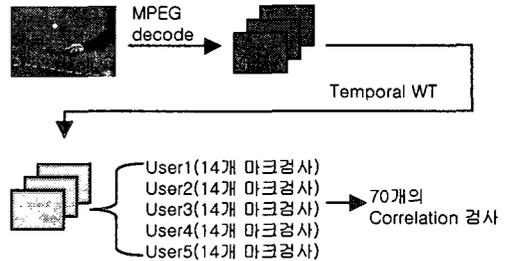


그림 3. 배포된 비디오 콘텐츠로부터 검사

핑거프린팅 정보의 추출은 원본을 이용하여 식(2)와 같이 추출할 수 있다.

$$M_{new} = F_{attack} - F_{old} \quad (2)$$

$(M_{new} : \text{extracted fingerprint})$

상관도 계산은 식(3)과 같은 linear correlation 으로 수행할 수 있다.

$$Cor = \frac{1}{N} \sum M_{new} M \quad (3)$$

$(N : \text{size of } M)$

3. 실험 및 결과

실험에 사용된 비디오는 240*360 크기의 32개 프레임이고 Matlab 프로그램에 의해 수행되었다.

그림4의 상관도 계산 결과를 분석하려면 그림1의 콘텐츠 배포경로를 참조하여야 한다. 그림4는 1 → 2 → 3 → 4의 경로로 user1영역에서 감지되었고, 15 → 16 → 17의 경로로 user2영역에서 감지되었고, 29경로가 user3영역에서 감지되었다. 즉, 그림1에서 user1의

컨텐츠 배포 경로와 일치하므로 최종 구매자는 user1 이 된다. Y축은 상관도를 나타내며, user1에 해당하는 (1)~(4)가 모두 다른 값에 비하여 크게 검출되었기 때문에 배포된 컨텐츠가 user1에 의한 것임을 특정할 수 있다.

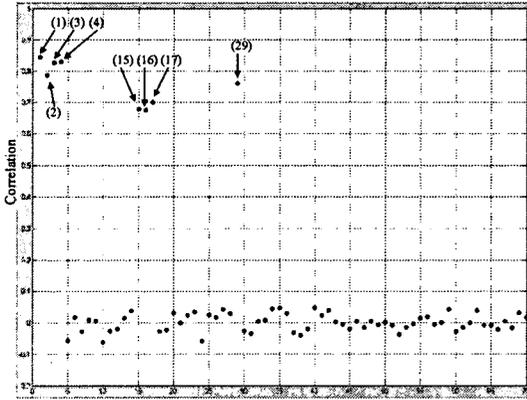


그림 4. 상관도 계산 (user1이 받은 비디오 프레임)

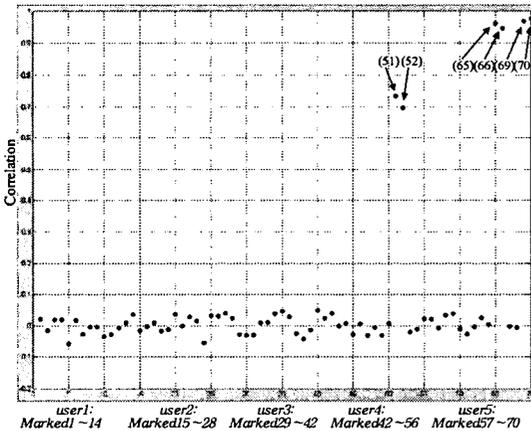


그림 5. 상관도 계산 (user5가 받은 비디오 프레임)

동일한 방법으로 분석하면 발견된 비디오 프레임에 대한 70개의 상관도 분석을 통하여 배포된 경로를 추적하는 것이 가능하게 된다.

4. 공격에 대한 실험결과

본 논문에서 다루어진 공격 실험은 크게 두 가지이다. 첫째로 핑거프린팅의 요구사항에서 중요하게 다루어지는 공모공격에 대한 것이고, 비디오 프레임에 대한 배포에 있어서는 MPEG2의 압축을 통해 배포되는 것이 일반적이므로 이에 대한 견고성이 두 번째로 다루어 지는 실험이다.

4.1 공모공격[7]

(1) 평균화공격

평균화 공격은 핑거프린팅된 다수의 컨텐츠를 서로 평균하여 새로운 컨텐츠를 생성하는 공격법이다. 본 실험에서는 user4와 user5의 공모를 실험한다. 그림6의 경우도 그림1의 컨텐츠 배포경로를 참조하여 분석한다. user4의 51 → 52 → 53 → 54경로와 user5의 65 → 66 → 69 → 70경로가 다른 값에 비하여 상관도가 크므로 user4와 user5가 공모했음을 알 수 있다.

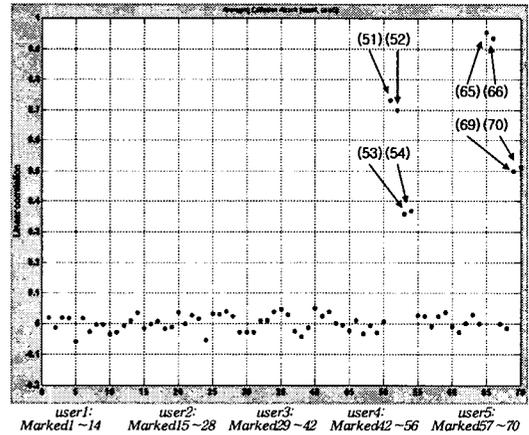


그림 6. 평균화 공격후의 상관도 계산

(2) 상관계수 음수화 공격

상관계수 음수화 공격은 상관계수를 이용하여 핑거프린팅 정보를 추출할 경우, 상관계수의 값을 음수로 만들어 공모자의 추적을 어렵게 만드는 공격법이다. 그림7의 경우 user4의 51 → 52 → 53 → 54경로와 user5의 65 → 66 → 69 → 70경로가 다른 값에 비하여 상관도가 크므로 user4와 user5가 공모했음을 알 수 있다.

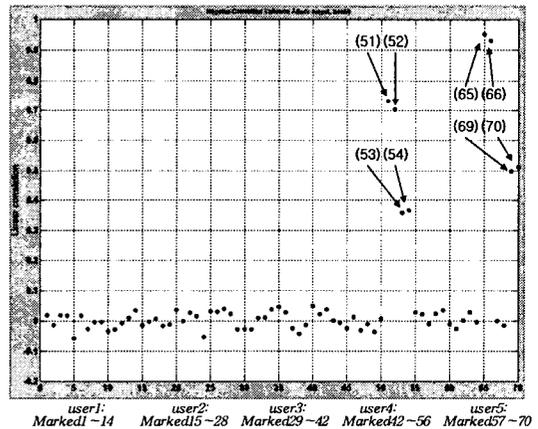


그림 7. 상관계수 음수화 공격후의 상관도 계산

(3) 상관계수 제로화 공격

상관계수 제로화 공격은 상관계수를 제로에 가깝게 유도하여 핑거프린팅 정보의 검출이 불가능하도록 만드는 공격법이다. 그림8의 경우 user4의 51 → 52 → 53 → 54경로와 user5의 65 → 66 → 69 → 70경로에서 (65) → (66)경로가 다른 값에 비하여 상관도가 크므로 user4와 user5가 공모했음을 알 수 있다.

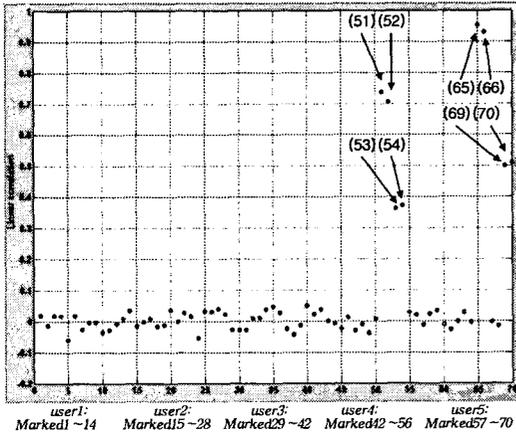


그림 8. 상관계수 제로화 공격후의 상관도 계산

4.2 MPEG2 압축에 대한 견고성

MPEG2 압축에 있어서는 영상화질을 2Mbits/s와 8Mbit/s의 두가지를 실험했다. 일반적으로 MPEG2에서는 4~10Mbits/s정도를 사용하고 있다. 그림9를 보면 2Mbits/s의 화질에서도 뚜렷하게 user1의 경로 1 → 2 → 3 → 4를 볼 수 있다. 편의상 논문에는 user1이 가지고 있는 비디오 영상에 대한 결과만 보이고 있지만 다른 유저 영상에도 마찬가지로 뚜렷하게 경로를 추적할 수 있다. MPEG2 압축의 견고성은 디지털 방송콘텐츠 보호기법의 적용에 있어서 필수적인 요건이라고 볼 수 있는데 본 결과는 적은 양의 데이터 처리이지만 실제 방송국에서의 활용에도 충분한 가능성이 있을 것으로 기대한다.

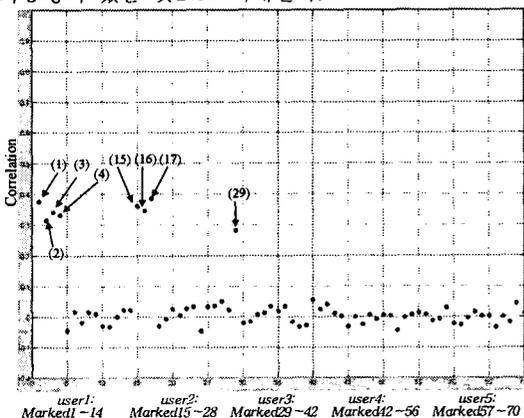


그림 9. MPEG2 압축후의 상관도 계산 (2Mbits/s)

5. 결론

디지털 콘텐츠에 대한 부정 배포자 추적에 대한 접근을 기존의 암호알고리즘이나 보안코드개발의 측면이 아닌 워터마킹 기술을 이용한 실제 구현의 측면에서 접근하였다. 특히, 비디오 프레임에 대한 삽입방법에 있어서 시간축 웨이블릿 변환을 활용하여 다양한 공격에 강인할 수 있었다. 추후, 암호 알고리즘 기술과의 접목을 통한 보다 향상된 시스템의 개발을 고려하여야 할 것이다.

[참고문헌]

- [1] 강현호, 박지환, 이해주, 홍진우, "시간축 웨이블릿 변환에 의한 비디오 워터마킹," 2002년도 정보보호 학회 영남지부 학술 발표대회 논문집, 2002.2
- [2] B. Pfitzmann, "Trials of Traced Traitors," Information Hiding, Lecture Notes in Computer Science, Vol. 1174, Springer-Verlag, pp.49-64, 1996.
- [3] B. Pfitzmann and M. Schunter, "Asymmetric Fingerprinting," in Advances in Cryptology, Proc. of EUROCRYPT'96, Vol. 1070, of Lecture Notes in Computer Science, Springer-Verlag, 1996.
- [4] D. Kirovski, H.S. Malvar and Y. Yacobi, "Multimedia Content Screening Using a Dual Watermarking and Fingerprinting System," ACM Multimedia, 2002.
- [5] J. Dittmann, A. Dehr, M. Stabenau, P. Schmitt, J. Schwenk and J. Ueberberg, "Combining digital Watermarks and collusion secure Fingerprints for digital Images," Security and Watermarking of Multimedia Contents, SPIE'99, Jan. 1999.
- [6] Y. Wang, J. Doherty and R.V. Dyck, "A Watermarking Algorithm for Fingerprinting Intelligence Images," 2001 Conference on Information Sciences and Systems, March. 2001.
- [7] V. Wahadaniah, Y.L. Guan and H.C. Chua, "A New Collusion Attack and Its Performance Evaluation," Digital Watermarking First International Workshop, IWDW 2002, Vol. 2613, of Lecture Notes in Computer Science, Springer-Verlag, Jan. 2003.