확률적 확산을 이용한 문서은닉 알고리즘

이근무(*)

(*) 위덕대학교 정보통신공학과 , kmrhee@uu.ac.kr

Steganography Algorithm Using Stochastic Duration Diffusion

Keun_Moo Rhee(*)

(*) Uiduk University, Department of Info & Comm

요 약

본 연구에서는 음악연주 정보를 기록하는 SMF (Standard MIDI File) 대한 정보 하이딩을 스테가노그래피의 관점에서 재고 해 보았다. 그 결과 그 중 SMF 데이터 스트림에 메시지를 은닉 하는 방법이 주로 이용되어 왔다. 연주 정보 통제 방법은 포함할 수 정보량의 증대가 어렵다는 문제가 있었다. 이 보고서는 기존 방식과는 다른 성분인 듀레이션의 확률적 확산을 이용해 정보를 은닉하는 SMF 스테가노그래피를 제안한다.

키워트 ; 문서은닉, 확률적확산

1. 서론

스테가노그래피는 개방적 통신 매체에 정보를 은닉하는 기술이다. 이는 통신의 내용을 비공개로 하는 암호 기술과 다른 관점에서 공개적으로 유용하게 정보의 비밀을 유지 해 주는 전략이다. 최근 디지털 콘텐츠의 대량으로 보급됨에 따라 스테가노그래피가 주목되고 있다. 스테가노그래피 연구의 주요 과제로 은닉된 정보를 분석 하여 은닉정보를 감지하고 이를 방지 하는 대책과 은닉 가능한 정보량의 증대하는 방법등 다양하게 연구되어 오고 있다.[1][2] 본 연구에서는 음악연주 정보를 기록하는 SMF (Standard MIDI File) 대한 정보 하이딩을 스테가노그래피의 관점에서 재고 해 보았다. 그 결과 그 중 SMF 데이터 스트림에 메시지를 은닉 하는 방법이 주로 이용되어 왔다. 연주 정보 통제 방법은 포함할 수 정보량의 증대가 어렵다는 문제가 있었다. 이 보고서는 기존 방식과는 다른 성분을 이용한 정보를 은닉하는 SMF 스테가노그래피를 제안한다. 본 연구 제안 방식은 MIDI 메시지 자체가 아니라 음의 duration 정보를 이용하여 정보를 은닉하는 방법을 제안 하였다. 따라서 연주 품질 저하가 적고, 기존의 기법보다 많은 정보를 은닉할 수 있으며 감지에도 강인할 것이라 예상할 수 있다.

2. 관련연구

SMF에 스테가노그래피로, 데이터 구조를 이용하는 방법[3][4], 연주 정보의 parameter를 제어하는 방법[5]이 연구 되어 왔다. 데이터 구조를 이용하는 방법은 SMF 데이터구조에 중복 제목, 연주 자체에 영향을 주지 않고 은닉정보를 포함하게 하고 있다. 이 방법은 데이터 구조에 은닉 흔적이 남아 있기 때문에 은닉검출이 쉽다. 그 대 방법은 은닉검출을 어렵게하는 방법이 연구[3]에 제안 되고 있다. 여기서는 SMF에 포함된 음의 강도를 나타내는 velocity의 매개 변수에 대해 정보를 포함 하는 방법을 이용하였다. 이 방법은 정보은닉에 의한 흔적을 데이터 구조에 남기지 않는 장점이 있다. 그러나 정보은닉에 의해 연주 자체가 변화 하게 된다. 그리고 연구[5]에서는 , 연주에 추가된 expression을 이용하여 기법을 적용하였다. 이 기법은 데이터 구조에 은닉 흔적을 남기지 않기 때문에 데이터 구조에 주목한 은닉 감지가 어렵다는 특징이 있다. 그러나 다른 방법에 비해 정보은닉 가능한 정보량이 매우 적어 전체 정보의 1-4 % 내로 제약된다는 단점이 있다. 본 연구는 과제를 해결하기 위해 SMF 의 Duration을 이용해 정보를 은닉하는 방법을 제안 한 연구를 참고 하였다.[6] 본 연구는 선행 연구들의 문제를 개선하기 위하여 duration을 이용하여 은닉정보 양을 늘리고 은닉 감지에도 강건 한 알고리즘

을 소개 하고자 한다.

3. MIDI의 구조와 SMF

MIDI는 전자 악기를 제어하기위한 표준규약이다. 악기의 제어에는 2 ~ 3byte의 제어 부호 (MIDI 메시지)를 사용한다. 이 연주 정보를 기록 하는 방식으로 SMF (Standard MIDI File)부호화 방식이 표준으로 이용되고 있다. 이는 MIDI 제어부호를 델타 타임[1] 과 함께 MIDI 이벤트로 기록하는 것이다.[7]

3.1 SMF 에서의 연주

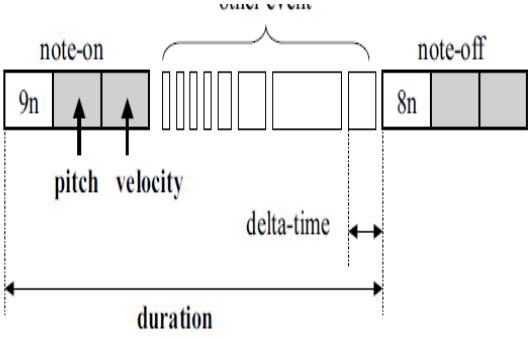

그림 1 SMF 연주 정보 parameter

MIDI에서 연주를 지시하는 부호는 3 바이트 note 메시지이다. note – on, note – off의 2 가지신호로,
음 생성시 note – on을 보내고 음 종료시 note – off를 보낸다. SMF는 MIDI 메시지의 시간차를 델타 타임 ($\delta time$) 으로 표현한다. 이는 note – on 게시 시간 note – off 시간의 차이를 취하는 것으로, 그 음의 duration 구할 수 있다 (그림 1 참조).
즉, SMF의 기본적인 발음 파라미터는 다음 4 가지이다.
(1) 음색
프로그램 체인지를 통해 차 채널 악기 (음색)을 할당한다.
(2) 소리의 높이 (pitch)
소리의 높이를 나타내는 매개 변수이며, note – on 이상시지에 포함된다. 7 비트의 지역을 가진다.
(3) 벨로시티 (velocity)
소리의 강도를 나타내는 매개 변수이며, note – on 이상시지에 포함된다. 7 비트의 지역을 가진다.
(4) duration (duration)
연주 시간이고 note – on, note – off 동안의 시간의 차이로 표시 된다.
본 연구에서는 이들 중 duration에 주목했다.

3.2 SMF 시간 관리

SMF는 시간 ($\delta time$)의 단위로 tick을 이용한다. 다음의 두 정데이터는 초 단위를시간을 tick 단위로 변환할 수있다.
(1) SMF headr chunk 정해져 있는 4 분 음표 의 빠르기(division)
(2) track chunk 에 있는 set tempo meta event 기록
예를 들어 set tempo meta event 기록에서 4분음표(기준이 되는 quarter note) 의 시간이 5000000(μsec) 이고 header chunk 의 division 이 480 [tick / beat] 인 경우, 1 tickekd 시간 t (m sec/tick) 는

$$t = \frac{500000}{480 \times 1000} = 1.04 \ [msec/tick]$$

로 계산 된다.
SMF는 이렇게하여 결정 tick – time으로 MIDI 이벤트의 델타 시간을 규정한다. 따라서 header chunk 에서 결정하는 4 분 음표에 해당하는 division을 바꿈으로서 $\delta time$ 은 길이가 변화된다. 즉 duration 은 바꾸어지는 것이다.

4. Duration을 이용한 정보은닉 알고리즘

기존의 SMF 스테가노그래피는 note on velocity 의 LSB를 은닉정보로 대체하는 아이디어를 발전시킨 것이다.[8] 특히 음색을 변화 시키지 않도록 하면서 은닉 용량을 보장하는 방법을 주목하였다.. 이 방법에 따르면, 연주 품질에 영향을 주지 않으면서 정보를 은닉할 수 있을 것을 예상한다. 그러나, velocity 구역이 7 비트로 좁아 은닉용량을 제한하고 있기 때문에 전체 은닉용량이 적다는 과제가 남아 있었다. 특히 MIDI 메세지의 파라미터가 7 비트이라는 제약은 크게, 다량의 정보은닉에는 설정 지역 이 외의 구역에 정보를 은닉할 필요가

1) MIDI 제어 부호를 발행하는 타이밍 정보. 이전 이벤트에서 시간 차이로 기록된다.

있다. 본 연구에서는 이러한 관점에서 먼저 duration diffusin 을 이용한 데이터 은닉 방법을 제안하였다.

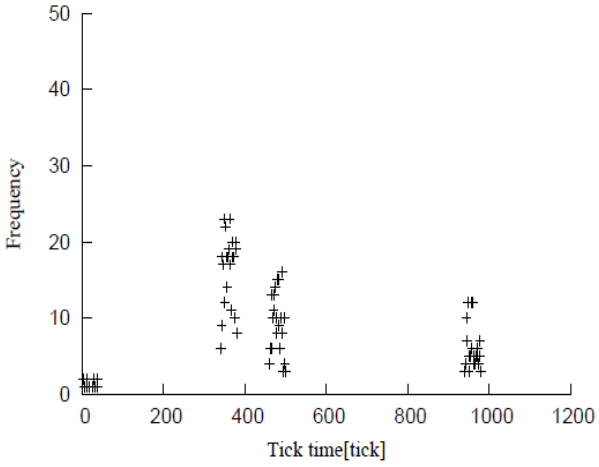

그림 2 duration diffusion

4.1 알고리즘의 전제

그림 2 는 실험 미디 파일 연주곡 중 (quater note division 960)의 duration 히스토그램을 나타낸 것이다. 가로축에 duration을 나타내고 세로축 각 값의 출현 빈도를 보였다. 이 그림에서 duration은 960,480,360 전후에 집중하고 있는지 알 수 있다. 이것은 δ *time* 의 division 이 960 임을 고려하면 duration은 각각 4 분 음표, 8 분 음표, 16 분 연속 부호 음가 주변에 차이가 편재되어 있기 때문이다.

여기서 실제로 연주되고 기록되는 듀레이션은, 악보의 음가에서 약간 흩어져 있는지 과 주목한다. 이 차이는 연주자나 제작자에 의해 추가된 억양이나 요동하다고 생각들이 된다.

제안 방식에서는이 듀레이션의 흔들림을 정보 포함 (표현)에 이용한다. 즉,

듀레이션을 "음가에 억양이나 요동이 추가된 것"이라고 파악해 SMF 헤더에서 얻을 수 음가의 변화를 신호로 포함된 정보를 표현하게 했다.

4.2 전처리

그림 3과 같이 인접한 음표의 음가 사이의 거리를 2 분할하여 cover SMF의 듀레이션을 구분한다. 그 때 소리 값을 기준으로 상하 각각 다른 표준편차를 구한다.

Step 1. SMF header chunk에서 4 분 음표마다 division T를 확인한다.

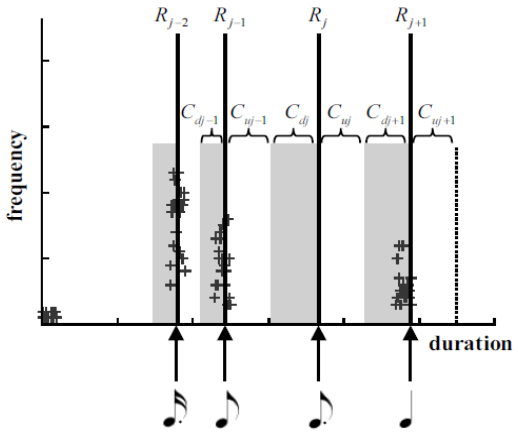

그림 3 duration 의 구분

Step 2. T를 기준으로 2 분 음표, 모든 음표, 8 분 음표, 16 분 음표, 32 분 음표, 64 분 음표의 음가 각각 얻는다. 마찬가지로 점 2 분 음표, 점 4 분 음표, 점 8 분 음표, 점 16 분 음표, 점 32 분 음표의 음가를 구한다.

Step 3 각 음가를 작은 순서로 배열하고 $R_i(0 \le i \le 11)$ 로 정한다.

Step 4. i 각각에 대해

$$D_i = \frac{R_{i-} R_{i-1}}{2}$$

$$U_i = \frac{R_{i+1} - R_I}{2} - 1$$

를 구한다.

Step 5 cover SMF duration에서 얻은 히스토그램에서 두 개의 치역 $[R_i - D_i, R_i], [R_i + 1, R_i + U_i]$ 으로 분할 한다. 여기서 치역$[R_i - D_i, R_i]$에 포함된 전체 샘플을 C_{di} 로 하고 그 이외를 C_{ui} 라 한다.

Step 6. C_{di} , C_{ui} 의 평균값은 같은 것으로 추정하고 각각의 표준 편차 σ_{di}, σ_{ui} 를 구한다.

Step 7 각 구간의 정보은닉 용량을 다음 식에 의해 구한다.

$$L_{di} = \log_2(\sigma_{di} \times M)$$
$$L_{ui} = \log_2(\sigma_{ui} \times M)$$

여기서 M은 매립 량을 외부에서 제어하는 매개 변수이다 (매입 강도). 그러나 은닉 정보 추출을 쉽게 하기 위하여. 샘플의 개수가 적은 구간에서는 다음 식에 의해 데이터 은닉용량을 결정한다.

$$L_{di} = \log_2(\frac{D_i}{3} \times M)$$
$$L_{ui} = \log_2(\frac{U_i}{3} \times M)$$

제안 방식은 데이터 은닉 용량을 음가의 상하 각각 duration 의 차이를 이용하기 때문에 연주의 질에 대한 영향을 줄 일 수 있을 것이다.

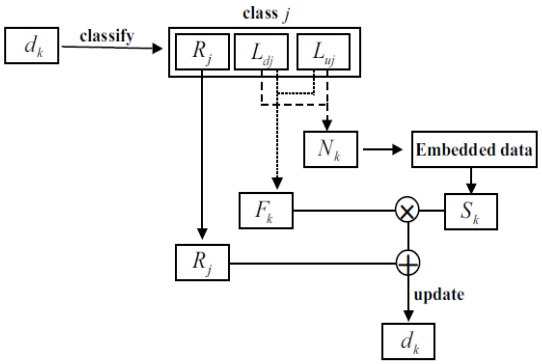

그림 4 처리 절차

4.3 정보은닉 처리 절차

k 번째 듀레이션 정보 d_k 에 데이터를 은닉하기 위한 절차는 다음과 같다.

Step 1 cover SMF의 에 포함된 듀레이션 d_k을 얻는다.

Step 2. d_k 를 C_{uj} 또는 C_{dj} 로 분할 한다.(두 집단 중 하나에 소속되도록 하는 j를 결정한다). 데이터 은닉 제어 함수 F_k 를 다음 식에 의해 결정한다.

$$F_k = \begin{cases} 1 & (d_k \text{ 가 } C_{uj} \text{ 에 속한 경우} \\ -1 & (d_k \text{ 가 } C_{dj} \text{ 에 속한 경우} \end{cases}$$

Step 3. 전처리에서 얻은 L_{dj} 또는 L_{uj} 에 의해 데이터 은닉 용량 N_k 를 결정하고 그 용량의 크기 정보 S_k를 구한다.

Step 4 다음 식에 의해 d_k 를 업데이트한다.

$$d_k = R_i + F_k \times S_k$$

4.4 은닉정보 추출절차

먼저 은닉 절차와 같이 마찬가지로 cover SMF의 각 duration d_k f를 C_{di} , C_{ui} 로 분할 하여 각각의 표준 편차를 구한다. 은닉 용량 L_{dj} 또는 L_{uj} 는 다음 식에 의해 구한다.

$$L_{di} = p(3 \times 2^{p-3} \le \sigma_{di} < 3 \times 2^{p-2})$$
$$L_{ui} = q(3 \times 2^{q-3} \le \sigma_{ui} < 3 \times 2^{q-2})$$

이후 k 번째 duration 정보 d_k에서의 정보 추출처리 절차는 다음과 같다.

Step 1. duration d_k 를 구한다.Step 2. d_k 를 C_{uj} 또는 C_{dj} 로 분할 할 수 있는 j 를 결정한다.

Step 3.L_{dj} 또는 L_{uj} 에 의해 은닉된 용량 I_k 를 구한다..

Step 4. $X_k = |d_k - R_j|$ 식에 의해, I_k bit 의 값을 X_k 에서 읽는다.

5. 결론

제안된 알고리즘은 추후 MIDI 의 각 채널을 이용하여 구현되고 그 성능과 감지능력 , 음질에 대한 영향 등이 평가되어야 할 것이다.

참고문헌

[1] Shawn D. Dickman, An Overview of Steganography, James Madison University Info sec Techreport Department of Computer, Science ,JMU-INFOSEC-TR-2007-002, July 2007.

[2]Kefa Rabah, Steganography-The Art of Hiding Data, Information Technology Journal 3 (3): 245-269, 2004.

[3]Inoue, Daisuke et al, Scheme of standard MIDI files steganography and its evaluation,Proc. SPIE Vol. 4675, pp. 194-205.

[4] Daisuke Inoue et al, ,Detection-Resistant Steganography
for Standard MIDI Files, *IEICE Trans. Fundamentals, Vol.E86-A, No.8, pp.2099-2106, 2003.*

[5] 山本紘太郎, 岩切宗利, 表情付けを考慮した SMF ステガノグラフィ, 情報処理学会論文誌, Vol.47, No.8, pp.2724-2732, 2006.

[6]Kotaro Yamamoto et al, A SMF Steganography Based on Fluctuation of Duration,

[7]정보통신부, eMusic Converting Solution 기술, 2002.

[8]www.chennaisunday.com/.../Steganography-Steganography for Data Hiding Messages in MIDI Songs