디지털 비디오 광 디스크의 복제방지를 위한 후처리 암호화 기록 장치의 설계

김형우* · 주재훈** · 김진애** · 최중경**

Design of After-processing Encrypted Record System
for Copy Protection of Digital Video Optical Discs

Hyeong-woo Kim* · Jae-hoon Joo** · Jin-ae Kim** · Jung-keyng Choi**

이 연구에 참여한 연구자(의 일부)는 『2단계 BK21사업』의 지원비를 받았음.

요 약

본 논문은 디지털 비디오 타이틀 제작 업체가 디스크 제작을 완료한 후 디스크 복제방지를 위한 목적으로 디스크의 일부영역에 타이틀 업체의 고유ID를 기록하는 후처리 암호화 기록장치에 대한 시스템을 제시한다. 그 방법으로서는 FPGA를 이용하여 광디스크의 메모리블록 동기화 신호인 SYNC를 검출하고, 기록(Write)을 위한 다중펄스(Multi Pulse)를 발생시키는 기록 패턴을 설계한다. 그리고 사용자가 광 디스크의 데이터영역을 어느 곳이라도 자유자재로 기록이 가능하도록 FPGA로서 기록하는 방법을 제시하고 설계한다. 이러한 디지털 비디오 광 디스크의 비기록 데이터영역을 사용자 임의대로 기록하는 시스템을 개발함으로써 소프트웨어 복제 방지에 효과적으로 대응이 가능하며, 향후 고밀도 광 디스크의 암호화 기록에도 응용이 가능하다.

ABSTRACT

This paper presents encrypted secret code recording system which can insert an unique manufacture ID code after complete disc process. First, we detect a memory block synchronizing signal which is SYNC. by using FPGA, then, design a recording pattern to write Multi Pulse. Finally, a method that any data is recorded in any place in any data area of optical disc by using a FPGA was proposed. Newly proposed method in this paper that any user records user data in protected data areas on digital video optical discs, can be very useful for effective software copy protection, and can be applicable to encrypted record on high density DVD in near future.

키워드

광 디스크 후처리 암호화, FPGA, 다중펄스, 복제방지

Key word

Encrypted record, FPGA, multi pulse, copy protection

* (주)대호아이엔티 기업부설연구소(nmi@korea.com)

** 창원대학교 전자공학과

접수일자 : 2010. 04. 15

심사완료일자 : 2010. 06. 07

I. 서 론

최근 고화질 HD급 영상을 녹화하여 가정에서 볼 수 있도록 하는 가장 잘 알려진 저장매체로 DVD를 꼽을 수 있다. 이처럼 DVD는 영화관에서 보는 것과 같은 박진감을 가정에서 즐길 수 있도록 고화질, 고음질을 실현함과 동시에 자녀에게 폭력 장면을 보여 주지 않는 락기능이나 갖가지 복제방지 기능 등을 실장 하여 지금은 마야호로 새로운 세기의 AV용 디스크로서 보급이 진행되고 있다. 그리고 기록형 DVD를 읽어 대량으로 복사가 가능한 시대에 이르러 각 타이틀 메이커 회사에서는 완성된 DVD에 자기회사의 고유코드를 DVD의 일부영역에 기록함으로써, 소비자가 DVD 타이틀을 구매한 후 초기 인식 과정에서 메이커 회사에서 제공한 고유코드와 일치하지 않으면 재생이 불가능하게 하도록 하는 연구를 계속적으로 하고 있는 추세이다.

이에 타이틀이 만들어진 이후에 고유의 코드를 DVD의 일정영역에 써넣는 기술의 요구가 급격히 늘어남에 있어, 본 논문은 FPGA(Altera EP1S25F780C6)로서 기록패턴을 구현하여 특정영역에 메이커의 코드를 저장할 수 있는 후처리 암호화 시스템을 구성하여 DVD 타이틀 메이커의 요구에 충실한 시스템을 제작하였고, 기존의 DVD 기록제어기로 개발된 양산칩의 제한된 기능들을 VerilogHDL언어를 이용하여 FPGA로 구현함으로써 DVD 주소와 데이터 크기를 제공하면 DVD의 어느 영역에도 자유자재로 기록가능하게 하였다.

II. 본 론

DVD 기록 메카니즘 구성에는 DVD 트랙 추종을 관할하는 DSP, 메카니즘을 통괄하는 마이컴, 데이터 획득을 위한 레이저 신호(Pick-up) 제어를 위한 ASP, 기록 펄스를 발생시키는 FPGA, 그리고 최종 DVD 기록 장치로서의 Pick-up 모듈로 구성된다.

그림 1. 전체시스템의 구성
Fig. 1 SYSTEM Block diagram

마이컴은 v850칩을 사용하는데 기록 지정 위치가 안정화된 시점에서 FPGA로 기록 펄스를 발생하도록 명령을 내려주는 역할을 한다. DSP는 SDRAM에서 기록할 데이터를 불러 하드웨어 기록 형식신호인(EFM+)신호로 출력시켜 FPGA 타이머 클럭(PLCK)신호와 함께 FPGA로 공급하게 된다. FPGA에서는 쓰고자하는 DVD의 주소와 사이즈를 받아 주소를 검출하고 기록형식신호(EFM+)를 멀티펄스로 변환시켜 Pick-up 모듈에 기록신호를 보내어 DVD의 원하는 영역에 데이터를 기록하는 기능을 한다.

III. FPGA 내부구성 및 역할

본 연구에 사용된 FPGA는 EP1S25F780로서 논리요소가 25,660개이며 I/O 핀 수가 597개, 메모리가 1.9Mbit 정도이며 6개의 PLL회로로 구성되며, 450MHz까지 출력이 가능하다. FPGA의 내부구성은 크게 마이컴과의 인터페이스부, 기록 펄스 검출부, 기록 펄스 해석부, 기록 펄스 발생부로 구성된다.

그림 2. FPGA의 내부 구성
Fig. 2 FPGA Block diagram

3.1 기록 펄스 검출부

DSP로부터 PLCK와 EFM+신호를 공급받고 DVD의 어드레스를 찾는 부분이 기록 펄스 검출부라 할 수 있다. DVD의 데이터 구조상 32KB의 용량을 하나의 기본 메모리 단위로 ECC라는 블록이 구성되어져 있는데 이러한 ECC는 다시 메모리 블록 동기화 신호 영역인 SYNC. 영역과 데이터영역으로 구분되어져 있다. 코드 데이터를 원하는 영역에 쓰고자 한다면 먼저 DVD의 SYNC.부분을 찾아야 하기 때문에 SYNC.영역 검출이 필요하다. SYNC.영역 검출을 FPGA로 구현하기 위해 먼저 PLCK에 맞추어 최소 데이터 필드 영역을 1T(1/26.15625MHz, 38.23178ns)로 지정한다. SYNC.는 32bit로 구성되어 있으므로 1bit당 1T로 할당하여 FPGA로 읽어 낸다.

SYNC.의 하위22bit(22'b00010000000000000010001)는 동일하므로 이 부분을 먼저 검출한 뒤 나머지는 각 SYNC.할당별로 FPGA에서 찾아내게 한다. 후처리 암호를 기록하는 부분은 DATA 프레임 구조상 PI(Pull-In)와 PO(Pull-Out)영역에 해당하는 부분이므로 SYNCn을 검출한 뒤 PI를 찾기 위해 카운트를 하여 각 PI의 시작부분을 찾아 기록 위치로 지정하게 한다.

그림 3. SYNC. 검출 방식
Fig. 3 SYNC. DETECTION METHODE

3.2 기록 펄스 해석부

고밀도 광 기록 장치에서는 채널에서 발생하는 오류를 줄이기 위해 변조 코드를 사용하는데, 코드 중 '1'과 '1'사이의 '0'의 개수를 최소 d개, 최대k개로 제한하는 런-길이 제한(run-length limited, RLL)코드를 사용한다. 이러한 변조 코드 방법은 천이 간격을 제한함으로써 인접 심벌간의 간섭을 감소시키고 기록 밀도의 향상을 가져올 수 있다. CD계열의 확장이라 볼 수 있는 DVD는 일반적인 CD에 비해 7배 이상 많은 저장 용량을 지닌 광기록 매체이고 이러한 고밀도 광기록 장치에서는 EFM+ 코드를 사용한다.[1] 본 논문에서는 DSP로부터 받은 EFM+신호를 FPGA에서 쉬프트레지스터로 저장하고 첫 상승에지신호이후 다음 상승에지가 발생하는 한 주기 동안 연속되는 '0'의 개수만큼을 공간(Space)으로 설정하고, '1'의 개수 만큼 기록(Mark)이 되도록 설계한다. Mark의 수만큼 기록되고 Space수만큼 기록하지 않는 Multi Pulse를 만들 수 있는 기반데이터가 형성되도록 설계한다. 이런 알고리즘을 FPGA로 구현 하고자 하는 시도가 이 논문의 특징 중 하나라고도 할 수 있다.

그림 4. FPGA 시뮬레이션 결과
Fig. 4 FPGA Simulation Result

그림 4의 시뮬레이션 결과에서 기록데이터가 Mark와 Space로 치환함을 시뮬레이션으로서 확인하였다.

SDRAM의 0번째 주소의 데이터가 3C383C1Ch일 경우 이를 2진화 하였을 경우 시뮬레이션 화면 아래 그림 처럼 0 과 1의 기록패턴을 쉽게 확인 할 수 있는데, ‘1’인 부분의 갯수와 ‘0’인 부분의 개수를 기록부분(MARK)와 공간(SPACE)부분으로 나누어 획득함을 FPGA 시뮬레이션 환경에서 확인되었다. 이는 멀티 펄스를 만드는데 중요한 역할을 하며 기존의 범용화된 칩의 처리능력에 비해 매우 빠른 FPGA에서 변환되므로 보다 빠른 기록을 할 수 있는 장점이 있다.

3.3 멀티 펄스 발생부

Mark와 Space로 변환하였으므로 이를 이용하여 멀티 펄스를 발생시켜 최종 Pick-up에 전송해주어야 한다. 멀티펄스를 발생시키는 방법은 이미 발표된 바있는 nT에 균일한 1T값을 n의 개수만큼 기록하는 방식 혹은 nT를 기준으로 펄스하나와 다중펄스 n-2개를 발생시키는 방법이 있었다[2]. 본 연구에서는 보다 정확하고 개선된 방식으로 멀티펄스 설계를 제안하게 되었다. 제안된 멀티펄스 방식은 모든 시작 펄스(그림5의 A)에는 3T만큼의 시간을 주며 중간 펄스(그림5의 C)기간은 1T의 시간을 주고, 마지막 펄스(그림5의 D)는 각T마다 시험상 가장 좋은 값을 선택하여 멀티 펄스를 개선하게 되었다.

그림 5. 멀티 펄스(3T~11T)
Fig. 5 Multi Pulse(3T~11T)

따라서 멀티 펄스는 그림5와 같이 시작(A), 중간(C), 마지막 펄스(D)로 이루어지며, 3T는 시작펄스로만 이루어졌으며, 4T는 시작펄스와 마지막 펄스로, 5T부터 11T까지는 시작과 마지막 펄스 사이에 중간 펄스가 존재하

도록 제안하였다. 특히 시험상에 보다 정확한 기록을 위하여 각T를 16등분하여 기록의 정확도를 높였으며, 이러한 과정이 FPGA로 처리되어 빠르고 정확하게 처리가 될수 있다는 것이 이 논문의 장점이라고 할 수 있다.

그림 6은 멀티 펄스를 설계한 후 오실로 스코프로 획득한 파형이다. 오실로 스코프의 채널2는 기록 개시 펄스이고 채널4는 멀티 펄스로 7T, 3T, 7T, 3T, 11T, 3T, 11T, 3T를 출력한 파형이다.

그림 6. 멀티 펄스 출력 파형
Fig. 6 Multi Pulse Output Wave

IV. 암호화를 위한 PI영역 기록 파라미터화

4.1 기본 메모리 블록(ECC)내부구조와 비기록 데이터 영역(PI-area)

DVD의 1섹터는 그림 7과 같은 구조로 1ECC당 16개의 프레임을 가지며 1 프레임당 13개의 열을 가지므로 총 208개의 열을 가진다[3].

그림 7의 흑색부분이 16개 프레임의 각 마지막 영역(224bit+10bit)으로 후처리 기록 가능한 PI영역이다. 그림7의 백색부분인 데이터 영역은 실제 메이커회사들이 영상이나 음원 데이터를 기록하는 부분이며 PI영역은 메이커가 기록하지 않는 부분이다. 메이커회사에서 타이틀을 제작한 뒤 메이커회사와 약속된 고유의 코드를 이 부분에 기록하는 방식을 제안하는 것이 본 논문의

참고문헌

- [1] 金亨錫, “EFMPlus 코드 디코더 설계,” 동국대학교 석사학위논문, 2005.
- [2] 이효찬, “DVD-RAM 미디어 기록방법 최적화에 관한 연구,” 성균관대학교 석사학위논문, 2003.
- [3] DVD Forum “DVD Specifications for Re-writable Disc(DVD-RAM) Part1 PHYSICAL SPECIFICATIONS Version 2.0” PH1-1~PH2-50, PHX-F1~PHX-F3 (1999).

최중경(Jung-Keyng Choi)

- 1986. 2. 고려대학교 전기공학과 공학사
- 1988. 2. 고려대학교 전기공학과 공학석사

1992. 8. 고려대학교 전기공학과 공학박사
1992년 ~ 현재 창원대학교 전자공학과 교수
※관심분야: 서보기기제어, 자동동조제어, 마이크로 프로세서응용, DSP응용, 영상제어.

저자소개

김형우(Hyeong-Woo Kim)

- 1995년 인제대학교 전자공학과 공학사
- 1997년 창원대학교 전자공학과 공학석사

2008년 창원대학교 전자공학과 박사과정수료
2009년~현재 (주)대호아이엔티 연구소 과장
※관심분야: FPGA, 마이크로프로세서응용

주재훈(Jae-hun Joo)

- 2004. 2. 창원대학교 전자공학과 공학사
- 2008. 2. 창원대학교 전자공학과 공학석사

2010. 2. 창원대학교 전자공학과 박사과정수료
현재 창원대학교 전자공학과 박사과정
※관심분야: 서보기기제어, DSP응용

김진애(Jin-Ae Kim)

- 2001. 8. 창원대학교 전자공학과 공학사
- 2004. 2. 창원대학교 전자공학과 공학석사

2007. 2. 창원대학교 전자공학과 박사과정수료
2005년 ~ 현재 창원대학교 전자공학과 박사과정
※관심분야: 마이크로프로세서 응용, DSP 응용