[5A-92]

카오스 시스템을 이용한 실시간 영상 암호화기의 FPGA 구현

김수민, 최현준, 서영호, 김동욱
광운대학교 전자재료공학과 디지털 설계 및 테스트 연구실
sumin@kw.ac.kr http://ddntlab.kw.ac.kr

FPGA Implementation of Chaotic System for Real-Time Video Encryption

Su-Min Kim, Hyun-Jun Choi, Yong-Ho Seo, and Dong-Wook Kim
Department of Electronic Materials Eng., Kwangwoon University

본 논문에서는 JPEG2000 표준에서 주파수 변환기법으로 채택된 이산 웨이블릿 변환과 선형양자화 방법을 사용하여 영상 전체가 아닌 영상의 부분 데이터만을 암호화하고, 암호화를 위한 계산양을 줄이는 방법을 제안하였다. 또한 계산양이 많은 암호화 알고리즘 대신 비교적 계산양이 적은 카오스 시스템을 적용함으로써 계산양을 더욱 감소시켰다. 이 방법은 영상의 압축비를 유지하기 위해서 양자화와 엔트로피 코딩 사이에서 암호화를 수행하며, 부대역의 선택과 카오스 시스템을 이용한 무작위 변환방법을 사용한다. 영상에 대한 실험방법은 우선 암호화할 부대역을 선택한 후 영상데이터를 일정한 블록으로 만든 후 랜덤하게 좌/우로 시프트 하는 방식을 사용하여 암호화 하였다. 구현된 하드웨어는 APEX20KC EP20K1000CB625-7의 FPGA 디바이스에서 1306(4%)개의 LAB(Logic Array Block)에 해당되는 자원을 사용하면서 사상되었고 64MHz의 동작 주파수에서 안정적으로 동작하였다. 또한, 2D DWT(Discrete Wavelet Transform)를 이용한 영상압축기에 적용해서 암호화 동작을 가능하도록 설계하였다

Ⅰ. 서 론

멀티미디어 시대를 맞이하여 영상과 비디오 컨텐츠에 대한 선호도가 급속히 증가하고 있다[1]. 데이터의 안전한 전송을 위해 여러 암호화 알고리즘이 개발 되었으며 몇몇 알고리즘들은 국내 및 국제 표준으로 선정되어 여러 분야에서 사용되고 있다[2]. 특히, 영상/비디오 같은 매체는 데이터양이 매우 많아서 영상/비디오 전체를 암호화 하는데 많은 비용과 시간이 소요됨으로 암호화 하는 양을 줄이는 연구가 이루어지고 있다. 영상/비디오의 데이터양을 줄이는 연구는 지금까지 두 주류를 형성하고 있다. 현재 가장 널리 사용되고 있는 분야는 JPEG 및 MPEG 분야로, 지금까지 상당부분이 국제표준으로 채택되었으며[3], 현재 대부분의 응용분야에 사용되고 있다. 이 기술의 기본적으로 DCT(Discrete Cosine Transform)을 사용하고 있는데, 이 방식은 8×8 화소블록으로 하고 있기 때문에 고 압축시 블록효과(Block effect)라는 문제점을 가지고 있다. 최근 이산 웨이블릿 변환(DWT, Discrete Wavelet Transform)을 영상 변환에 사용하는 방식이 연구되고 있는데, 이 방식은 영상 전체를 변환 단위로 사용하기 때문에 DCT 변환에서 가지는 블록효과가 없고 같은 압축률에서도 좋은 화질을 보인다[4]. 최근에는 JPEG2000에서 영상 표준 방식으로 채택되었다[5].

본 논문에서는 [6]에서의 웨이블릿 영상압축기를 기반으로 영상 암호화기를 구현하였다. 특히, 계산양이 많은 암호화 알고리즘을 사용하지 않고 비교적 계산양이 적은 Chaotic System을 사용하여 하드웨어로 구현 하였다. 본 논문에서 제안하는 암호화 방식으로는 Chaotic system을 기반으로 랜덤비트(random bit)를 생성하여 일정한 블록을 기준으로 좌/우로 쉬프트해서 암호화를 수행한다.

Ⅱ. Chaotic System과 암호화 알고리즘

2-1. 카오스시스템

카오스 시스템이 가지는 특징으로 두 가지를 들 수 있는데 위상공간상에 유한한 영역내에서 주기성이 없이 그려지는 이상한 끌개(strange attractor)와 초기 조건의 민감성을 들 수 있다. 이상한 끌개는 이상한 끌개 위의 두 개의 초기점이 아무리 가깝다 하더라도 이들로부터 진화하는 궤도는 곧 기하급수적으로 멀어지며 판이하게 다른 진화 양상을 보여준다는 의미이다. 이러한 성질을 만족하기 위해서는 이상한 끌개의 기하학적 구조가 프랙털(Fractal) 구조를 가져야 한다. 프랙털 구조의 차원은 정수가 아니라는 특성 때문에 이상한 끌개라고 불린다. 초기