키 추출 공격을 회피하는 이미지를 이용한 동적 키 생성 매커니즘

정명우*, 오윤석*, 서승현*, 강유성**, 최두호**
*고려대학교 세종캠퍼스 수학과
**한국전자통신연구원 정보보호연구본부 암호기술연구실
e-mail: jung4651@korea.ac.kr, ashbringer@korea.ac.kr, crypto77@korea.ac.kr
youskang@etri.re.kr, dhchoi@etri.re.kr

A Study on Dynamic Key Generating Mechanisms Using Images to Avoid Key Extraction Attack

Myeong-Woo Cheong*, Yoon-Seok Oh*, Seung-Hyun Seo*
You-Sung Kang**, Doo-Ho Choi**
* Dep. of Mathematics, Korea University, Sejong Campus
** Lab. of Cryptography Research, Information Security Research Division, ETRI

요 약

현대 사회는 IoT의 대중화와 함께 늘어나는 보안 위협에 노출되어 있다. 특히 CCTV의 설치 구역 확대는 그 보안 취약성과 맞물려 사생활 침해 등 문제를 야기할 가능성이 높다. 기존의 보안 솔루션은 키를 기기에 저장해야 하는 점 때문에 키 추출 공격 등으로 쉽게 보호능력을 상실할 수 있다. 본 논문은 키를 저장하는 것이 아닌 이미지를 씨드(Seed)로 사용하여 동적으로 키를 생성하는 개념과 매커니즘을 제안한다.

1. 서론 및 개요

현대는 본격적인 사물인터넷(IoT, Internet of Things) 시대를 맞아 각종 디바이스에 네트워크를 연결해 생활의 편리를 추구하는 노력이 활발하게 시도되고 있다. 이에 비례하여 보안 위험 및 취약성으로 인한 피해 사례 역시 증가 추세이다. 적절한 보안 솔루션을 갖추지 못한 제품의 유통은 소비자, 기업, 정부 모두에게 위협이 된다. 따라서 각각의 디바이스 환경에 적합하면서도 최대의 보안 강도를 가지는 보안 메커니즘이 요구된다.

CCTV는 오랫동안 특정 구역을 감시하는 용도로 애용된 모니터링 디바이스이다. 최근에는 인터넷 망에 연결되어 네트워크 카메라라는 명칭을 쓰기도 하며, 주로 범죄에 따른 사회적 이슈로 CCTV가 설치되는 구역이 확대되고 있다. CCTV를 사용함으로써 보호하고자 하는 구역의 물리적 보안이 달성된다고 일반적으로 생각되지만 CCTV 자체는 보안이 취약하다는 것이 알려져 있다[1]. 도청 및 해킹을 통해 사생활 침해는 물론이요, 중요 증거로 활용될 수 있는 영상정보를 조작하거나 파기할 수 있는 위험성이 크다. 기존 기법을 활용한 보안 솔루션은 키를 어떤 식으로든 저장해야 하기 때문에 물리적인 접근을 전제로 하는 키 추출 공격에는 취약하다. 또한 키를 하드웨어에 내장할 경우 유통과정에서 키가 변조될 수 있는 가능성을 고려해야 한다.

본 논문은 키를 디바이스 내부에 저장하는 것이 아닌, 디지털 이미지를 씨드(Seed)로 사용하여 동적으로 생성하는 개념과 방법을 제안한다. 적용되는 주요 대상은 CCTV 등 정지된 이미지를 생성 가능한 모니터링 카메라가 된다. 2장에서 관련연구를 언급하고, 3장에서 임시로 Raspberry Pi Camera를 CCTV 환경으로 조성하고, 씨드로 사용될 이미지를 촬영하고 처리하는 기법을 소개한다. 4장에서는 실험 결과 및 결론을 도출한다.

2. 관련연구

[1]에서는 CCTV 보안관제에 있어서 생기는 보안 위협과 취약성들을 분석했다. 공인IP를 사용할 때의 문제, 아날로그 CCTV 카메라 사용 시의 문제, 악의적인 공격자에 의한 보안 위협 등을 분석하였으며, 이러한 공격으로 보안관제망의 전체 성능이 저하될 수 있음을 보였다. CCTV가 영상 정보를 주고받는 과정의 보안체계가 허술해 많은 공격에 노출되어 있는데, AES 암호를 이용하여 디지털 영상을 암호화하는 기법[2] 등 안전성을 확보하려는 시도가 계속되고 있다. 그러나 서론에서 언급했던 것과 같이 기존의 기법들은 키를 디바이스에 하드웨어 혹은 소프트웨어 기반으로 저장해야 한다. 키가 저장

되어 있다면 그 키를 물리적으로 찾는 것은 적극적인 공격자에게 높은 복잡도를 요구하지 않는다.

따라서 본 논문에서는 키 추출 공격을 회피하기 위해 키를 물리적으로 저장하지 않고 이미지로 씨드를 추출해 동적으로 키를 생성하는 방법을 제안한다. 이를 위해서 오차 보정을 위한 BCH 코드와 Fuzzy Extractor 개념을 활용하였다. Fuzzy Extractor는 생체 인식 분야에서 활발히 연구되던 매커니즘으로[4], 매 추출마다 값이 완전히 같을 수 없는 생체 데이터를 보정해 인증하는 기법이다. 오차를 보정하는 방법은 [3]에서 설명하는 BCH 코드를 사용하였다. 본 논문에서는 이에 착안하여 디바이스에서 추출한 이미지를 생체 데이터처럼 사용해 씨드 추출기법(씨드 Extractor)을 구현한다. 이에 더해 디바이스의 일련 번호(Serial Number)를 사용해 씨드 추출의 정확도를 높일 수 있는 구상을 하였다.

3. 암호키용 씨드 추출기법

씨드 값을 동적으로 생성하여 키 추출 공격을 회피하기 위해서는 디바이스에서 동적으로 씨드를 추출할 수 있는 데이터를 수집하여야 한다. 해당 연구에서는 이러한 데이터를 수집하기 위해 CCTV환경에 대해서 고정된 이미지 수집을 통한 씨드 값 추출에 대하여 연구하였다. 고정된 이미지에서 일정한 씨드 값을 추출하는 알고리즘의 경우 다음과 같다.

3-1. 이미지 추출 및 처리 단계

사물인터넷과 같은 환경에서 이미지를 이용한 씨드 값 추출 프로그램을 만들기 위해 이와 비슷한 환경을 구축할 수 있는 Raspberry Pi와 이미지 데이터 수집을 위해 Pi camera를 사용한다. 이를 위한 실험환경은 다음과 같다.

(표 1) 실험환경

	Version	Name
Device	Model B	Raspberry Pi 2
Module	Version 1.3	Pi Camera
OS	4.4	RASPBIAN JESSIE

해당 환경에서 Pi Camera를 통해 수집한 이미지 데이터의 크기는 50 X 50의 이미지를 수집한다. 이미지 데이터 수집은 100개의 데이터를 3초당 1장씩 수집하는 프로그램을 통해 수집하며 해당 데이터를 Binary 이미지로 변환하는 과정을 추가한다. 이는 RGB 이미지의 경우 0~255 값을 가지는 3개의 열로 구성되어있어 경량 디바이스에서 계산하기 힘들며 같은 이미지간의 오차 또한 크기 때문에 0~255의 값을 가지는 Grayscale 이미지로 변환한다. 이후 빛에 의한 오차를 조금 더 줄이고자 해당 이미지를 Binary 이미지로 변환하여 데이터간의 오차를 최소화 한다. 실제 이미지 변환과정은 다음 (그림 1)과 같다.

(그림 1) 이미지 처리 과정

이미지 처리이후, 데이터들 중에서 다른 데이터들과의 비교를 위한 원본 데이터(original data)를 결정해야한다. 원본 데이터를 선정하기 위한 기준으로 유클리드 거리를 계산하여 이미지간의 유사도가 가장 높은 데이터를 원본 데이터로 선정한다. 이렇게 원본 데이터를 설정하는 이유는 새로운 데이터와의 오차를 줄임으로써 오차 보정률을 증가시킬 수 있기 때문이다.

3-2. BCH 코드를 활용한 오차 보정 단계

생체 인증 정보와 비슷하게 해당 알고리즘에서 사용하는 이미지 정보는 데이터간의 오차가 존재한다.[3] 이러한 오차가 발생하면 같은 이미지 데이터에 대해서 다른 씨드 값이 나오기 때문에 이미지 데이터를 씨드값으로 사용하기 위해서 오차를 제거하는 메커니즘이 필요하다. 이를 구현하기 위해서 BCH 코드를 사용하였다.[4] 먼저 원본 데이터를 입력 값으로 사용하여 해당 데이터에 대한 패리티 비트 값을 인코딩한다. 이때 BCH 인코딩을 위한 매개변수로 블록의 크기(N), 메시지 길이(K), error-correction capability(t)가 필요하다. 해당 매개변수의 경우 보정되어야할 오차의 개수, 블록당 메시지의 길이 등 여러 조건을 만족하는 적절한 (N,K,t)를 선택한다. 이와 같이 BCH 인코딩을 통해 나오는 결과값인 패리티 비트를 프로그램 내부에 저장을 한다. 저장된 패리티 비트는 원본 데이터와 오차가 존재하는 이미지에 적절히 패딩(Padding)되어 BCH 디코딩을 통해 원본 데이터를 얻어 낼 수 있다.

3-3 고정값 추가를 활용한 오차 보정률 개선 단계

BCH 코드의 매개변수를 결정할 때 K/N의 비율이 높을수록 효율적인 계산을 수행한다 할 수 있다. 고

정된 K/N에서 BCH 코드의 오차 보정 능력을 증가시키기 위해서 일련 번호를 사용한다. 실험에서 사용된 일련 번호 목록의 경우 다음 (표 2)와 같다.

(표 2) 일련 번호 목록

Serial List	Serial Number Length
Mac Address	119bit
SD card Serial Number	231bit
CPU Serial Number	182bit
Total Length = 532bit	

즉, 이미지 데이터 $Data(x)$에 일련 번호 $Serial(x)$를 추가한 새로운 데이터 $f(x) = Data(x) + Serial(x)$ 를 계산한다. 새로운 데이터 $f(x)$를 입력 데이터로 위의 방법과 같이 알고리즘을 수행하였을 경우 오차 보정 능력이 상승된다.

3-4. 무작위화(Randomization) 단계

BCH 코드를 통해 얻어낸 결과값을 SHA-1을 사용하여 무작위화를 진행한다. 이미지 데이터의 경우 엔트로피가 주변 환경에 영향을 많이 받아 임의성(Randomness)을 항상 가지고 있다 할 수 없다 . 이러한 문제를 해결하고자 SHA-1 알고리즘을 사용하여 씨드 값에 임의성을 추가할 수 있다.

4. 실험결과 및 결론

해당 알고리즘을 일정한 간격으로 모은 300개의 데이터를 사용하여 실험을 하였으며 실험의 결과를 측정하기 위해서 FRR(False Rejection Rate), FAR(False Acceptance Rate)을 측정하였다.

(표 3)의 결과를 보면 BCH 코드의 매개변수에 따라 FAR, FRR 값이 달라지는 것을 알 수 있으며 고정 값인 일련 번호를 사용하였을 때 올바른 씨드 값을 계산할 확률이 더 높음을 알 수 있다. 또한 블록당 메시지 길이의 비율이 낮아질수록 올바른 씨드값을 계산할 확률이 높아지지만, False data에 대해서도 올바른 씨드값을 만들 확률이 높아져 적절한 매개변수를 선택하는 것이 중요함을 알 수 있다.

(표 3) 매개변수에 따른 FAR, FRR 측정결과

N/K/T	Error Rate	No BCH	Only BCH	BCH with Serial
511/358/18	FAR	0%	0%	0%
	FRR	100%	24.72%	20.66%
511/322/22	FAR	0%	0%	0%
	FRR	100%	11.81%	10.33%
511/286/27	FAR	0%	0%	0%
	FRR	100%	1.11%	0.74%
511/1112/59	FAR	0%	0%	43%
	FRR	100%	0.37%	0.00%

본 논문에서는 이미지 처리 및BCH 코드를 응용하여 이미지로부터 정확한 씨드를 추출하는 기법과 위 기법에 수반되는 이론을 기술하였다. 또한 실험결과를 통해서는 씨드를 안정적으로 생성하기 위해 일련 번호 같은 고정 값을 첨가해주는 것이 좋고, BCH 코드에 사용되는 매개변수의 선택이 중요함을 보였다. 차후 연구에서는 본 논문에서 검증하지 못한 공격 시나리오 테스트를 진행하고 내용을 확장시키고자 한다.

참고문헌

[1] 서태웅, 이성렬, 배병철, 윤이중, 김창수 “CCTV 보안관제 취약성 및 성능 분석”, 멀티미디어학회논문지 15(1), 93~100pages 2012.1

[2] 강민석, 배지수, 장태민, 강민섭 “AES 암호 알고리듬 기반 디지털 영상 보안 시스템의 설계“, 보안공학연구논문지, 제8권 제2호, 2011.4

[3] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith "Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data" Advances in Cryptology - EUROCRYPT 2004 pp 523-540

[4] Hank Wallace "Error Detection and Correction using the BCH code " 2001