Journal of The Korea Society of Computer and Information
Vol. 19, No. 9, September 2014
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2014.19.9.085

암호화와 감사 로깅에서 보안 요건 정의 연구

신 성 윤*, 이 강 호**

A Study of Definition of Security Requirements on Encryption and Audit Logging

Seong-Yoon Shin*, Kang-Ho Lee**

요 약

암호화란 정보를 의미를 알 수 없는 암호문으로 변환하여 불법적인 방법에 의해 데이터가 손실되거나 변경되는 것을 방지하는 방법이다. 감사 로깅이란 사용자의 활동, 예외사항, 정보보안사건에 대한 감사 로그를 생성하고, 조사와 접근통제 감시 지원을 위하여 일정 기간 동안 보존하는 것이다. 본 논문에서는 암호화에서는 중요 정보의 전송 또는 저장 시 정보의 기밀성과 무결성을 보장하여야 한다는 것을 제시한다. 암호화는 단방향 및 양방향 암호화를 적용하며 암호화 키는 안전성이 보장되어야 한다는 것도 제시한다. 또한, 감사 로그에서 부인 방지를 위해 모든 전자금융 거래 관련 내역은 로깅 및 보관되어야 한다는 것도 제시한다. 그리고 어플리케이션 접속로그 및 중요 정보에 대한 조회 및 사용 내역은 로깅 및 검토되어야 한다는 것도 제시하도록 한다. 본 논문에서는 암호화 및 로그 감사에 관한 실제 예를 들어 설명하도록 하여 안전한 데이터 전송과 주기적인 검토가 이루어지도록 하였다.

▸ Keywords : 암호화, 감사 로깅, 기밀성, 무결성, 접근 통제

Abstract

Encryption is a method to convert information to no-sense code in order to prevent data from being lost or altered by use of illegal means. Audit logging creates audit log of users' activities, exceptions, and information security events, and then conserves it for a certain period for investigation and access-control auditing. Our paper suggests that confidentiality and integrity of information should be guaranteed when transmitting and storing important information in encryption. Encryption should consider both one-way encryption and two-way one and that encryption key should assure security. Also, all history related to electronic financial transactions

•제1저자 : 신성윤 , 교신저자 : 이강호
•투고일 : 2014. 8. 1, 심사일 : 2014. 8. 12, 게재확정일 : 2014. 8. 28.
* 군산대학교 컴퓨터정보공학과(Dept. of Computer Information Engineering, Kunsan National University)
** 한국복지대학교 컴퓨터정보보안과(Dept. of Computer Information Security, Korea National University of Welfare)

should be logged and kept. And, it should be considered to check the details of application access log and major information. In this paper, we take a real example of encryption and log audit for safe data transmission and periodic check.

▸ Keywords : Encryption, Audit Logging, Confidentiality, Integrity, Access Contro

I. 서 론

암호화란 데이터 전송 시 타인의 불법적인 방법에 의해 데이터가 손실되거나 변경되는 것을 방지하기 위해 데이터를 변환하여 전송하는 방법이다[1]. 또한 암호화는 암호키를 이용해서 정보를 바로 해독할 수 없도록 변환하는 것으로 특정인만 해독할 수 있게 하는 것[2]이란 정의도 있다.

암호화에 관련된 연구로는 맵리듀스 기반의 분산 암호화 처리 방법[3], Java API에 포함되어 암호화 기능을 제공하는 JCA(Java Cryptography Architecture)를 이용하여 HDFS 암호화를 구현하고 성능 실험을 수행한 방법[4], 깊이정보 영상 콘텐츠를 숨기기 위한 암호화 방식[5]과 그 밖의 방법[6-10]같이 다양한 분야에 걸쳐서 암호화를 수행하고 실험하였다.

감사 로깅 시스템이란 컴퓨터 시스템에 대한 사용자의 접속 내역 및 각종 작업의 수행내역을 감사 로그에 저장하도록 하는 시스템이다.

감사 로깅 시스템은 사용자의 활동, 예외사항, 정보보안사건을 기록하는 감사로그를 생성하여야 하며 추후 조사와 접근통제 감시 지원을 위해 합의한 기간 동안 보존하여야 한다[11].

감사 로깅 시스템은 시스템 사용 내역과 통신망을 통한 접근 내역을 기록하는데, 이 내역은 불법적인 시스템 자원의 사용이나 통신망을 통한 불법 접근이 발생하였을 때, 그 경로를 추적하는 자료로 사용된다[12]고 하였다.

본 논문에서는 특정한 분야의 암호화 및 감사 로깅에 대하여 다루지는 어플리케이션 구현 단계 중 분석 단계에서 암호화와 감사 로깅에 대한 요건을 정의하도록 한다. 이에 따라 본 논문의 구성은 2장에서는 암호화에 대한 원칙, 암호화 대상 선정, 암호화 알고리즘 및 키 선정 기준, 그리고 암호화 키 관리 기준을 살펴보고, 3장에서는 감사 로깅의 원칙, 어플리케이션 로그 생성 기준 정의, IT 인프라 로그 생성 기준 정의, 그리고 로그 감사 기준을 정의한다. 4장에서는 실제 암호화와 로그 감사의 사례를 들어 설명하도록 하며, 5장에서 결론을 맺도록 한다.

II. 암호화

1. 암호화를 위한 원칙

암호화를 적용하기 위한 대상 데이터는 사전에 합의된 기준에 따라 식별되어야 하며, 암호화의 실행을 위한 알고리즘과 키의 강도 및 암호화 키 관리 요건은 명확하게 정의되어야 한다.

2. 암호화 대상 선정

암호화의 대상 선정은 그림 1과 같이 데이터의 등급 및 해당 데이터의 존재 양태에 따라서 정의한다.

데이터등급 / 암호화	DB 내 저장	어플리케이션 사용 시	네트워크 전송
1 등급	암호화	암호화	암호화
2 등급	일부 데이터 암호화	불필요	외부망:암호화 내부망:평문(전용선 사용)
3 등급	불필요	불필요	외부망:암호화 내부망:평문(전용선 사용)

그림 1. 데이터 암호화 기준 정의
Fig. 1. Definition of Data Encryption Standard

3. 암호화 알고리즘 및 키 선정 기준

암호화의 유형별로 그림 2와 같이 사용 가능한 안전한 알고리즘의 목록과 해당 암호화 유형의 안전성을 보장하기 위한 최소한의 키 길이 및 형태에 대한 기준을 정의한다.

구분		알고리즘	최소 키 길이	
			1 등급 데이터	2 등급 이상 데이터
암·복호화	대칭키	AES, SEED, ARIA, TWOFISH	128	128
	비대칭키	RSA, ElGamal	2048	2048
	타원곡선	ECC-ElGamal	224	224
전자서명		DSS, DSA, RSA	2048	2048
해쉬		MD5, SHA-1, SHA-512	256	256
MAC		HMAC-MD5, SHA-1	256	256

그림 2. 암호화 알고리즘 및 키 채택 기준
Fig. 2. Selection Standard of Encryption Algorithm and Key

4. 암호화 키 관리 기준

암호화 키의 안전한 관리를 위한 다음 그림 3과 같은 관리 기준을 정의한다.

키 관리 영역	키 관리 원칙 (예시)
키 생성(Generation)	모든 암호키는 승인된 알고리즘에 의해 생성 비밀키는 접근이 통제되는 설비에서 생성 마스터키와 세션키는 분리해서 관리
키 분배(Distribution) 및 등록(Registration)	분배를 위해 전송 중인 암호키는 유출, 변조되지 않고 수신자에게 전달 분배를 위해 전송 중인 키 재료(Keying Material)는 유출, 변조되지 않고 수신자에게 안전하게 전달 공개키를 등록할 때에는 그 무결성 및 신뢰성이 확인되어야 함
키 저장(Storage), 예비(Backup), 보관(Archive) 및 복구(Recovery)	모든 암호키 및 키 재료(Keying Material)는 운용 중 복구를 위해 적절한 백업이 이루어져야 함 유효기간 이후에도 복구가 필요한 암호키 및 키 재료(Keying Material)는 적절이 보관되어야 함 e.g. 서명 검증키, 키 암호화키, 마스터키 등
키의 삭제(Destruction) 및 폐기(Revocation)	폐기 예정 키의 모든 복사된 키는 삭제되어야 함 키가 등록해제 되기 전에 사용되었던 키 재료(Keying Material)는 삭제되어야 함

그림 3. 암호화 키 관리 기준
Fig. 3. Standard of Encryption Key Management

III. 감사 로깅

1. 감사 로깅의 원칙

시스템의 보안 수준을 유지하고, 법적인 규제 사항을 만족시키며, 악의적인 침해 행위나 내부 정보의 유출 행위를 감시하기 위해 필요한 모든 정보들은 저장되어야 하며 안전하게 관리되고 주기적으로 검토가 가능한 형태로 리포트가 생성되어야 한다.

2. 어플리케이션 로그 생성 기준 정의

시스템에서 수행되는 거래들 중 전자 금융 시행 세칙, 전자상거래법, 정보 통신망 법, 상법 등에서 강제하는 거래 로그에 대해서 그 종류와 형태별로 정의한다. 어플리케이션 로그 생성 기준을 정의한 예는 그림 4와 같다.

업무 유형	대상정보
거래 직접 내용	거래종류
	거래금액 및 거래 수수료,거래 일시, 당사자 정보
	전자적 장치 종류
	전자적 장치 식별 정보
	거래계좌의 명칭 또는 번호
	해당 거래 관련 전자적 장치 접속 기록
	전자지급수단별 거래 승인 기록
거래 관련 정보	접속 일시 및 접속 종료 일시
	접속 실패 회수(연속) 및 접속 실패 사유
	거래 실패 회수(연속) 및 거래 실패 사유
요청 및 처리 사항	오류정정 요구사실 및 처리결과에 대한 사항
	전자금융거래의 신청 및 조건의 변경에 대한 사항
이용 및 관리 기록	정보시스템 가동기록
	이용자정보 조회기록
	중요 원장 사용기록

그림 4. 어플리케이션 로그 생성 기준
Fig. 4. Creation Standard of Application Log

3. IT 인프라 로그 생성 기준 정의

시스템의 IT 인프라에서 내부 정보 유출 및 시스템 침해 시도 탐지를 위해서 저장이 필요한 로그에 대해서 정의한다. 그림 5는 IT 인프라 로그 생성 기준의 예시를 나타낸 것이다.

인프라	영역	로그
서버	인증	로그인 성공/실패
	계정	사용자/그룹 계정 생성,삭제,변경
	권한	권한의 생성,변경,삭제
	침해시도	프로세스 생성,변경,정지,삭제 시도(성공/실패)
데이터베이스	인증	로그인 성공/실패
	계정	사용자/그룹 계정 생성,삭제,변경
	권한	권한의 생성,변경,삭제
	정보작업	SQL DML, DDL, DCL 작업 구문 및 리턴데이터
네트워크장비	인증	로그인 성공/실패

그림 5. IT 인프라 로그 생성 기준
Fig. 5. Creation Standard of IT Infra

4. 감사 로깅의 기준 정의

정의된 생성 로그에 대해서 내부적 보안 요건이나 외부적 법적 요건 및 내부적 감사 역량을 고려하여, 로그에 대한 정기적 감사 실행 여부를 결정한다.

인프라	로그	정기 감사	실시간 모니터링
어플리케이션	전자금융 거래로그	-	-
서버	로그인 성공/실패	주간 감사 레포트	-
	업무 프로세스 중지 시도	주간 감사 레포트	실시간 SMS 경보
데이터베이스	로그인 성공/실패	주간 감사 레포트	-
	SQL DML, DDL, DCL 실행명령	주간 감사 레포트	-
네트워크장비	로그인 성공/실패	월간 감사 레포트	-

그림 6. 감사 로깅 기준 정의
Fig. 6. Definition of Audit Logging Standard

Ⅳ. 암호화와 감사 로깅의 실례

암호화는 우리 삶에 많은 원동력을 제공하여 우리가 하고 싶은 것이나 우리가 가고 싶은 곳이나 우리가 소중하다고 느끼는 것들을 보관하는 곳 등에서 많은 도움을 주고 있다. 특히 요즘에는 인터넷을 통한 정보의 거래가 급증하고 있으며 아울러 보다 안전하게 정보를 상용할 수 있는 환경의 조성을 위하여 암호화의 가치는 높아만 가고 있다.

또한 컴퓨터 시스템의 성능의 효율성과 신뢰성, 시스템의 안전성을 확인하기 위해 컴퓨터 시스템에서 독립적인 감사자가 정해진 규칙과 기준을 기반으로 컴퓨터 시스템의 성능을 종합적으로 평가하고 시스템 운용 관계자에게 조언이나 권고를 하는 감사 로깅 도한 그 중요성이 매우 커지고 있다.

여기서 우리는 암호화와 감사 로깅의 전반적인 실례를 들어서 설명하고 앞에서 설명한 내용들을 종합적으로 생각해 볼 수 있는 계기를 마련하고자 한다.

1. 암호화의 실례

암호화의 실례로서 암호화 프로그램 및 키 관리와 1등급 데이터의 암호화에 관한 상세 요건을 다음 표 1과 표 2에서 설명하고 있다.

표 1. 암호화 프로그램 및 키 관리
Table 1. Encryption Program and Key Management

요건 ID	요건 명	번호	상세 요건
O-O-01	암호화 프로그램 및 키 관리	1	암호 프로그램은 담당자를 정하고 원시 프로그램은 봉인하여 별도로 보관한다.
		2	암호 및 인증 시스템에 적용되는 키에 대하여 주입, 운용, 갱신, 폐기에 한 절차 및 방법을 마련하여 안전하게 관리 하여야한다.
		3	상용 암호화 솔루션 채택 시 국가 기관의 보안적합성 심의 제품 또는 CC 인증 획득 여부를 확인한다.

표 2. 1등급 데이터 암호화
Table 2. 1st Grade Data Encryption

요건 ID	요건 명	번호	상세 요건
O-O-02	1등급 데이터 암호화	1	1등급 데이터 입력 시 암호화 프로그램에 의거 단말에서 암호화 한다.
		2	내부망: 전용선을 통하여 데이터 전송 시 해당 데이터가 암호화된 상태로 전송한다.
		3	업무 서버(업무 어플리케이션)에서 해당 데이터가 처리될 때 암호화된 상태로 처리한다.
		4	업무 서버에서 처리된 해당 데이터가 데이터베이스 저장 시 암호화된 상태로 저장된다.

다음은 데이터 보안 등급의 예시로서 각 등급별로 데이터 등급을 정의하였고 각 등급에 해당하는 데이터의 예시들 들어서 설명하고 있다.

표 3. 데이터 보안 등급
Table 3. Data Security Grade

구분	데이터 등급 정의	예시
1등급	정보 유출 시 금융 거래 및 업무 처리 간에 치명적 영향을 미칠 수 있어, 단말, 네트워크, 서버, 데이터베이스까지 정보처리 및 보관 전 구간에 걸쳐 암호화 되어야 데이터로써, 사용자(고객 및 임직원 포함)를 인증하는 패스워드와 고객 및 내외부인의 금융 거래 시 필요한 비밀번호를 1등급으로 정의한다.	(1등급 데이터(예시)) 접속용 비밀번호(로그인 패스워드), 계좌 비밀번호, 이체 비밀번호, 일회용 비밀번호, 보안카드 DATA, 카드 비밀번호, 거래 승인 비밀번호
2등급	정보 유출 시 금융 거래 및 업무 처리 간에 중대한 영향을 미칠 수 있어, 정보의 일부분이 제한되어 보이고, 정보의 일부분이 암호화 저장 되어야 하는 데이터로써, 개인을 식별할 수 있는 고유 번호와 계좌 및 고객을 식별 할 수 있는 고유 번호를 2등급으로 정의한다.	(2등급 데이터(예시)) 주민번호, 계좌번호, 현금카드번호, 체크카드번호, 고객번호
3등급	정보 유출 시 고객 개인에게 영향을 미칠 수 있는 개인 정보로 정보의 일부분이 제한되어 보여야 하는 데이터로써, 주소, 전화번호, 핸드폰 번호, 이메일 주소를 3등급으로 정의한다.	(3등급 데이터(예시)) 주소, 전화번호, 핸드폰 번호, 이메일 주소
4등급	상기 1등급, 2등급, 3등급에 포함되지 않은 모든 업무 데이터	

2. 감사 로깅의 실례

감사 로깅의 실례로서 금융 거래 내역 기록과 상세 요건에 대한 내용과, 접속 및 사용 내역 기록과 상세 요건에 대한 내용을 표 4와 표 5에서 설명하고 있다.

표 4. 금융 거래 내역 기록
Table 4. Record of Financial Trade History

요건 ID	요건 명	번호	상세 요건
O-O-01	금융 거래 내역 기록	1	전자금융거래 관련 내역은 반드시 로깅 및 보관한다. - 전자금융 거래내용: 거래종류, 거래금액 및 수수료, 거래 일시, 거래자 정보, 전자적 장치(ATM/CD/지급용 단말기 등) - 식별정보, 거래 계좌 번호, 거래 관련 접속 기록, 전자 지급 수단별 거래 승인 기록 등 - 전자금융거래 관련정보: 접속 일시 및 접속 종료 일시, 접속 실패 횟수 및 내역, 거래 실패 횟수 및 내역 등
		2	전자금융거래를 위하여 데이터에 접근하여 읽기, 추가, 삭제, 변경 등의 사용 내역은 로깅 되어야 한다. - 사용자ID, 일시, 작업내역(변경 또는 조회내역) 등
		3	로그 데이터는 별도의 백업 시스템에 보관하는 것을 원칙으로 하며, 로그 데이터의 무결성이 보장되어야 한다.
		로그	- 로그 생성 시기: 전자금융거래 발생시 - 로그 포함 항목: 전자금융거래 내용, 사용자 ID, 일시, 작업내역 등 금융감독원에서 규제하는 항목 ※ 어플리케이션 보안 아키텍처 "로깅 및 감사" 부분에 세부 항목을 정의함
		감사	거래실패 내역 리포팅: 사용자 ID/IP, 실패횟수, 실패원인 등 로그 보관 주기 - 전자금융거래 관련 로그: 5년 - 1만 원 이하의 거래내역, 오류정정 요구사실 및 처리결과 등에 관한 사항: 1년

표 5. 전송 및 사용내역 기록
Table 5. Record of Transmission and Usage

요건 ID	요건 명	번호	상세 요건
O-O-02	전송 및 사용 내역 기록	1	모든 어플리케이션 사용자의 접속 내역은 로깅 되어야 한다. - 사용자 ID, 일시, 단말 IP/ID, 접속 성공/실패, 실패 내역 등
		2	어플리케이션에서 파일 다운로드, 출력/인쇄 시 관련사용 내역은 로깅 되어야 한다. - 사용자 ID, IP, 일시 등
		로그	접속 및 사용 관련 로그를 생성한다. 1. 로그 생성 시기: 사용자 시스템 접근(Log in), 조회, 변경 시 2. 로그 포함 항목: 사용자 ID, 일시, 단말 IP/ID, 접속 성공/실패 여부, 접속 실패 내역, 접속 방법, 사용 내역 등
		감사	접속내역 보고서를 생성한다. 1. 접속 실패 내역 리포트 생성 - 연속 접속 시도 시 실패 횟수가 5회 이상인 ID 리스트, 접속 실패 내역 2. 사용내역 리포트 생성 - 조회, 변경 내역 3. 로그 보관 주기 - 업무 시스템 접속 및 사용 기록: 1년

다음 표 6은 업무 유형에 따른 금융거래로그 대상 및 기준에 대한 설명으로서 로깅 대상별로 해당하는 거래에 대한 설명이 자세히 나타나 있다.

표 6. 금융거래로그 대상 및 기준
Table 6. Target and Standard of Financial Trade Log

업무 유형	로깅 대상	설명
전자금융거래 내용	거래종류	전자 지급거래, 전자 여-수신거래(인터넷 예금, 대출 등), 전자 증권거래(온라인 주식거래), 전자 보험거래 등
	거래금액 및 거래 수수료, 거래 일시, 당사자 정보	당사자 성명, ID, 접근매체에 관한 정보 등
	전자적 장치 종류	ATM, CD, 지급용 단말기, 컴퓨터, PDA, 유/무선 전화기, 디지털 TV 등
	전자적 장치 식별 정보	단말기 식별번호, IP, HDD 시리얼 번호, MAC 주소 등
	거래계좌의 명칭 또는 번호	계좌번호, 보험증권번호 등
	해당 거래 관련 전자적 장치 접속 기록	전자금융거래(단순조회 포함)관련 접속 기록 모두 포함
	전자지급수단별 거래 승인 기록	전자화폐, 선불전자지급수단, 전자자금이체, 직불전자지급수단, 전자채권, 신용카드(선불/직불), 전자어음, 기타 후불지급수단 등
전자금융거래 관련정보	접속 일시 및 접속 종료 일시	
	접속 실패 회수(연속) 및 접속 실패 사유	접속 실패 사유: 패스워드 오류
	거래 실패회수(연속) 및 거래 실패 사유	거래 실패 사유: 계좌비밀번호 오류, 이체비밀번호 오류, 공인인증 비밀번호

		오류, 수신계좌 오류 등
거래 확인 금융 감독원 고시 사항	오류정정 요구사실 및 처리결과에 대한 사항	오류정정 요구사항: (전자)요구서면, 요구통화내용 녹음기록, 처리결과(전자) 등
	전자금융거래의 신청 및 조건의 변경에 대한 사항	전자금융거래 신청서 및 조건변경신청서, 온라인 신청 및 변경 기록
이용 및 관리	정보시스템 가동기록	서버접속기록, 전산자료 사용기록, 접근기록 등
	이용자정보 조회기록	사용자, 사용일시, 변경 또는 조회 내용, 접속 방법 등
	원장 사용기록	조회, 수정, 삭제, 삽입 시 작업자, 작업 내용 등
	전산원장 파일 상호 불일치 원인 및 조치내용	

※ 금융거래 관련 로그 보관 기관: 5년, 단 1만 원 이하 거래 내역은 1년 보관

이와 같이 감사 로깅 시스템은 관련 시스템들의 사용 내역 및 네트워크를 이용한 접근 내역의 기록을 가지고 있다. 이러한 내역들은 비합법적 또는 불법적인 시스템 자원들의 사용이나 네트워크를 이용한 비합법적 또는 불법적 접근이 생겼을 때 그 접근 경로를 추적하는 데이터로 이용한다.

V. 결 론

본 논문에서는 정보의 전송에서 매우 중요한 암호화와 감사 로그의 정의 및 역할에 대하여 논하였다. 암호화는 중요 정보의 전송 또는 저장 시 정보의 기밀성과 무결성을 보장하여야 한다는 것과 단방향 및 양방향 암호화를 적용하여야 한다는 것, 그리고 암호화 키는 안전성이 보장되어야 한다는 것도 제시하였다. 또한, 감사로그에서 부인 방지를 위해 모든 전자 금융 거래 관련 내역은 로깅 및 보관되어야 한다는 것과 어플리케이션 접속로그 및 중요 정보에 대한 조회 및 사용 내역은 반드시 로깅 및 검토되어야 한다는 것 또한 제시하였다. 그리고 안전한 데이터 전송과 주기적인 검토가 이루어지기 위해서 수행하는 암호화 및 로그 감사에 관한 실제 예를 들어 설명하여 모든 사람들이 쉽게 이해하도록 하였다.

참고문헌

〔1〕 http://terms.naver.com/entry.nhn?docId=932499&cid= 43667&categoryId=43667

〔2〕 http://cafe.naver.com/handrake/46

〔3〕 Hyun-wook Kim, Sung-eun Park, Seong-yul Euh, "The Distributed Encryption Processing System for Large Capacity Personal Information based on MapReduce," J. Korea Inst. Inf. Commun. Eng., Vol. 18, No. 3, pp. 576~585, Mar. 2014

〔4〕 Seonyoung Park, Youngseok Lee, "A Performance Analysis of Encryption in HDFS," Journal of KIISE : Database, Vol. 41, No. 2, pp. 21-27, 2014

〔5〕 Hyun-Jun Choi, "Data Encryption Technique for Depth-map Contents Security in DWT domain," J. Korea Inst. Inf. Commun. Eng., Vol. 17, No. 5, pp. 1245-1252, 2013

〔6〕 Junho Jeong, Young Sik Hong, "Efficient Multi-indices Scheme for Searchable Encryption System against Brute Force Attack in Cloud Computing Environments," Journal of KIISE : Information Networking, Vol. 40, No. 5, pp. 286-293, 2013

〔7〕 JangYoung Chung, YoungSik Hong, "Distributed Image Encryption Schemes for Privacy-Preserving of Ultra High Resolution Images in Cloud Environments," Journal of Korea Convergence Security Association, Vol. 20, No. 4, pp.262-266, 2014

〔8〕 Youngho Seo, Eui-Sun Choi, Dong-Wook Kim "Efficient Encryption Technique of Image using Packetized Discrete Wavelet Transform," Journal of Korea Convergence Security Association, Vol. 17, No. 3, pp. 603-611, 2013

〔9〕 Sang Keun Gil," Optical CBC Block Encryption Method using Free Space Parallel Processing of XOR Operations," Korean Journal of Optics and Photonics, Vol. 24, No. 5, pp. 262-270, October 2013

〔10〕 Sangjin Kim, Heekuck Oh, "A Security Hole in Comparable Encryption," Jonornal of The Korea Institute of information Security & Cryptology, Vol. 23, No. 4, pp. 267-271, 2013

〔11〕 http://cafe.naver.com/softwarequality/book1621832/7 31

〔12〕 Kim Min Soo, Noh Bong Nam, "Information Security : Secure logging system with self-protecting function," The Transactions of the Korea Information Processing Society , Vol. 6, No. 9, pp. 2442-2450, 1999

저 자 소 개

신 성 윤

2003년 2월 : 군산대학교
컴퓨터과학과 이학박사
2006년~현재 : 군산대학교
컴퓨터정보공학과 교수
관심분야 : 영상처리, 컴퓨터비전,
가상현실, 멀티미디어
Email : s3397220@kunsan.ac.kr

이 강 호

1986.2. : 중앙대학교
전자공학과 공학석사
1991.8. : 중앙대학교
전자공학과 공학박사
현 재 : 한국복지대학교
컴퓨터정보보안과 교수
관심분야 : 정보보안, 디지털 영상처리
Email : lkh@knuw.ac.kr