논문 2022-1-4 http://dx.doi.org/10.29056/jsav.2022.06.04

디지털 홀로그래픽 프린팅 콘텐츠 저작권 보호를 위한 프록시 재암호화 기반 마켓 시스템 설계

김원빈*, 박경엽*, 조용준*, 신동명*†

Design of Proxy Re-encryption Based Market System for Copyright Protection of Digital Holographic Printing Contents

Won-Bin Kim*, Kyung-Yeob Park*, YongJoon Joe*, Dong-Myung Shin*†

요 약

홀로그램 프린팅 기술은 디지털 홀로그래픽 프린팅 콘텐츠를 현실세계의 평면에 출력하는 기술이다. 프린팅된 홀로그래픽 프린팅 콘텐츠는 평면 물체상에서 관측자의 시점에 따라 서로 다른 이미지를 보여주기 때문에 입체 형상을 별도의 장치 없이도 보여줄 수 있다. 하지만 디지털 홀로그래픽 프린팅 콘텐츠 원본은 A4 용지 크기를 출력하기 위해 약 10TB의 데이터 용량이 요구된다. 따라서 디지털 홀로그래픽 프린팅 콘텐츠 원본을 거래하는 마켓을 구성하기 위해서는 대용량의 데이터를 안정적으로 전송하기 위한 기술이 요구된다. 또한 디지털 홀로그래픽 프린팅 콘텐츠의 사용 범위와 권한을 넘어선 행위가 허용될 경우, 불법 복제 및 부당 이득으로 인한 금전적인 피해가 발생될 수 있다. 이러한 문제를 해결하기 위해 대용량의 디지털 데이터를 안정적으로 전송하면서도 안전하고, 효율적으로 전달하기 위한 마켓 및 DRM 기술이 필요하다. 본 연구에서는 이러한 요구사항을 만족하는 시스템을 설계하기 위해 프록시 재암호화 기술을 이용하였으며, 이 과정에서 요구되는 사항과 시스템 모델을 설계하고, 데이터를 안전하게 공유할 수 있는 프로토콜을 설계하였다. 프록시 재암호화 기술은 허가되지 않은 사용자에게 데이터와 암·복호화 키를 노출하지 않고도 데이터를 안전하고 효율적으로 전달할 수 있는 기술로 완전히 신뢰되지 않는 통신 및 서버 환경에 적합한 기술이다. 본 연구에서는 이러한 프록시 재암호화 기술을 기반으로 하여 디지털 홀로그래픽 프린팅 콘텐츠의 안전하고 효율적인 거래를 수행할 수 있는 기반을 마련하며, 더 나아가 홀로그램 프린팅 시장이 성장할 수 있는 동력을 제공할 것으로 기대한다.

Abstract

Hologram printing technology is a technology that outputs digital holographic printing contents on a flat surface of the real world. Since the printed holographic printing content shows different images depending on the observer's point of view on a flat object, a three-dimensional shape can be displayed without a separate device. However, the source of digital holographic printing content requires about 10 TB of data capacity to output A4 paper size. Therefore, in order to construct a market for trading original digital holographic printing contents, a technology for stably transmitting large amounts of data is required. In addition, if an act beyond the scope and authority of digital holographic printing content is allowed, financial damage may occur due to illegal copying and undue gain. To solve this problem, a market and DRM technology are needed to safely and efficiently transmit large amounts of digital data while stably transmitting it. In this study, proxy re-encryption technology was used to design a system that satisfies these requirements, and in this process, the required information and system model were designed, and a protocol to share data safely was designed. Proxy re-encryption technology is a technology that can safely and efficiently deliver data without exposing data and encryption/decryption keys to unauthorized users, and is suitable for communication and server environments that are not completely trusted. In this study, based on such proxy re-encryption technology, it is expected that the foundation for safe and efficient transaction of digital holographic printing contents will be prepared, and furthermore, it will provide a driving force for the growth of the holographic printing market.

한글키워드 : 디지털 홀로그래픽, 홀로그램 프린팅, 디지털 콘텐츠 마켓, 암호학, 프록시 재암호화
keywords : Digital Holographic, Hologram Printing, Digital Contents Market, Cryptography, Proxy Re-encryption

* 엘에스웨어(주) 소프트웨어연구소 연구개발본부
† 교신저자: 신동명(email: roland@lsware.com)

접수일자: 2022.06.07. 심사완료: 2022.06.12.
게재확정: 2022.06.20.

www.kci.go.kr

1. 서 론

최근 정보통신기술(ICT)의 발달과 함께 가상과 현실 사이의 경계가 사라지는 '초실감' 사회가 주목받게 되면서, 이러한 초실감 사회를 실현 가능하게 하는 기술로 VR/AR 기술도 발전하였다. 하지만 이러한 실감형 디지털 콘텐츠 기술은 장시간 사용할 수 없다는 단점과 기술적 제약이 존재한다. 따라서 별도의 전용기기가 필요없이 다수의 사용자에게 입체영상을 제공해줄 수 있는 홀로그램(Hologram) 기술이 다양한 분야에서 사용되고 있다. 하지만, 홀로그래픽 데이터의 생성을 위해서는 수많은 계산량이 필요하며 또한 생성되는 데이터 크기가 매우 방대하다는 단점이 존재한다. 이렇게 생성되는 데이터 크기가 매우 크기 때문에 데이터를 전송하기 위해 암호화할 경우 대칭키를 통한 암호화가 효율적이나 대칭키 암호는 사용자 간의 키 분배 문제(key distribution problem)가 발생한다.

따라서 본 논문에서는 디지털 홀로그램 이미지 데이터를 암복호화할 때 사용되는 대칭키를 안전하게 사용자 간 공유할 수 있는 프록시 재암호화 방식을 제안한다.

2. 관련 연구

2.1 홀로그램

홀로그램이란 홀로그래피(Holography) 기술을 통해 획득한 패턴 데이터를 복원한 영상을 의미한다. 홀로그래피란 두 빛의 간섭효과를 통해 어떤 물체의 3차원 정보를 기록 및 재생하는 기술을 의미한다. 이러한 홀로그램 기술은 아날로그 홀로그램과 디지털 홀로그램으로 나눌 수 있는데, 아날로그 홀로그램은 필름에 광원으로 레이저를 사용하여 필름을 통해 실물을 입체로 제작하는 방식이고, 디지털 홀로그램은 사물에 반사된 빛을 디지털화하여 기록 및 생성하고 이를 디스플레이 장치를 통해 재현하는 기술을 의미한다. 이러한 홀로그램 기술은 여가, 의료, 유통 등 여러 분야에 적용될 수 있으나 프로세서 속도, 용량 등의 기술적 난제 또한 존재한다.

2.2. 홀로그램 마켓

홀로그램 마켓은 디지털 홀로그래피 원본 이미지를 거래하는 마켓을 의미한다. 더 나아가 본 연구에서는 홀로그램 프린팅을 수행하기 위한 디지털 홀로그래피 원본 이미지를 거래하는 디지털 마켓 및 DRM 시스템을 목표로 한다. 이러한 홀로그램 마켓이 갖는 기존의 데이터 거래 시스템, 데이터 마켓과의 대표적인 차별점은 데이터의 크기를 들 수 있다. 일반적으로 디지털 데이터 마켓 또는 DRM 시스템에서 거래·전송되는 데이터는 수 KB에서 수백 GB까지 천편일률적인 데이터 크기를 갖는다. 하지만 A4용지 크기의 홀로그램 프린팅을 위한 디지털 홀로그래피 원본 이미지의 용량은 10TB에 이른다. 따라서 대용량의 데이터를 안정적으로 제공하기 위한 방법이 요구된다. 또한 상업적인 목적을 위한 데이터 원본이 제공되는 형태이기 때문에 허가된 사용 범위를 넘어선 데이터 이용 또는 데이터의 유출 문제를 고려해야만 한다. 본 연구에서는 이러한 문제를 고려하여 데이터를 안전하고 효율적으로 제공할 수 있는 방법으로 프록시 재암호화를 이용하여 시스템을 설계하였다.

2.3. 프록시 재암호화 (Proxy re-encryption)

프록시 재암호화는 완전히 신뢰할 수 없는, 반신뢰(Semi-trusted) 환경의 프록시 서버를 통해 데이터 소유자가 제 3자에게 데이터를 안전하게 위임하는 기술이다[1]. 기존의 peer-to-peer 데이터 공유 방식은 데이터 소유자가 데이터 수신자

www.kci.go.kr

의 수만큼 데이터를 암호화하고 전송해야 하기 때문에 수신자 수에 비례하여 많은 계산 및 통신 오버헤드가 발생한다. 프록시 재암호화 기술은 이러한 문제를 해결하기 위해 프록시 서버를 이용한다. 데이터 소유자는 프록시 서버에 데이터를 한 번만 업로드한 뒤, 수신자의 요청에 따른 데이터 전송은 프록시 서버가 수행하는 방법을 이용한다. 이 과정에서 프록시 서버는 암호화된 데이터의 내용을 볼 수 없으며, 오로지 데이터 소유자의 요청에 따라 암호화된 데이터를 변환하고, 수신자에게 전송하는 역할만을 수행한다. 이러한 특징을 이용하여 본 연구에서는 홀로그램 데이터의 내용을 노출하지 않고도 프록시 서버를 통해 데이터를 안전하게 제공하기 위한 방법으로 프록시 재암호화 기술을 활용한다.

2.4 ID기반 프록시 재암호화 (IBPRE; ID-based PRE)

ID 기반 프록시 재암호화는 ID 기반 암호화(IBE; ID-based Encryption)를 기반으로 하는 프록시 재암호화 기법이다. 이 기법은 사용자의 식별자인 ID를 이용하여 공개키를 생성하기 때문에 ID를 사용하는 다양한 환경에서 효과적으로 이용될 수 있다. 예를 들어, 클라우드 서비스는 모든 사용자가 ID를 가지고, ID로 각 사용자를 식별할 수 있도록 하여 상호간의 데이터 전달이 이루어질 수 있다. IBPRE는 다양한 형태가 제안되었으며, 2012년 Lei Xu 등은 인증서를 사용하지 않는 방법인 Certificateless PRE(CL-PRE)를 제안하였다[2]. CL-PRE는 인증서를 사용하지 않기 때문에 인증서를 생성하고 사용하는 기존의 IBPRE 보다 더욱 낮은 연산량으로 사용자를 식별·증명할 수 있다. 또한 키 생성 센터(KGC; Key Generation Center)가 직접 사용자의 개인키를 생성하지 않기 때문에 KGC로 인한 키 에스크로 문제에도 안전하다. 현재 CL-PRE를 기반으로 한 다양한 연구가 수행되고 있다[3-5].

2.5. 브로드캐스트 프록시 재암호화(BPRE; Broadcast PRE)

일반적으로 PRE는 한 명의 송신자가 한 명의 수신자에게 데이터를 위임하는 형태를 갖는다. 따라서 수신자의 수가 증가함에 따라 재암호화 횟수도 증가하게 되어 다수의 수신자에게 데이터를 위임할 경우 많은 오버헤드를 발생시키게 된다. 이러한 문제를 해결하기 위해 다중 수신자 암호화(MRE; Multi-Receiver Encryption)[6-13]을 기반으로 하는 브로드캐스트 프록시 재암호화가 Chu, C, K et al.에 의해 제안되었다[14]. 이와 같은 방법을 통해 한 번에 한 명의 수신자에게만 데이터를 위임할 수 있는 기존의 PRE의 제약을 벗어날 수 있게 되었다. 하지만 이러한 BPRE는 대부분 KGC 또는 브로드캐스트 센터(BC; Broadcast Center)를 통해 재암호화키를 생성하는 방식을 이용한다. 이러한 방식은 데이터를 브로드캐스트 할 때 송신자의 연산 부담을 줄여줄 수 있다. 하지만 반대로 KGC/BC가 데이터 수신자를 식별할 수 있기 때문에 프라이버시 노출 문제가 발생할 수 있다. 또한 기존의 MRE는 대부분 IBPRE를 이용하기 때문에 키 에스크로 문제 또는 인증서 생성에 불편함을 가질 수 밖에 없다. 이러한 문제를 해결하기 위해 본 연구에서는 CL-PRE와 MRE를 기반으로 하는 CL-BPRE를 제안한다.

3. 시스템 설계

본 장에서는 본 연구에서 제안하는 방식의 기본 설계를 수행하고 요구사항을 분석한다.

www.kci.go.kr

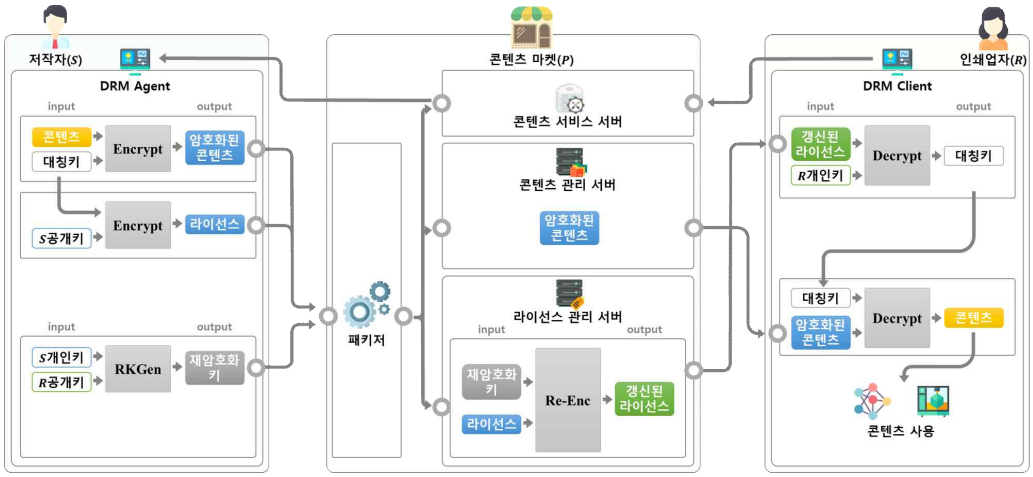


그림 1. 제안하는 시스템의 구조도
Fig. 1. Structural diagram of the proposed system

3.1 시스템 모델

본 연구에서 제안하는 시스템의 전체적인 형태는 그림 1과 같다. 본 연구에서 제안하는 시스템 모델에는 총 4개의 참여객체로 이루어져 있으며, 실제 데이터 거래에는 세 개의 객체가 참여하게 된다.

- **KGC(Key Generation Center):** KGC는 사용자의 키를 생성·등록하고 관리하는 역할을 수행한다. 이러한 KGC는 시스템을 이용하기 위한 공통 매개변수를 제공하여 모든 사용자가 동일한 연산 프로세스를 수행할 수 있도록 한다.
- **콘텐츠 마켓(Proxy Server):** 콘텐츠 마켓은 프록시 재암호화에서의 프록시 서버의 역할을 수행한다. 콘텐츠 마켓은 저작자로부터 수신한, 암호화된 콘텐츠와 라이선스를 보관하고 관리하는 역할을 한다. 본 제안방식에서 콘텐츠 마켓은 콘텐츠의 정보를 게시하고 제공하는 콘텐츠 서비스 서버, 암호화된 콘텐츠를 보관하는 암호화된 콘텐츠, 허가된 사용자만 콘텐츠를 이용할 수 있도록 하는 라이선스를 보관 및 관리하는 라이선스 관리 서버로 구성된다.
- **저작자(Sender):** 저작자는 프록시 재암호화의 송신자에 해당하는 사용자를 의미한다. 저작자는 콘텐츠를 생성하고 콘텐츠 마켓에 등록하는 사용자이다. 따라서 자신이 직접 생성한 콘텐츠를 안전하게 콘텐츠 마켓에 등록하기 위해 데이터의 암호화를 수행하고 라이선스를 생성한다. 또한 인쇄업자의 요청에 따라 저작자의 공개키로 재암호화키를 생성하여 콘텐츠 마켓에 제공하는 역할을 수행한다. 저작자는 사용자에 포함된다.
- **인쇄업자(Receiver):** 인쇄업자는 프록시 재암호화의 수신자에 해당하는 사용자를 의미한다. 인쇄업자는 콘텐츠 마켓이 제공한 콘텐츠 목록에서 자신이 필요한 콘텐츠를 선택하고 요청한다. 이후 저작자가 제공한 라이선스를 통해 콘텐츠 마켓으로부터 암호화된 콘텐츠와 갱신된 라이선스를

www.kci.go.kr

획득한다. 인쇄업자는 획득한 암호화된 콘텐츠와 갱신된 라이선스, 자신의 개인키를 이용하여 콘텐츠 원본을 획득할 수 있다. 이후, 획득한 콘텐츠 원본을 이용하여 홀로그램을 출력할 수 있다. 인쇄업자는 사용자에 포함된다.

3.2 시스템 요구사항

본 연구에서 제안하는 시스템의 요구사항은 다음과 같다.

- **기밀성(Confidentiality):** 모든 프로세스에서 데이터 권한이 없는 사용자는 데이터의 내용을 알 수 없어야 한다.
- **가용성(Availability):** 콘텐츠 마켓에 저장된 데이터는 적법한 사용자에게 제공할 수 있어야 한다. 이를 위해 데이터에 접속하는 사용자는 자신이 적법한 사용자임을 증명해야 하며 언제든지 원하는 데이터를 사용할 수 있어야 한다.
- **프라이버시 보존(Privacy Preserving):** 데이터를 수신하는 인쇄업자는 자신이 수신한 데이터와 라이선스를 통해 다른 인쇄업자를 식별할 수 없어야 한다.
- **반신뢰(Semi-trust):** 콘텐츠 마켓은 완전한 신뢰를 갖지 않는 것으로 가정한다. 콘텐츠 마켓은 요청한 것은 정확히 처리하지만 저작자가 위탁한 콘텐츠를 이용하여 부당이득을 취하거나 저작자에게 손해를 발생시킬 수 있다. 따라서 반신뢰된 환경에서도 안전하고 정확한 데이터 거래가 이루어질 수 있어야 한다.
- **복호화 공정성(Decryption Fairness):** 데이터를 수신한 인쇄업자는 다른 인쇄업자가 데이터를 복호화하는 과정에서 불리하도록 영향을 줄 수 없어야 한다.

4. 제안방식

본 장에서는 본 연구에서 제안하는 방식의 설명을 수행한다.

4.1 시스템 매개변수

본 제안방식의 시스템 매개변수는 다음과 같다.

표 1. 시스템 매개변수
Table 1. System parameters

매개변수	설명
*	참여객체 (KGC, 사용자 i, 송신자 S, 콘텐츠 마켓 P, 수신자 R)
p,q	λ-bit 소수 정수
E	타원곡선
F_q	위수 q에 대한 유한체
λ	비밀 매개변수
l_1,l_2	메시지 공간의 길이
P	G_q 상의 랜덤 매개변수
G	타원곡선 E 상의 덧셈군
G_q	위수 q에 대한 G의 부분군
ID_*	참여 객체 $*$의 ID
msk	KGC의 마스터 비밀키
mpk	KGC의 마스터 공개키
sk_i	사용자 i의 개인키
pk_i	사용자 i의 공개키
$RK_{(SND\rightarrow RCV)}$	재암호화키
M	메시지 공간
m	콘텐츠 원본
CT	암호화된 콘텐츠
LC	라이선스
LC_{Re}	갱신된 라이선스
$H_1 - H_7$	일방향 해시함수

www.kci.go.kr

4.2 메인 알고리즘

본 제안방식은 다음과 같은 알고리즘으로 구성되어 있다.

4.2.1 Setup Phase

이 단계에서는 KGC에 의해 시스템의 공개 매개변수를 선택 및 계산하고 공개된다.

- **Setup:** 이 알고리즘은 KGC가 수행하는 알고리즘으로 비밀 매개변수 λ를 입력으로 하여 msk, mpk를 출력한다.
  1. KGC는 λ-bit 소수 정수 p, q를 선택하고 유한체 F_q 상의 타원곡선 E을 정의한다. 그리고 E상의 곱셈군 G와 G의 부분군 G_q를 정의한다.
  2. KGC는 $P \in G_q$와 $d \in Z_q^*$를 선택하고 $P_{pub} = s \cdot P$를 계산한다.
  3. KGC는 일방향 해시 함수 $H_1 - H_7$을 정의하고 마스터 공개키 $mpk = \{p, q, l_1, l_2, E, G, G_q, P, P_{pub}, M, H_1 - H_7\}$를 공개한다.

4.2.2 Key Generation Phase

이 단계에서는 각 사용자의 키를 생성한다.

- **Set-Secret-Value:** 이 알고리즘은 사용자 i에 의해 수행되는 알고리즘이다. 사용자 i는 랜덤으로 $w_i \in Z_q^*$를 선택하고 이를 이용하여 $W_i = w_i \cdot P$를 계산한다. 이후 (W_i, ID_i)를 KGC에게 전송한다.
- **Partial-Key-Extract:** 이 알고리즘은 KGC에 의해 수행되는 알고리즘이다. KGC는 사용자 i가 전송한 (W_i, ID_i)를 이용하여 다음의 연산을 수행하고 (V_i, t_i)를 사용자 i에게 반환한다.
  1. KGC는 랜덤하게 $v_i \in Z_q^*$를 선택하고 $V_i = v_i \cdot P$와 $t_i \leftarrow v_i + sH_7(V_i, W_i, ID_i) + H_5(sW_i, ID_i) \pmod q$를 계산한다.
  2. KGC는 (V_i, t_i)를 사용자 i에게 반환한다.
- **Set-Private-Key:** 이 알고리즘은 사용자 i에 의해 수행되는 알고리즘이다. 사용자 i는 KGC가 전송한 (V_i, t_i)와 자신이 생성한 w_i를 이용하여 연산 $u_i \leftarrow t_i - H_5(w_i P_{Pub}, ID_i)$을 수행하고 개인키 $sk_i = (u_i, w_i)$를 생성한다.
- **Set-Public-Key:** 이 알고리즘은 사용자 i에 의해 수행되는 알고리즘이다. 사용자는 KGC가 전송한 (V_i, t_i)와 자신이 생성한 W_i를 이용하여 $pk_i = (V_i, W_i)$를 생성한다.

4.2.3 Data Storing Phase

이 단계에서는 저작자에 의해 데이터가 생성 및 암호화되고 라이선스가 생성되어 콘텐츠 마켓에 보관된다,

- **Enc:** 이 알고리즘은 저작자에 의해 수행되는 알고리즘이다. 저작자는 자신의 공개키 pk_{SND}로 다음의 연산을 수행하여 콘텐츠 m을 암호화한다.
  1. 저작자는 $k \leftarrow H_7(V_{SND}, W_{SND}, ID_{SND})$, $z \leftarrow H_2(m \| k)$, $Z \leftarrow zP$를 순차적으로 계산한다.
  2. 저작자는 공개키 pk_{SND}를 이용하여 $\Phi_{SND} \leftarrow z \cdot (V_{SND} + H_7(V_{SND}, W_{SND}, ID_{SND})P_{pub} + W_{SND})$를 계산한다.
  3. 저작자는 $\alpha \leftarrow H_1(u_{SND} \cdot w_{SND})$, $\theta \leftarrow H_1(\Phi_{SND} \cdot \alpha)$, $C \leftarrow H_4(Z, \theta) \oplus (m \| k)$를 순차적으로

www.kci.go.kr

계산한다.

4. 저작자는 암호화된 콘텐츠 $CT = C$와 라이선스 $LC = Z$를 콘텐츠 마켓에 전송한다.

4.2.4 Data Provision Phase

이 단계에서는 인쇄업자의 요청에 따라 저작자가 재암호화키를 생성하고 콘텐츠 마켓에 의해 인쇄업자에게 데이터가 제공되는 단계이다.

- **Re-Key-Gen:** 이 알고리즘은 저작자에 의해 수행되는 알고리즘이다. 저작자는 인쇄업자가 콘텐츠 마켓을 통해 전달한 요청 따라 재암호화키 $RK_{S \to R}$를 다음과 같이 생성한 뒤 콘텐츠 마켓에 전달한다.
  1. 저작자는 수신자 $j (j \in RCV)$ $\Phi_j \leftarrow z \cdot (V_j + H_7(V_j, W_j, ID_j) \cdot P_{pub} + W_j)$을 계산한다.
  2. 저작자는 무작위로 $\beta \in Z_q^*$를 선택하고 $f(x) = \Pi_{j=0}^{n}(x - \Phi_j) + \beta (\mathrm{mod} q) = x^n + a_{(n-1)}x^{(n-1)} + \cdots + a_1 x + a_0$ 을 계산한다.
  3. 저작자는 개인키 sk_{SND}를 이용하여 $\sigma \leftarrow (u_{SND} + w_{SND}) \cdot \alpha \cdot \beta^{(-1)}$를 계산한다.
  4. 저작자는 재암호화키 $RK_{(SND \to RCV)} = (rk_1, rk_2) = (\sigma, a_0, a_1, \cdots, a_{(n-1)})$를 콘텐츠 마켓에 전송한다.
- **Re-Enc:** 이 알고리즘은 콘텐츠 마켓에 의해 수행되는 알고리즘이다. 콘텐츠 마켓은 저작자가 전송한 라이선스 LC와 재암호화키 $RK_{(SND \to RCV)}$를 이용하여 갱신된 라이선스 LC_{Re}을 생성한다.
  1. 콘텐츠 마켓은 갱신된 라이선스 $LC_{Re} = \{LC_{Re,1}, LC_{Re,2}, LC_{Re,3}\} = \{LC, LC \cdot rk_1, rk_2\}$을 계산한다.
  2. 콘텐츠 마켓은 갱신된 라이선스 LC_{Re}과 암호화된 콘텐츠 CT를 인쇄업자에게 전송한다.
- **Dec:** 이 알고리즘은 인쇄업자에 의해 수행되는 알고리즘이다. 인쇄업자는 콘텐츠 마켓이 전송한 갱신된 라이선스 LC_{Re}와 자신의 개인키 sk_{RCV}, 암호화된 콘텐츠 CT를 이용하여 콘텐츠 원본을 획득할 수 있다.
  1. 인쇄업자는 sk_{SND}와 $LC_{Re,3}$을 이용하여 $\Phi'_{RCV} \leftarrow (u_{RCV} + w_{RCV}) \cdot LC'_{Re,1}$를 계산한 뒤, $f(x) = x^n + a_{(n-1)}x^{(n-1)} + \cdots + a_1 x + a_0$와 $\beta' = f(\Phi'_{RCV})$, $\theta' = H_1(LC'_{Re,2} \cdot \beta')$를 순차적으로 계산한다.
  2. 인쇄업자는 $m \leftarrow CT' \oplus H_4(LC'_{Re,1}, \theta')$를 계산하여 콘텐츠 원본을 획득한다.

5. 제안방식 분석

본 장에서는 본 연구에서 제안하는 방식의 시스템 요구사항 분석을 수행한다.

- **기밀성(Confidentiality):** 본 제안방식에서는 허가되지 않은 사용자에 의한 데이터 내용의 노출을 방지하기 위해 타원곡선 암호화 기반의 암호 프로토콜을 구성하였다. 또한 다수의 인쇄업자에게 동일한 데이터를 제공하기 위해 다항식을 구성하여 수신자 증명-복호화 프로세스를 구성하였다. 이러한 프로세스는 먼저 수신자 증명과정을 수행하며, 이 과정에서 사용된 다항식

www.kci.go.kr

은 다음과 같다.

$$f(x) = \Pi_{i=0}^{n}(x - \Phi_j) + \beta(\mathrm{mod}q)$$
$$= x^n + a_{(n-1)}x^{(n-1)} + \cdots + a_1 x + a_0$$

저작자는 이 다항식을 생성하기 위해 수신자의 공개키를 이용하여 Φ_{RCV}을 다음과 같이 생성한다.

$$\Phi_{RCV} \leftarrow z \cdot (V_{RCV} + H_7(V_{RCV}, W_{RCV}, ID_{RCV}) \cdot P_{pub} + W_{RCV})$$

하지만 수신자는 이 다항식을 통해 본인이 수신자임을 증명하기 위해 자신의 개인키를 이용하여 Φ'_{RCV}을 다음과 같이 생성한다.

$$\Phi'_{RCV} \leftarrow (u_{RCV} + w_{RCV}) \cdot LC'_{Re,1}$$

이때, $\Phi_{RCV} = \Phi'_{RCV}$가 성립할 때만 복호화가 가능하며, 다음의 등식이 성립한다.

$$\begin{aligned}\Phi'_{RCV} &= (u_{RCV} + w_{RCV}) \cdot LC'_{Re,1} \\ &= ((t_{RCV} - H_7(w_{RCV} \cdot P_{Pub}, ID_{RCV})) \\ &\quad + w_{RCV}) \cdot Z \\ &= ((t_{RCV} - H_7(w_{RCV} \cdot P_{Pub}, ID_{RCV})) \\ &\quad + w_{RCV}) \cdot z \cdot P \\ &= ((v_{RCV} + sH_7(V_{RCV}, W_{RCV}, ID_{RCV}) \\ &\quad + H_5(s W_{RCV}, ID_{RCV}) \\ &\quad - H_5(w_{RCV} \cdot P_{Pub}, ID_{RCV})) + w_{RCV}) \\ &\quad \cdot z \cdot P \\ &= ((v_{RCV} + sH_7(V_{RCV}, W_{RCV}, ID_{RCV})) \\ &\quad + w_{RCV}) \cdot z \cdot P \\ &= (v_{RCV} \cdot P + sH_7(V_{RCV}, W_{RCV}, ID_{RCV}) \cdot P \\ &\quad + w_{RCV} \cdot P) \cdot z \\ &= (V_{RCV} + H_3(V_{RCV}, W_{RCV}, ID_{RCV}) \cdot P_{Pub} \\ &\quad + W_{RCV}) \cdot z \\ &= \Phi_{RCV}\end{aligned}$$

이에 따라 지정된 인쇄업자 외에는 수신자 인증 및 복호화가 불가능하다.

- **가용성(Availability):** 저작자로부터 이용 콘텐츠 권한을 제공받은 인쇄업자는 저작자와의 직접적인 통신을 수행하지 않고도 콘텐츠 데이터를 이용할 수 있어야 한다. 이를 위해 본 제안방식에서는 저작자로부터 권한을 제공 받은 이후에는 콘텐츠 마켓과의 통신을 수행하여 콘텐츠 데이터를 이용할 수 있도록 설계하였다. 일반적으로 콘텐츠 마켓은 클라우드 서비스 또는 CDN(Content Delivery Network)와 같은 형태로 구성되기 때문에 저작자-소유자간의 peer-to-peer 통신에 비해 더욱 안정적인 서비스 제공이 가능하다. 또한 본 제안방식에서 콘텐츠 마켓은 반신뢰된 환경을 전제로 하기 때문에 콘텐츠 데이터 원본과 저작자가 설정한 암·복호화 키가 노출되지 않으면서도 저작자가 설정한 증명 과정을 수행할 수 있도록 설계되었다.
- **프라이버시 보존(Privacy Preserving):** 본 제안방식에서는 여러 수신자 중 한 명이 다른 수신자를 식별할 수 있을 경우 해당 수신자에 대한 프라이버시 침해가 발생할 수 있을 것으로 판단하였다. 따라서 이러한 문제를 해결하기 위해 본 제안방식은 수신자 증명 과정에서 수신자 본인 외에는 다른 수신자를 식별할 수 없도록 설계하였다. 이러한 프로세스는 기밀성 항목에 서술된 증명 방식과 같이 수신자인 인쇄업자는 자신의 개인키로만 증명을 수행할 수 있으며, 다른 수신자를 식별하기 위해서는 해당 수신자의 개인키가 요구된다. 따라서 수신자인 인쇄업자들의 개인키의 유출이 발생하지 않는 이상 다른 수신자를 식별할 수 없다.
- **반신뢰(Semi-trust):** 본 연구제서는 콘텐츠 마켓을 반신뢰된 환경으로 가정하였다. 이를 위해 콘텐츠 마켓은 저작자가 업로드한 데이터의 내용 C와 라이선스 정보 LC,

www.kci.go.kr

재암호화 키 $RK_{(SND \rightarrow RCV)}$의 내용을 알 수 없도록 비가역적인 설계를 하였다.

$$C \leftarrow H_4(Z,\theta) \oplus (m \parallel k)$$

$$LC \leftarrow Z = zP = H_2(m \parallel k) \cdot P$$

$$RK_{(SND \rightarrow RCV)} \leftarrow (rk_1, rk_2) = (\sigma, a_0, a_1, \cdots, a_{(n-1)})$$

이와 같은 설계를 통해 콘텐츠 마켓은 저작자가 제공한 정보를 보관하고 정해진 연산만을 수행할 수 있으며, 이 과정에서 데이터의 내용이 노출되지 않는다.

- **복호화 공정성(Decryption Fairness):** 본 연구에서는 여러명의 수신자를 지정할 수 있도록 설계하였다. 따라서 지정된 모든 수신자들은 동등한 수준의 권리와 역할을 부여받는다. 하지만 내·외부 공격자에 의해 일부 수신자가 동등한 수준의 권리와 역할을 부여받지 못할 수 있는 잠재적인 위협이 존재한다. 대표적으로 제공된 데이터의 일부 값을 변경하여 특정 수신자의 복호화를 불가능하게 하거나 연산 측면에서 불리하게 만드는 방법이 존재한다. 본 연구에서는 이러한 문제를 해결하기 위해 다음과 같은 다항식을 구성하였다.

$$f(x) = \Pi_{j=0}^{n}(x - \Phi_j) + \beta (\mathrm{mod} q)$$

$$= x^n + a_{(n-1)}x^{(n-1)} + \cdots + a_1 x + a_0$$

이 다항식은 수신자들의 정보를 하나의 다항식으로 구성하여 특정 수신자에게만 불공정함을 제공할 수 없도록 하였다. 만약 본 다항식을 이용하여 특정 수신자에게 불공정성을 제공하려면 모든 수신자 정보를 알고 있어야 하며, 이는 송신자인 저작자만이 가능한 공격으로 볼 수 있다.

6. 결 론

홀로그램 프린팅 시장은 미개척된 시장으로 현재 다양한 연구가 시도되고 있다. 먼저, 디지털 홀로그래픽 프린팅 콘텐츠를 현실 세계에 출력하기 위한 방법이 지속적으로 연구되고 있다. 홀로그램 기술은 향후 Head Mount Display(HMD) 등을 기반으로 하는 3D 이미지의 구현을 대체할 수 있는 기술로 자리매김 할 것으로 전망하며, 이를 통해 현실세계에서도 별도의 웨어러블 디바이스 없이 AR(Augmented Reality)·MR(Mixed Reality) 기술을 활용할 수 있을 것이다. 하지만 현재 홀로그램 기술은 디지털 홀로그래픽 프린팅 콘텐츠를 현실 세계에 출력하는 단계에서부터 어려움을 겪고 있으며, 이를 해결하기 위해서 지속적인 연구가 수행되고 있다. 또한 디지털 홀로그래픽 프린팅 콘텐츠는 사용자가 바라보는 시점과 각도에 따라 다른 이미지를 보여주어야 하기 때문에 많은 용량을 요구할 수 밖에 없다. 일반적으로 A4 용지 크기의 홀로그램을 보여주기 위해서는 약 10TB 용량의 디지털 홀로그래픽 프린팅 콘텐츠 원본을 이용해야만 한다. 하지만 이러한 대용량 데이터를 안정적이고 빠르게 전송하는 것은 현 시점에서는 매우 어려운 일이다. 또한 데이터의 크기 만큼 많은 인력과 시간이 투입되기 때문에 만약 디지털 홀로그래픽 프린팅 콘텐츠 원본이 허가된 범위를 넘어서 남용되거나 부당하게 사용될 경우 큰 피해를 발생시킬 수 있다. 본 연구에서는 이러한 점을 고려하여 홀로그램 프린팅 시장이 성장되는 시점에서 시장을 안정적으로 지지할 수 있는 기반인 마켓 및 DRM 기술을 연구하는 것을 목표로 하였다. 이를 위해 본 연구에서는 프록시 재암호화 기술과 타원곡선암호화 기술 등을 활용하여 완전히 신뢰할 수 없는 환경에서도 안전하고 안정적으로 데이터를 거래·제공할 수 있는 시스템을 설계하였다. 이를 통해 홀

www.kci.go.kr

로그램 프린팅 시장이 성장하기 위한 기본 발판을 제공할 수 있을 것으로 기대하며, 더 나아가 홀로그램이 아닌 다른, 대용량 데이터 거래 시장에서도 활용될 수 있는 핵심 기술로 자리매김 할 것이라 기대한다.

본 연구는 문화체육관광부 및
한국콘텐츠진흥원의 2022년도 저작권기술
연구개발사업으로 수행되었음
(과제명 : 디지털 홀로그래픽 프린터용 콘텐츠
저작권 보호 및 응용 기술 개발,
과제번호 : CR202104002, 기여율: 100%)

참 고 문 헌

[1] Matt Blaze, Gerrit Bleumer, and Martin Strauss. Divertible protocols and atomic proxy cryptography. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 127 - 144. Springer, 1998. DOI: https://doi.org/10.1007/BFb0054122

[2] Lei Xu, Xiaoxin Wu, and Xinwen Zhang. Cl-pre: a certificateless proxy re-encryption scheme for secure data sharing with public cloud. In Proceedings of the 7th ACM symposium on information, computer and communications security, pages 87 - 88, 2012. DOI: https://doi.org/10.1145/2414456.2414507

[3] Xiaoxin Wu, Lei Xu, and Xinwen Zhang. Poster: a certificateless proxy re-encryption scheme for cloud-based data sharing. In Proceedings of the 18th ACM conference on computer and communications security, pages 869 - 872, 2011. DOI: https://doi.org/10.1145/2046707.2093514

[4] Kang Yang, Jing Xu, and Zhenfeng Zhang. Certificateless proxy re- encryption without pairings. In International Conference on Information Security and Cryptology, pages 67 - 88. Springer, 2013. DOI: https://doi.org/10.1007/978-3-319-12160-4_5

[5] Xiaoyu Zheng, Yuyang Zhou, Yalan Ye, and Fagen Li. A cloud data deduplication scheme based on certificateless proxy re-encryption. Journal of Systems Architecture, 102:101666, 2020. DOI: https://doi.org/10.1016/j.sysarc.2019.101666

[6] Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Efficient multi- receiver identity-based encryption and its application to broadcast encryption. In International Workshop on Public Key Cryptography, pages 380 - 397. Springer, 2005. DOI: https://doi.org/10.1007/978-3-540-30580-4_26

[7] Sanjit Chatterjee and Palash Sarkar. Multi-receiver identity-based key encapsulation with shortened ciphertext. In International Conference on Cryptology in India, pages 394 - 408. Springer, 2006. DOI: https://doi.org/10.1007/11941378_28

[8] Pandi Vijayakumar, Sundan Bose, Arputharaj Kannan, and L Jegatha Deborah. Computation and communication efficient key distribution protocol for secure multicast communication. KSII Transactions on Internet and Information Systems (TIIS), 7(4):878 - 894, 2013. DOI: https://doi.org/10.3837/tiis.2013.04.016

[9] Intae Kim and SeongOun Hwang. An optimal identity-based broadcast encryption scheme for wireless sensor networks. IEICE transactions on communications, 96(3):891 - 895, 2013. DOI: https://doi.org/10.1587/transcom.E96.B.891

[10] Jongkil Kim, Willy Susilo, Man Ho Au, and Jennifer Seberry. Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. IEEE Transactions on Information Forensics and Security, 10(3):679 - 693, 2015. DOI:

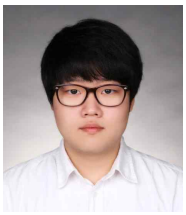
www.kci.go.kr

https://doi.org/10.1109/TIFS.2014.2388156
[11] Fu-Cai Zhou, Mu-Qing Lin, Yang Zhou, and Yu-Xi Li. Efficient anonymous broadcast encryption with adaptive security. KSII Transactions on Internet and Information Systems (TIIS), 9(11):4680 - 4700, 2015. DOI: https://doi.org/10.3837/tiis.2015.11.024
[12] Jiguo Li, Qihong Yu, and Yichen Zhang. Identity-based broadcast encryption with continuous leakage resilience. Information Sciences, 429:177 - 193, 2018. DOI: https://doi.org/10.1016/j.ins.2017.11.008
[13] Jianchang Lai, Yi Mu, Fuchun Guo, Peng Jiang, and Sha Ma. Identity-based broadcast encryption for inner products. The Computer Journal, 61(8):1240 - 1251, 2018. DOI: https://doi.org/10.1093/comjnl/bxy062
[14] Chu, Cheng-Kang, et al., "Conditional proxy broadcast re-encryption", Australasian conference on information security and privacy. Springer, Berlin, Heidelberg, 2009. DOI: https://doi.org/10.1007/978-3-642-02620-1_23

저 자 소 개

김원빈(Won-Bin Kim)

2015.2 순천향대학교 소프트웨어공학과 졸업
2017.2 순천향대학교 컴퓨터학과 석사
2022.2 순천향대학교 소프트웨어융합학과 박사
2022.1-현재 : 엘에스웨어 소프트웨어연구소 연구개발본부 팀장(수석연구원)
<주관심분야> 암호프로토콜, 암호학, 클라우드 보안, 프록시 재암호화, 암호데이터 중복제거



박경엽(Kyung-Yeob Park)

2019.2 서울과학기술대학교 컴퓨터공학과 석사
2019-현재 : 엘에스웨어(주) 선임
<주관심분야> IoT 보안, 블록체인, 빅데이터, 메타버스

조용준(YongJoon Joe)

2011.3 큐슈대학교 전기정보공학과 졸업
2013.3 큐슈대학교 정보학부 석사
2016.3 큐슈대학교 정보학부 박사과정 수료
2013.4-2016.3 일본 학술진흥원 특별연구원
2016.4-현재 : 엘에스웨어 이사
<주관심분야> 병렬·분산 컴퓨팅, 게임이론, 분산 제약 최적화 문제

신동명(Dong-Myung Shin)

2003.2 대전대학교 컴퓨터공학과 박사
2001-2006 한국정보보호진흥원 응용기술팀 선임연구원
2006-2014 한국저작권위원회 저작권기술팀 팀장
2014-2016 한국스마트그리드사업단 보안인증팀 팀장
2016-현재 엘에스웨어(주) 소프트웨어연구소 연구소장/상무이사
<주관심분야> 오픈소스 라이선스, 저작권기술, 시스템/네트워크보안, SW취약점분석·감정, 블록체인 기술, 홀로그램

www.kci.go.kr