논문 2023-3-5 http://dx.doi.org/10.29056/jsav.2023.09.05

메타버스 환경에서 사용되는 디지털 에셋의 n차 창작물 유사도 판별을 위한 데이터 중복성 판별 기술

김원빈*, 노창현*, 조용준*, 신동명*†

Data redundancy determination technology to determine the similarity of n-th creations of digital assets used in the metaverse environment

Won-Bin Kim*, ChangHyun Roh*, YongJoon Joe*, Dong-Myung Shin*†

요 약

최근 메타버스 환경이 빠르게 확산됨에 따라 메타버스 환경의 특징을 활용하여 가상세계에서 공연을 수행하는 사례가 증가하고 있다. 이렇게 가상세계에서 수행하는 공연을 가상공연이라 부른다. 가상공연은 현실세계의 공간에 제약받지 않고도 어디에서든 참여가 가능하기 때문에 공간에 제약을 받는 감염병 팬데믹, 물리적 거리로 인해 참여할 수 없는 해외 콘서트 등을 대체할 수 있는 수단으로 여겨지고 있다. 이러한 가상공연은 디지털 에셋이라고 부르는 여러 디지털 요소를 복합적으로 사용하여 하나의 콘텐츠를 구성한다. 따라서 디지털 데이터의 특징인 복제 및 재사용의 용이성을 그대로 활용할 수 있다. 하지만 이러한 특징을 악용하여 무단 복제, 재사용, 변형하는 등의 저작권을 침해하는 사례가 증가하고 있다. 본 연구에서는 이러한 문제를 해결하기 위해 디지털 데이터의 중복성 판별 및 유사도 판별기술을 제안한다. 이 기술은 저작자가 디지털 에셋 마켓에 새로운 디지털 에셋을 등록하려 할 때, 기존에 등록된 디지털 에셋과 동일한 데이터인지, 더 나아가서는 일부 변형된 데이터인지를 판별하는 기술이다. 이를 통해 본 연구에서는 디지털 에셋 데이터를 블록화하여 여러 조각으로 나누고, 해당 블록이 기존에 등록된 디지털 에셋과의 일치 여부를 분석하는 식으로 디지털 에셋의 중복성 및 유사도 판단을 수행한다. 이를 통해 권리 침해자에 의해 무단으로 복제 및 변형된 디지털 에셋이 무단으로 등록되는 것을 사전에 차단할 수 있다.

Abstract

In recent times, with the rapid proliferation of the metaverse environment, there has been a notable upswing in instances of performance within virtual realms, capitalizing on the inherent characteristics of this environment. These performances, conducted within virtual settings, are commonly referred to as virtual performances. The distinctive advantage of these virtual performances lies in their unrestricted accessibility, transcending the spatial confines of the physical world. As such, they are emerging as a viable substitution for overseas concerts that might be impeded by spatial constraints brought about by infectious disease pandemics or geographical remoteness. These virtual performances integrate a myriad of digital components, termed digital assets, to coalesce into a singular content. Consequently, the inherent trait of digital data, characterized by its ease of duplication and reuse, can be directly leveraged. Nevertheless, there is a concurrent rise in instances of copyright infringement, stemming from the unauthorized replication, reuse, and manipulation of these features. In this study, we propose technologies centered around redundancy and similarity determination for digital data, aiming to address these issues. This technology is employed to ascertain whether a given dataset corresponds to a previously registered digital asset or if it has undergone partial modifications when an author endeavors to register a new digital asset within the digital asset market. Through this, this study blocks digital asset data, divides it into several pieces, and determines the redundancy and similarity of digital assets by analyzing whether the blocks match existing registered digital assets. Through this, it is possible to prevent unauthorized registration of digital assets that have been copied or modified by rights infringers in advance.

한글키워드 : 메타버스, 가상공연, 디지털 에셋, 데이터 중복성 판별, n차 창작물
keywords : Metaverse, Virtual Performance, Digital Assets, Data Redundancy Determination, n-th Creation

* 엘에스웨어(주) 소프트웨어연구소 연구개발본부
† 교신저자: 신동명(email: roland@lsware.com)
접수일자: 2023.08.31. 심사완료: 2023.09.09.
게재확정: 2023.09.20.

1. 서 론

메타버스 환경은 초월을 의미하는 메타(meta)와 세계를 의미하는 버스(verse)의 합성어이며, 그 이름대로 현실 세계를 초월하는 또 다른 세계를 의미한다[1][2]. 일반적으로 메타버스라는 환경은 디지털 데이터로 이루어진 가상의 컴퓨팅 환경을 지칭한다. 이러한 메타버스 환경은 1990년대부터 등장하기 시작한 온라인 게임에 그 근간을 두고 있으며, 게임 제작 기술이 발달함에 따라 다양한 형태로 진화해왔다.

최근 공간적 제약에서 자유로운 메타버스의 특징을 이용하여 가상환경에서 공연하는 사례가 나타나고 있다. 이러한 공연을 가상공연(Virtual Performance)이라 부르며, 디지털 의상, 배경, 음악, 아바타, 효과 등을 이용하여 하나의 공연을 완성한다[3]. 따라서 적절한 요소의 선별과 사용은 공연의 질을 결정하는 매우 중요하다. 하지만 공연 제작자가 자신의 공연에 사용되는 모든 디지털 의상, 배경, 음악, 아바타, 효과 등을 제작하기는 현실적으로 불가능에 가깝다. 그렇기에 공연 제작자는 디지털 의상, 배경, 음악, 아바타, 효과 등 제작자들과 이용허락 계약을 통해 사용 권리를 획득하고, 이를 공연에 사용하게 된다. 따라서 하나에 공연에는 다양한 저작권이 복합적으로 이용될 수밖에 없으며, 이용허락 계약에 따라 동일한 공연을 반복적으로 실연할 수 없는 경우도 발생한다.

디지털 에셋은 디지털 콘텐츠에 사용하기 위해 디지털 데이터로 제작된 의상, 배경, 음악, 아바타, 효과 등을 의미한다. 디지털 에셋은 디지털 데이터로 이루어졌기 때문에 디지털 저작물 범주에 포함된다. 하지만 디지털 데이터의 특성상 복제와 변형이 용이하며, 재창작과 현실세계와의 연계성 여부 등 복잡한 관계를 가진다. 그럼에도 불구하고 디지털 저작권의 잘못된 해석이나 디지털 데이터의 특징을 악용하여 무단으로 복제, 재사용, 변형을 통한 새로운 저작물로서 저작권을 행사하는 사례도 빈번히 발생되고 있다. 이러한 문제를 해결하기 위해서는 최소한 새롭게 등록되는 디지털 에셋 저작물이 기존에 등록된 저작물과 중복되는지 여부와 유사도 비교를 통해 일부 변형된 저작물인지를 판단하는 장치가 요구된다.

본 연구에서는 이러한 문제를 해결하기 위해 디지털 데이터의 중복성 판별 기술을 통해 디지털 에셋의 유사도를 비교하며, 더 나아가 원본 데이터의 n차 변형 여부를 추적할 수 있는 방법을 제안한다. 이를 위해 본 논문의 2장에서는 데이터의 중복성 판별에 대한 관련연구를 살펴본다. 3장에서는 본 제안방식의 시스템을 설계한다. 4장에서는 n차 창작 유사도 판별을 위한 데이터 중복성 판별 기술을 제시하고, 5장에서는 제시한 기술의 분석을 진행한다. 그리고 6장에서는 결론으로 마무리한다.

2. 관련 연구

2.1 데이터 중복성 판단 기술

데이터 중복성 판단 기술은 동일한 데이터가 이미 존재하는지 여부를 판단하는 기술이다. 따라서 두 데이터의 동일성 여부를 판단하는 것이 이 기술의 핵심이다. 데이터의 동일성 여부를 판단하는 방법은 다양한 방식이 이용될 수 있다.

먼저, 그림 1과 같이 두 데이터를 하나의 파일로 두고 비교를 수행하는 방법이 이용될 수 있다. 이 방법은 속도는 매우 빠르지만 두 데이터 중 한 bit라도 다를 경우 서로 다른 데이터라는 결과가 출력된다. 따라서 속도는 빠르나 정확도는 낮은 방식이다.

반면, 그림 2와 같이 데이터를 블록 단위로 나누어서 각 블록 단위로 중복성을 판별하는 방법이 이용될 수 있다[4]. 이 방법은 블록의 수 만큼 비

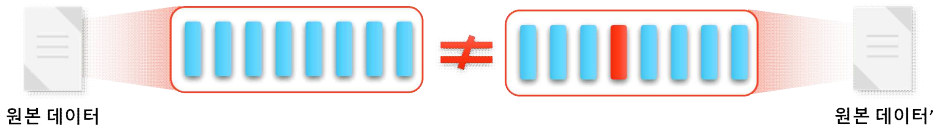

그림 1. 파일 단위 데이터 중복성 판별 방법
Fig 1. Method of file-level data duplication determination

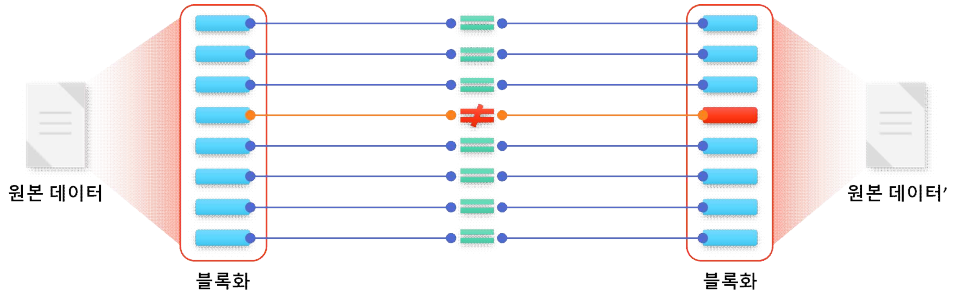

그림 2. 블록 단위 데이터 중복성 판별 방법
Fig 2. Method of block-level data duplication determination

교 횟수가 증가하기 때문에 판단 시간은 비교적 길지만 파일 단위 비교 방법보다 정확도가 월등히 높다. 따라서 목적에 따른 적절한 선택이 필요하다.

2.2. 일방향 해시 알고리즘

일방향 해시 알고리즘은 데이터를 변형시켜 원본으로 복구할 수 없도록 하는 동시에 데이터의 크기를 줄이는 기술이다. 따라서 데이터를 해시화할 경우 원본 데이터에 비해 매우 작은 크기의 데이터로 압축되고, 원본으로 복구할 수 없기 때문에 암호학적인 요소를 포함하고 있다. 이러한 해시 알고리즘의 특징을 활용하여 비교할 데이터를 변환하고 크기를 줄일 수 있다. 또한, 해시 알고리즘에 따라 충돌 저항성을 높일 수도 있으며 솔트(salt) 값을 추가할 수도 있다. 일반적으로 해시 알고리즘은 SHA-256, 512 또는 SHA-3가 이용되며, 가끔 드물게는 universal hashing 기법이 이용되기도 한다.

2.3. Convergent Encryption(CE)

CE는 암호화된 데이터의 중복성 비교를 가능하도록 만드는 기술이다[5][6]. 일반적으로 데이터의 중복성 비교를 수행할 때에는 데이터의 원본을 직접 비교하는 방식이 이용될 수 있다. 하지만 이러한 방식을 이용할 경우, 민감한 데이터의 비교 시 원본이 노출된다. 이는 디지털 데이터의 특성상 데이터 원본의 노출 시 즉각적으로 복제가 이루어지기 때문에 민감한 데이터의 유출로 이어지게 된다. 따라서 일반적으로 공개되어도 되는 데이터가 아닌, 허가된 대상에게만 제한되거나 공개되지 않아야 하는 데이터의 경우 원본을 알지 못하게 하

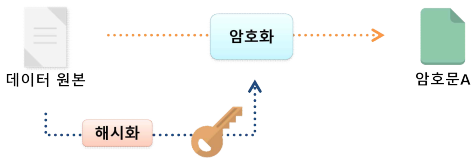

그림 3. Convergent Encryption의 개요
Fig 3. Overview of Convergent Encryption

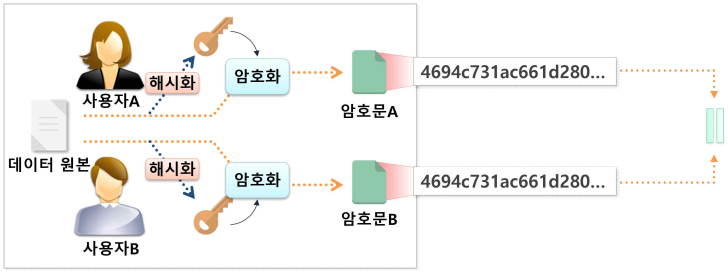

그림 4. Convergent Encryption 수행 시 데이터 중복성 비교 예시
Fig 4. Example of data redundancy determination with Convergent Encryption

는 동시에 데이터의 중복성 비교를 수행해야 한다. 따라서 이러한 조건을 충족시킬 수 있도록 하는 것이 CE이며, CE를 사용할 경우, 데이터 원본이 노출되지 않도록 암호화를 수행하는 동시에 데이터의 중복성 여부를 비교할 수 있다. CE의 기본적인 동작 방식은 그림 3과 같다. 그림 3에서 데이터 원본을 해시화하여 암호화 키를 생성하고, 생성된 암호화 키를 이용하여 데이터를 암호화하는 방법을 이용한다. CE를 기반으로 데이터를 암호화 할 때, 동일한 데이터 원본을 입력할 경우 동일한 암호문 출력이 이루어지기 때문에 데이터 중복성 판단이 가능해지며, 이 과정은 그림 4와 같다.

2.4 MLE(Message-Locked Encryption)

Message Locked Encryption(MLE)은 CE를 기반으로 2013년 Bellare 등에 의해 제안된 데이터 암호화 기술이다[7][8]. 이 기술은 동일한 데이터 원본에서 동일한 암호화된 데이터를 생성하기 위한 방법을 제시하였다. MLE의 일반적인 접근법은 데이터 원본 M을 이용하여 K←H(M)을 계산하고, K를 키로 사용하여 C←E_K(M)을 생성하는 방법을 이용한다. MLE에는 총 4가지의 암호화 기술이 포함되며 이는 각각 Convergence Encryption(CE), Hash and CE without Tag Check (HCE1), Hash and CE with Tag Check (HCE2), and Randomized Convergent Encryption (RCE)이다. CE와 HCE1은 오로지 데이터의 암호화, 복호화만을 수행한다. HCE2는 태그를 이용한 무결성 검증과 함께 암호화 및 복호화를 수행한다. RCE는 HCE2를 기반으로 하며, 키 생성 과정에서 One Time Pad를 이용한 무작위 키를 생성하여 암호화를 수행하고, 무작위 키를 K로 암호화하는 과정을 갖는다. 이로인해 RCE는 키 생성 엔트로피가 향상되는 장점을 갖는다. 따라서 MLE를 이용할 경우 CE만을 이용할 때 보다 키 생성 엔트로피가 증가하여 데이터의 보안성이 향상되는 효과를 가져다 준다.

2.5 중복성 판단 위치

데이터 중복성 판단을 수행하는 위치에 따라 Client-side 방식과 Server-side 방식으로 구분할 수 있다[9][10].

먼저, Client-side 방식은 사용자가 데이터 원본

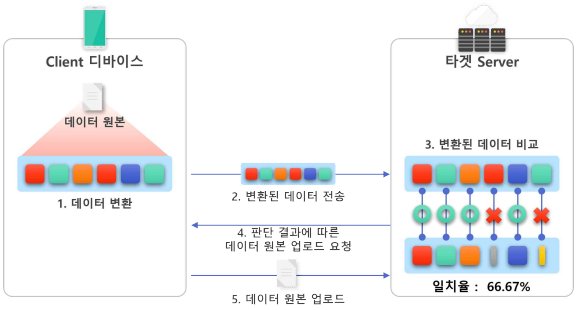

그림 5. Client-side 데이터 중복성 판단 방식
Fig 5. Method of client-side data redundancy determination

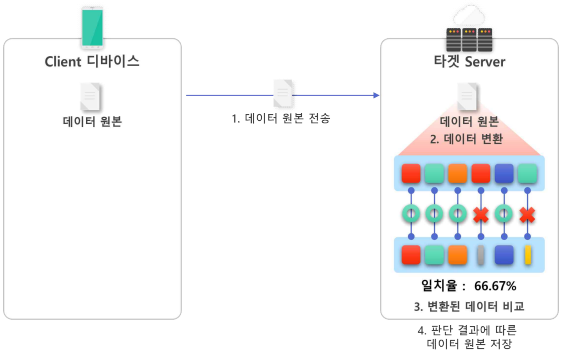

그림 6. Server-side 데이터 중복성 판단 방식
Fig 6. Method of server-side data redundancy determination

을 업로드 하지 않고, 타겟 서버에 동일한 데이터가 이미 존재하는지를 판단하는 기술이다. 이를 위해서는 그림 5와 같이 데이터 원본을 변환하고, 변환된 데이터를 타겟 Server로 업로드하여 서버에서 그 결과만을 비교하는 방식을 이용한다. 이 방식은, 중복되는 데이터가 존재할 경우 전송되는 데이터 크기를 줄일 수 있으며, 데이터 원본 노출을 최소화 할 수 있는 장점을 가지지만, 통신 횟수가 증가하며, Client 디바이스의 컴퓨팅 리소스를 요구한다는 단점이 존재한다.

반면, Server-side 방식은 그림 6와 같이 Client 디바이스에서 별도의 연산 수행하지 않고 타겟 Server에 데이터 원본을 전송하는 방식이다. 따라서 Client 디바이스의 측면에서는 컴퓨팅 비용이 절감되지만, 타겟 Server 입장에서는 컴퓨팅 비용이 증가하는 특징을 갖는다. 또한 데이터 원본을 직접 전송하기 때문에 데이터의 중복성 판단 결과와 관계없이 데이터 원본이 노출될 수 밖에 없다.

3. 시스템 설계

본 장에서는 메타버스 환경의 가상공연에서 디지털 에셋의 저작권 침해를 방지하기 위한 디지털 에셋의 등록 단계에서 중복성 및 n차 창작물 판단을 수행하는 시스템 설계를 수행한다.

3.1 시스템 요구사항

본 시스템을 위한 요구사항 및 분석은 다음과 같다.

- **정확성(Accuracy):** 본 시스템의 최우선 목표이며, 두 개의 비교 데이터가 주어졌을 때 두 데이터가 완전히 일치하거나 일부 변경 여부를 판단할 수 있어야 한다.
- **효율성(Efficiency):** 중복성 판단 과정에서 높은 비교 정확성을 확보하면서도 컴퓨팅 연산, 비교 시간 등의 효율성을 가져야 한다.
- **기밀성(Confidentiality):** 데이터의 중복성을 비교하는 과정에서 데이터 원본을 노출시키지 않고도 데이터의 비교를 수행할 수 있어야 한다.

3.2 시스템 구성

3.1 요구사항 분석을 기반으로 한 시스템의 구성은 그림 7과 같다. 본 시스템은 서버 측에 새로운 디지털 에셋이 업로드 될 경우, 해당 에셋을 시스템에 등록하기 전에 기존에 등록된 디지털 에셋과의 중복성 및 n차 창작물 판단을 수행하도록 구성하였다. 또한 이 과정에서 단순히 두 데이터가 동일한지 여부만을 판단하는 것이 아닌, 데이터의 일치율을 판단하여 n차 창작물 여부를 동시에 판단한다. 이러한 시스템의 구성요소에 대한 상세한 설명은 다음과 같다.

- **타겟 Server:** 사용자들이 업로드한 데이터를 등록 및 보관하고, 메타버스 상에서의 가상공연에 이용할 수 있는 디지털 에셋 마켓 시스템을 제공한다.
- **사용자(공통):** 디지털 에셋을 생성하는 저작자이며, 자신이 생성한 디지털 에셋 데이

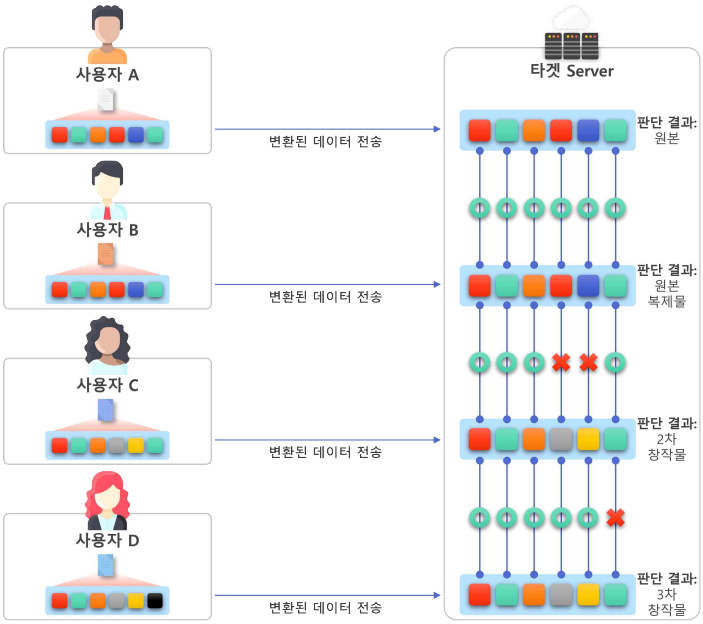

그림 7. 데이터의 중복성 및 n차 창작물 판단 시스템 구성도
Fig 7. Configuration of data redundancy and n-th creation determination system

터를 타겟 Server에 등록 및 업로드하여 타겟 Server와 연계된 메타버스 환경에서 이용할 수 있도록 한다.

- **사용자 A:** 디지털 에셋 원본을 제작하고 타겟 Server에 등록하는 저작자이다. 사용자 A는 디지털 에셋 원본을 직접 제작하고 저작권을 보유한 저작자이다.
- **사용자 B:** 사용자 A가 제작한 디지털 에셋 원본을 무단으로 복제하여 타겟 Server에 등록하려는 권리 침해자이다. 사용자 A의 디지털 에셋 원본을 변형 없이 등록하려 하므로 예외없이 권리 침해자가 된다.
- **사용자 C, D:** 사용자 A가 제작한 디지털 에셋 원본을 변형하여 n차 창작을 수행한 저작자이다. 이 경우, 사용자 A와 n차 창작 이용허락 계약 수행 여부에 따라 정당한 저작권을 인정받을 수도 있다.

4. 제안방식

본 장에서는 3장에서 설계한 디지털 에셋 등록 시스템의 타겟 서버와 저작자의 디바이스에서 동작하는 디지털 에셋의 n차 창작 및 중복성 판단을 위한 방식을 제안한다.

4.1 시스템 파라미터

본 제안방식의 시스템 파라미터는 표 1과 같다.

4.2 데이터 업로드 요청 단계

데이터 업로드 요청 단계에서는 업로드 할 데이터 원본을 블록화하고, 블록의 암호화 키, 태그를 생성한다. 그리고 이를 이용하여 타겟 Server로 중복성 판단을 요청하는 과정을 포함한다.

표 1. 시스템 파라미터
Table 1. System parameters

파라미터	설명
$*$	참여 객체 (u : 사용자, TS : 타겟 Server)
i	전체 블록의 인덱스
j	중복되지 않은 블록의 인덱스 ($j \in i$)
k	중복된 블록의 인덱스($k \in i$)
f	데이터 원본
b_i	데이터 원본의 블록 ($f = b_1, b_2, \dots, b_i$)
sk	사용자의 비밀키
K_i	CE를 통해 생성된 키 암호화 키
L_i	b_i의 암호화 키
T_i	b_i의 태그(블록 식별자)
C_{1_i}	암호화된 b_i
C_{2_i}	암호화된 키 L_i
O_j	L_{j-1}와 L_j의 사이의 연결 데이터
Rq_D	중복된 블록의 암호화 키 목록
Rq_{nD}	중복되지 않은 블록의 목록
$Meta_f$	데이터 원본 f의 중복 및 n차 창작 정보 메타데이터

- ***Step 1.*** 사용자는 데이터 원본을 나누어 블록 $b_i(1 \leqq i \leqq n)$을 생성한다. 그리고 블록을 이용하여 블록 b_i의 암호화 키 $K_i \Leftarrow H(b_i)$와 식별자인 태그 $T_i \Leftarrow H(K_i)$를 각각 생성한다.

- ***Step 2.*** 사용자는 생성된 데이터 블록의 태그 T_i의 리스트를 타겟 Server로 전송한다.

- ***Step 3.*** 타겟 Server는 사용자가 전송한 태그 목록 중 타겟 Server에 존재하지 않는 데이터 블록의 태그 T_j를 Rq_{nD}에 추가한다. 그리고 타겟 Server에 존재하는 데이터 블록의 암호화된 키 데이터 C_{2_k}를 Rq_D에 추가한다.

- ***Step 4.*** 타겟 Server는 중복되지 않은 블록의 목록 Rq_{nD}을 이용하여 데이터의 중복성 여부와 일치율을 확인하고 그 결과를 $Meta_f$에 기록한다.

- ***Step 5.*** 타겟 Server는 사용자에게 중복성 판단 결과에 따라 데이터 원본 업로드를 요청한다.

4.3 데이터 업로드 단계

데이터 업로드 단계에서는 타겟 Server가 전송한 Rq_D, Rq_{nD}에 포함된 목록을 확인하여 이미 보관된 데이터의 암호화 키를 획득한다. 그리고 신규 업로드를 수행하는 데이터의 연결 데이터 O_j와 암호화된 데이터를 생성하여 타겟 Server로 전송하는 과정을 포함한다.

- ***Step 1.*** 사용자는 이전 단계에서 타겟 Server로부터 전송 받은 Rq_D를 확인하여 중복된 데이터의 C_{2_k}를 획득한다. 그리고 $L_k \Leftarrow C_{2_k} \oplus K_k'$를 통해 암호화 키 L_k를 획득한다.

- ***Step 2.*** 사용자는 Rq_{nD}에 포함된 태그 T_j의 암호화 키 L_j를 무작위로 선택한다. 사용자는 전체 데이터 블록 중 타겟 Server에 존재하지 않는 데이터의 암호화 키와 이전, 이후 데이터 블록의 암호화 키를 이용하여 $O_{j_1} \Leftarrow L_{j-1} \oplus L_j$와 $O_{j_2} \Leftarrow L_j \oplus L_{j+1}$을 계산한다.

- ***Step 3.*** 사용자는 $C_{1_j} \Leftarrow E_{L_j}(b_j)$를 통해 암

호문 C_{1_j}를 획득한다. 그리고 $C_{2_j} \Leftarrow L_j \oplus K_j$를 통해 암호화된 키 C_{2_j}를 획득한다.

- ***Step 4.*** 사용자는 생성된 O_{j_1}, O_{j_2}의 리스트, C_{1_j}, C_{2_j}의 리스트를 타겟 Server로 전송한다.

- ***Step 5.*** 타겟 Server는 C_{1_j}를 스토리지 서버에 저장하고, 타겟 Server에 $C_{1_{j-1}} \rightarrow C_{1_j} \rightarrow C_{1_{j+1}}$을 연결하는 데이터 O_{j_1}, O_{j_2}와 암호화된 키 데이터 C_{2_j}를 저장하여 업로드 단계를 마친다.

5. 제안방식 분석

본 장에서는 3장에서 제시한 시스템 요구사항을 기준으로 4장에서 제안한 방식을 분석한다.

- **정확성(Accuracy):** 본 제안방식에서는 데이터 중복성 비교의 정확성을 향상시키기 위해 블록 단위의 데이터 비교 방식을 이용하였다. 이 방식은 파일 단위 비교에 비해 속도가 느릴 수 밖에 없으나, 데이터 블록의 크기 설정에 따라 KB(Kilo Bytes) 단위 이하의 유사도 까지도 분석이 가능하다. 따라서 이미지와 같은 형태의 디지털 데이터를 가시도 훼손 없이 일부 bit를 변경할 경우 파일 단위의 데이터 비교 방식에서는 다른 파일로 인식된다. 하지만 블록 단위의 데이터 비교 방식의 경우에는 해당 블록을 제외한 나머지 블록이 일치하게 되므로 유사도 판단이 가능해진다. 이를 통해 본 제안방식은 중복성, 유사도를 높은 정확도로 비교할 수 있다.

- **효율성(Efficiency):** 본 제안방식은 중복성 및 유사도 비교 효율을 극대화 하기 위해 비교하는 데이터의 크기를 축소하고, Client 디바이스보다 높은 성능의 자원을 가지고 있는 타겟 Server 상에서 탐색 및 비교를 수행한다. 또한 이 과정에서 중복된 데이터라 판단될 경우 데이터 원본의 업로드 과정을 생략하여 데이터 전송 트래픽량을 감소시킬 수 있도록 하였다.

- **기밀성(Confidentiality):** 본 제안방식은 데이터의 중복성 및 유사도 비교 과정에서 데이터의 원본이 노출되지 않도록 설계하였다. 일반적인 데이터 암호화 기술은 데이터 원본을 변형시키기 때문에 동일한 데이터라도 암호화를 수행하는 사용자에 따라 출력물이 달라 데이터의 비교가 불가능하다. 따라서 이러한 문제를 해결하기 위해 본 제안방식에서는 CE와 MLE를 이용하여 데이터 암호화를 수행하였다. 이를 통해 본 제안방식은 암호화된 데이터의 비교가 가능하게 되었으며, 이를 통해 데이터의 중복성, 유사도 비교 과정에서 데이터 원본 노출을 최소화 할 수 있게 되었다.

6. 결 론

최근 감염병 팬데믹 등 현실 세계의 공간에서 수행되던 다양한 활동이 제약됨에 따라 현실 세계의 공간을 대체 또는 보완하기 위한 연구가 수행되고 있다. 메타버스 환경은 이러한 연구의 결과 중 하나이며, 현실세계와 물리적인 영향을 주지 않으면서도 현실세계의 활동을 이어서 수행할 수 있는 장점을 가지고 있다. 가상공연은 이와 같은 메타버스의 특징을 이용하여 가상환경에서 수행

되는 공연을 일컫는다. 가상공연은 현실세계의 공연이 가지는 가장 큰 제약인 물리적인 공간 문제를 해소할 수 있기 때문에 공간의 제약 없이 공연을 수행할 수 있다. 또한 가상공연은 디지털 데이터로 구성되기 때문에 반복하여 재실연하기에도 매우 용이하다.

가상공연은 앞에서 설명한 것과 같이 디지털 환경에서 수행되는 활동이기 때문에 디지털 의상, 배경, 음악, 아바타, 효과 등 다양한 디지털 에셋이 복합적으로 사용된다. 디지털 에셋은 디지털 데이터이므로 복제와 재생산이 매우 용이하기 때문에 반복된 공연 또는 파생 공연에도 이용될 수 있다. 하지만 이러한 특징을 악용하여 디지털 에셋을 무단으로 복제, 변형, 재사용하는 사례가 발생하고 있다. 이는 해당 에셋의 저작권을 침해하는 행위이며, 해당 저작물을 소유한 저작권자에게 직접적인 피해를 발생시킨다. 본 연구에서는 이러한 문제를 해결하기 위해 디지털 에셋을 등록하고 관리하는 마켓 서버에 무단으로 복제되고 변형된 디지털 에셋이 등록되지 못하도록 하는 연구를 수행하였다. 만약 마켓 서버에 새로운 디지털 에셋의 등록 요청이 발생할 경우 디지털 데이터의 중복성 및 유사도 비교를 수행하여 원본이 이미 존재하는지를 파악한다. 또한 정확히 일치하는 원본뿐만 아니라 일부 일치하는 유사도 판단을 통해 원본 데이터에서 일부 변형된 2차 창작물인지 여부를 판단할 수 있도록 하였다. 하지만 본 연구의 제안방식의 설계상 한계로 인해 n차 창작의 경우 유사도 분석을 위한 연산량과 n차 창작물의 n차 창작 등과 같이 n^n차 창작물의 파생 depth가 증가함에 따른 엔트로피의 증가에 대한 한계가 존재한다. 따라서 후속 연구에서는 이와 같은 문제를 해결하기 위한 연구를 수행할 계획이다. 결과적으로 본 연구를 통해 점차 확산되어가는 메타버스 환경에서 저작권 침해없는 가상공연에 기여할 수 있을 것으로 기대한다.

본 연구는 문화체육관광부 및
한국콘텐츠진흥원의 2023년도 문화기술
연구개발 사업으로 수행되었음
(과제명 : 대규모 가상공연 플랫폼을 지원하는
블록체인 기반 저작물 보호 및 활용 기술
개발, 과제번호 : R2022020057, 기여율 : 100%)

참 고 문 헌

[1] Mystakidis, Stylianos. "Metaverse." Encyclopedia 2.1 (2022): 486-497. DOI: https://doi.org/10.3390/encyclopedia2010031

[2] Sparkes, Matthew. "What is a metaverse." (2021): 18. DOI: https://doi.org/10.1016/S0262-4079(21)01450-0

[3] Baía Reis, António, and Mark Ashmore. "From video streaming to virtual reality worlds: an academic, reflective, and creative study on live theatre and performance in the metaverse." International Journal of Performance Arts and Digital Media 18.1 (2022): 7-28. DOI: https://doi.org/10.1080/14794713.2021.2024398

[4] Puzio, Pasquale, et al. "Block-level de-duplication with encrypted data." Open Journal of Cloud Computing (OJCC), Vol. 1, No. 1 pp. 10-18, 2014. DOI: https://www.ronpub.com/ojcc/OJCC-v1i1n02_Puzio.html

[5] Kim, K., Chang, K. Y., & Kim, I. K. (2018). Deduplication technologies over encrypted data. Electronics and Telecommunications Trends, 33(1), 68-77. DOI:https://doi.org/10.22648/ETRI.2018.J.330107

[6] Storer, Mark W., et al. "Secure data deduplication." Proceedings of the 4th ACM international workshop on Storage security and survivability. ACM, 2008. DOI: https://doi.org/10.1145/1456469.1456471

[7] M. Bellare, et al. "Message-locked encryption and secure deduplication." Annual

international conference on the theory and applications of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. DOI: https://link.springer.com/chapter/10.1007/978-3-642-38348-9_18

[8] M. Bellare, et al. "DupLESS: server-aided encryption for deduplicated storage." Presented as part of the 22nd USENIX Security Symposium, 2013. DOI:https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/bellare

[9] Xu, Jia, Ee-Chien Chang, and Jianying Zhou. "Weak leakage-resilient client-side deduplication of encrypted data in cloud storage." Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. 2013. DOI: https://doi.org/10.1145/2484313.2484340

[10] Kaaniche, Nesrine, and Maryline Laurent. "A secure client side deduplication scheme in cloud storage environments." 2014 6th International Conference on New Technologies, Mobility and Security (NTMS). IEEE, 2014. DOI: https://doi.org/10.1109/NTMS.2014.6814002

저 자 소 개

김원빈(Won-Bin Kim)

2015.2 순천향대학교 소프트웨어공학과 학사
2017.2 순천향대학교 컴퓨터학과 석사
2022.2 순천향대학교 소프트웨어융합학과 박사
2022.1-현재 엘에스웨어 소프트웨어연구소 연구개발본부 팀장(수석연구원)
<주관심분야> 저작권 보호, 디지털 홀로그래픽 프린팅 보안, 암호프로토콜, 암호학, 클라우드 보안, 프록시 재암호화, 암호데이터 중복제거, 오픈소스 라이선스 보안

노창현(ChangHyun Roh)

2017.8 순천향대학교 소프트웨어공학과 졸업
2020.2 순천향대학교 컴퓨터학과 석사
2022.2-현재 가천대학교 정보보호학과 박사과정
2022.12-현재 엘에스웨어 소프트웨어연구소 연구개발본부 수석연구원
<주관심분야> 정보보호, CPS 보안, 블록체인, DID, NFT, 저작권 기술, 메타버스, 디지털휴먼

조용준(YongJoon Joe)

2011.3 큐슈대학교 전기정보공학과 학사
2013.3 큐슈대학교 정보학부 석사
2016.3 큐슈대학교 정보학부 박사 수료
2013.4-2016.3 일본학술진흥원 특별연구원
2016.4-현재 엘에스웨어㈜ 기술이사
<주관심분야> 오픈소스, 저작권, 병렬·분산 컴퓨팅, 게임이론, 분산 제약 최적화 문제

신동명(Dong-Myung Shin)

2003.8 대전대학교 컴퓨터공학과 박사
2001-2006 한국정보보호진흥원(KISA) 응용기술팀 선임연구원
2006-2014 한국저작권위원회 저작권기술팀 팀장
2014-2016 한국스마트그리드사업단 보안인증팀 팀장
2016-현재 엘에스웨어㈜ 연구소장/상무
<주관심분야> 오픈소스 라이선스, 저작권기술, 시스템/네트워크보안, SW취약점분석, SW감정, 블록체인 기술, 홀로그램