웹 채팅 환경에서 시그니처 각인을 활용한 파일 송수신 이력 관리 서비스

김다연[1], 이보배[2], 박태준[3]
[1]전남대학교 물리학과 학부생
[2]전남대학교 자율전공학부 학부생
[3]전남대학교 소프트웨어공학과 교수
210941@jnu.ac.kr, 202780@jnu.ac.kr, taejune.park@jnu.ac.kr

A File Transmission History Management Service Using Signature Engraving in a Web Chat Environment

Da-Yeon Kim[1], Bo-Bae Lee[2], Taejune Park[3]
[1]Dept. of Physics, Chonnam National University
[2]Dept. of Faculty of Interdisciplinary Studies, Chonnam National University
[3]Dept. of Sofeware Engineering, Chonnam National University

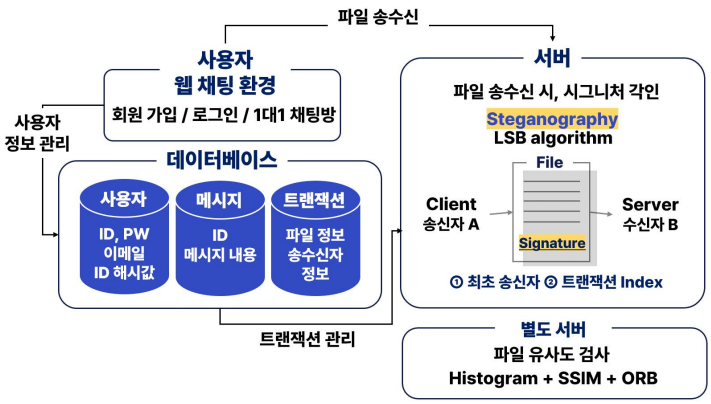
요 약

최근 채팅 서비스에서 파일 공유의 증가와 함께 디지털 콘텐츠의 무단 공유 사례가 급증하고 있다. 기존 채팅 서비스에서는 무단 공유 발생 시 모든 트랜잭션 이력을 확인해야 하며, 이는 상당한 시간이 소요되는 문제점이 존재한다. 본 논문에서는 시그니처 각인을 활용하여 파일 송수신 이력을 효율적으로 관리하고, 웹 채팅 서비스 내에서 신뢰할 수 있는 파일 공유 서비스를 제안한다. 제안된 서비스에서는 채팅방에서 공유된 파일에 송신자의 시그니처 정보를 포함하여 전송함으로써, 데이터베이스에서 해당 파일의 트랜잭션 이력을 신속하게 확인할 수 있고, 이를 통해 책임자를 명확히 식별할 수 있다. 시그니처가 각인된 파일은 원본과 외관상 구별이 불가능할 정도로 유사하게 처리되며, 유사도 검사 기능을 통해 파일 수정 시 시그니처 손실을 방지하고 트랜잭션의 무결성을 유지하여 경로 훼손을 방지한다. 본 논문에서 제안하는 서비스는 디지털 콘텐츠의 안전한 공유와 저작권 보호를 목표로 하며, 학습 자료나 창작물의 무단 배포로 인한 법적 분쟁과 경제적 손실을 줄일 수 있다. 또한, 파일 유포의 책임자를 명확히 하여 범죄 수사에 기여할 수 있을 것으로 기대된다.

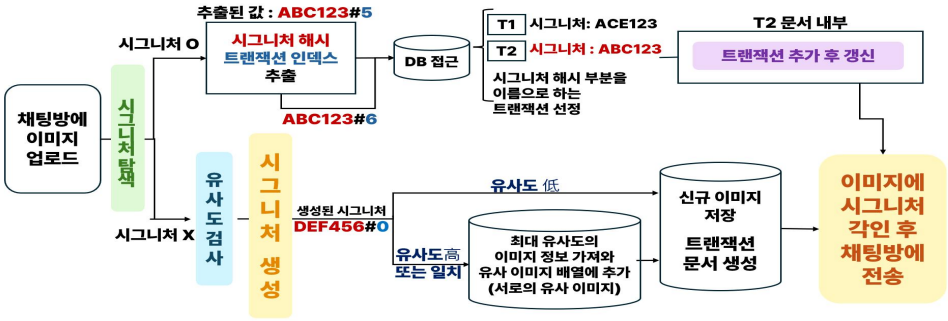
1. 서론

디지털 커뮤니케이션이 활발해짐에 따라 채팅 서비스에서 이미지와 문서 공유의 편의성이 크게 향상되었다[1]. 그러나 다양한 파일이 자유롭게 공유되면서 디지털 콘텐츠의 무단 복제 및 배포 사례도 급증하고 있다. 일반 사용자는 채팅 서비스에서 파일을 전송하거나 공유할 때, 해당 파일이 저작권 문제를 일으킬 가능성을 미리 인지하기 어렵고, 자신이 제작한 콘텐츠가 불법적으로 복제되어 유포되었는지 확인하는 것도 쉽지 않다[2][3]. 이러한 문제는 특히 민감한 정보를 주고받는 경우 더 큰 위험을 초래하며, 현재의 대부분의 채팅 서비스는 파일 식별 및 이력 추적 시스템이 부족하여 이러한 상황에 대한 효과적인 대응이 어렵다.

따라서 본 논문에서는 웹 채팅 서비스에서 시그니처 각인을 활용한 파일 송수신 이력 관리 서비스를 제안한다. 제안한 시스템은 송신자의 시그니처를 파일에 각인하고, 이를 통해 파일의 원출처를 신속하게 식별하며 배포 경로를 추적할 수 있는 방법을 제시한다. 이를 통해 채팅 서비스에서 파일 공유의 안전성을 확보하고, 파일 송수신 이력의 무결성을 보장하여 창작물 무단 공유 및 법적 분쟁에 대한 해결책을 제공할 수 있을 것으로 기대된다.



(그림 1) 전체 시스템 구조



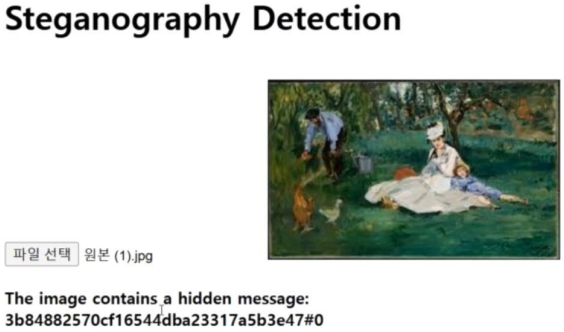
(그림 2) 시그니처 각인 모듈

2. 설계 목표 및 내용

본 논문의 목표는 시그니처 각인을 통한 파일 송수신 이력 관리와 신뢰할 수 있는 파일 공유 환경을 제공하는 채팅 서비스의 구현이다. 이를 위해, 채팅방에서 공유되는 파일에 송신자의 시그니처 정보를 각인하고 해당 트랜잭션을 관리하는 서비스 구조를 (그림 1)과 같이 설계하였다.

2.1. 시그니처 각인 모듈

시그니처는 최소 송신자의 UID와 타임스탬프 값을 salt 값으로 추가하여 해시화하고, 트랜잭션 index를 삽입한 값이다. 파일에 시그니처가 각인되면 육안으로 볼 때 원본과 거의 차이가 없도록 처리되며, 이러한 방법을 통해 무단으로 공유되는 파일을 방지할 수 있다.



(그림 3) 시그니처 각인 결과

2.2. 유사도 검사 모듈

파일이 수정되거나 변형된 경우를 대비해 유사도 검사 기능을 도입하여 시그니처 손실을 방지한다. 이를 통해 파일의 트랜잭션 경로가 훼손되지 않도록 하여, 파일의 무결성을 유지한다.

2.3. 트랜잭션 관리 데이터베이스 모듈

제안한 서비스는 별도의 트랜잭션 관리 데이터베이스를 구축하여 파일의 송수신 이력을 기록하고 관리한다. 이를 통해 원출처를 확인하고 배포 경로를 추적함으로써 무단 복제 및 공유를 방지할 수 있다.

2.4. 추적 시스템 모듈

(그림 2)의 과정으로 데이터베이스에 기록된 트랜잭션을 바탕으로 파일의 배포 경로를 추적하는 시스템을 구현하였다. 파일을 디코딩하여 시그니처를 추출하고, 이를 데이터베이스에서 검색하여 파일의 유포 경로를 파악한다. 또한 유사 이미지 배열을 이용해 수정된 이미지의 경로도 추적 가능하다.

3. 결론 및 향후 연구

본 논문은 웹 채팅 환경에서 시그니처 각인을 활용한 파일 송수신 이력 관리 서비스를 제안하였다. 향후 연구는 웹 채팅 서비스를 넘어 모바일 애플리케이션이나 소셜 네트워크 서비스 등 다양한 플랫폼에 시그니처 생성 및 삽입 모듈의 이식을 목표로 한다. 이를 위해 기존 서비스의 데이터베이스를 수정하는 대신, 별도의 새로운 데이터베이스를 구축하여 통신 프로토콜로 시그니처 생성에 필요한 정보만 주고받는 API를 개발할 예정이다.

감사의 글

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 소프트웨어중심대학사업의 연구결과로 수행되었습니다.(2021-0-01409)

참고문헌

[1] The Knowledge Academy. “Digital Communication: Definition, Examples and its Types.” 2024. http://theknowledgeacademy.com

[2] Shinydocs. “10 Common Problems in File Sharing and How to Solve Them.”, https://shinydocs.com/blog/10-common-problems-in-file-sharing-and-how-to-solve-them/

[3] Y.Y Kim and S.S. Shin. “A Study on Multi-Media Contents Security Using Android Phone for Safety Distribution,” Journal of Digital Convergence, 10(6), pp. 231-239, Jan. 2012.