제20회 한국정보처리학회 추계학술발표대회 논문집 제10권 제2호 (2003. 11)

워터마킹 기술을 활용한 멀티미디어 전자화폐 기술에 관한 연구

이정수*, 김종원*
*㈜ 마크애니 부설 연구소
e-mail : jslee@markany.com, jwkim@markany.com

A Study on Technology for Multimedia E-Money based on Watermarking Technique

Jung-Soo Lee*, Jong-Weon Kim*
*MarkAny Research Institute

요 약

시스템은 자발성, 자율성, 사회성, 반응성을 갖는 독립된 프로그램인 에이전트를 조합하여 구성되는 시스템으로, 일반 사용자에게 편리하고 자연스러운 메타포를 제공한다. 그러나, 개발자 측면에서는 에이전트 시스템에서 요구하는 각종 기능 및 제약규칙...

1. 서론

전자화폐는 전자적 수단을 사용하는 화폐로 은행계좌를 직접적으로 접근하지 않고 자신이 보유하는 화폐가치로 대금지불이 가능한 기술적인 수단으로써 인터넷상의 거래나 정보서비스를 제공하는 사이버 비즈니스가 증가하고 전자상거래가 급속하게 부상함으로써 그 필요성이 부각되고 있다.

전자화폐는 복사, 위조 등의 부정사용을 막을 수 있어야 하고 많은 데이터를 삽입할 수 있어야 한다.

본 논문에서는 새로운 개념의 전자화폐를 소개하고자 한다. 기존의 전자화폐의 복사, 위조 방지 기능은 물론 사용자의 프라이버시를 보호할 수 있도록 화폐 사용의 익명성을 제공하고 필요에 따라 양도가 가능한 전자화폐로 멀티미디어(이미지, 오디오, 비디오)를 이용하여 화폐의 개념을 부여하고 이를 보급하는 기술이다.

이 기술은 현재 부각되고 있는 워터마킹 기술을 이용한 것으로써 Fragile watermarking 기술을 이용하여 위·변조시 데이터의 활용을 막을 수 있도록 설계하여 전자화폐의 기본적인 위·변조 방지 기술을 제공하고 데이터로써 각 멀티미디어에 미디어 ID 와 비밀번호를 이용함으로써 익명성 및 양도성을 부과할 수 있도록 하였다.

본 논문은 2 절에서 전체시스템의 개요를 설명하고, 3 절에서는 데이터 구조와 워터마킹 기술을 나타낸다. 마지막으로 결론이 4 절에 나타난다.

2. 멀티미디어 전자화폐 시스템 구조

본 논문에서 제안하는 시스템의 전체적인 구조는 다음과 같다.

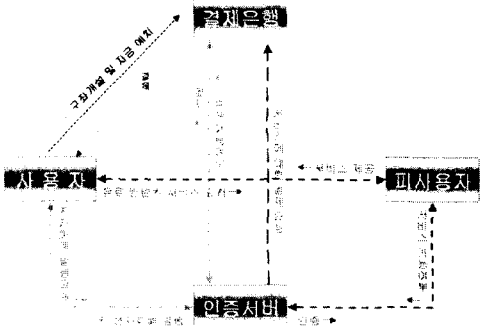

그림 1. 전체 시스템의 개략도

2.1 멀티미디어 전자화폐의 발행 및 거래

사용자는 인증서버를 통해 전자화폐를 발급받을 수 있다. 인증서버는 사용자의 계좌번호를 통해 요청해온 만큼의 전자화폐를 발행한다. 전자화폐는 이미지, 오디오, 비디오 등의 멀티미디어에 워터마크를 삽입하고 인증서버의 데이터 베이스에 멀티미디어에 대한 정보를 기록함으로써 발급된다.

멀티미디어 전자화폐를 사용하기 위해 사용자는 멀티미디어 전자화폐를 저장하거나 온라인으로 쇼핑몰에 접속하여 물건을 구매할 수 있다. 온라인 쇼핑몰에서 구매를 위해 접속한 사용자는 결제과정에서 기존의 전자화폐와 같이 물건을 구매할 수 있다. 그러나 사용자의 익명성을 보장하기 위해 사용자 정보는 물건을 받기 위한 자료이외의 개인정보는 입력할 필요가 없다. 멀티미디어 전자화폐마다 고유한 ID 가 있어서 이 ID 를 이용하여 물건 값을 결제할 수 있다. 결제를 위해 인증서버를 접속하여 사용자가 제시한 멀티미디어 전자화폐의 사용 가능성을 타진하고 사용가능한 전자화폐에 대해서는 결제를 위한 절차를 마친다. 인증서버에서는 결제된 전자화폐에 대해 결제금액만큼의 사용 금액을 차감하고 이를 쇼핑몰의 계좌로 입금시켜준다.

2.2 멀티미디어 전자화폐의 양도

멀티미디어 전자화폐는 위의 기능이외에도 전자화폐를 타인에게 양도할 수 있는 기능을 가지고 있다. 기존의 전자화폐가 양도가 불가능하다라는 단점이 있는 반면 멀티미디어 전자화폐는 익명성에 전제를 두고 있기 때문에 타인에게 양도가 가능하다 물론 양도하는 사람의 부정적인 이용을 막기 위한 장치도 마련되어있다.

멀티미디어 전자화폐를 양도하기 위해서는 단순히 사용자간에 주고 받는 과정이 아니라 인증서버를 통해야 한다. 인증서버를 통해 양도하고자 하는 전자화폐를 입력하면 인증서버에서는 이 전자화폐에 대한 고유 ID 를 삭제하고 새로운 ID 를 발급하여 새로운 사용자에게 E-메일을 통해 전송하게 된다.

2.3 멀티미디어 전자화폐의 익명성

익명성은 멀티미디어 전자화폐의 사용 주체를 알 수 없도록 하여 사용자의 구매, 지불에 대한 프라이버시가 상점이나 은행이 결탁해도 노출되지 않는 것을 의미 한다. 사용자는 최초에 멀티미디어 전자화폐를 구매하기 위해서 은행의 계좌번호 및 개인정보를 인증서버에 보내게 된다. 인증서버에서는 사용자가 입력한 정보를 통해 전자화폐를 발행하게 되고 입력한 사용자 정보를 삭제한다. 즉, 인증서버에는 사용자에 대한 어떤 개인정보도 남아 있지 않고 단지 발행한 멀티미디어 전자화폐에 대한 정보만이 인증서버에 남아 있게 되어 일종의 현금처럼 사용할 수 있게 된다.

멀티미디어 전자화폐는 발행된 전자화폐의 고유 ID 를 기반으로 하고 있기 때문에 익명성을 강조할 수 있다.

3. 데이터 구조와 워터마킹 기술

3.1 데이터 구조

다음 그림은 인증서버에 대한 데이터베이스 구조를 설명하고 있다.

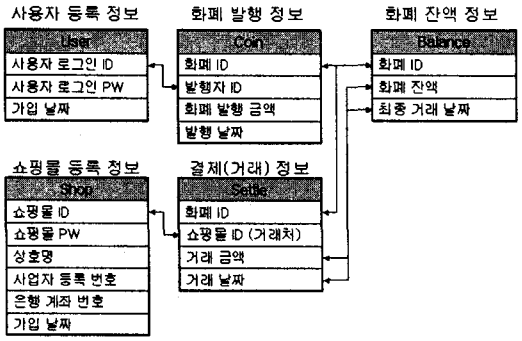

그림 2. 인증서버의 데이터 구조.

인증서버의 데이터베이스 구조는 기본적으로 사용자의 익명성을 기본으로 하여 설계되었다. 거래내역을 기준으로 결제가 이루어진다. 사용자가 쇼핑몰을 통해 물건을 구매하게 되면 인증서버를 통해 사용자의 멀티미디어 전자화폐의 잔액을 확인하고 쇼핑몰에 결제를 해 주게 된다. 그러나 실제 멀티미디어 전자화폐의 잔액은 인증서버에서 관리하기 때문에 실제적인 결제 과정은 인증서버에서 쇼핑몰에 하게된다.

3.2 워터마킹 기술

워터마킹 기술은 멀티미디어 데이터에 사용자 정보를 삽입함으로써 사용자의 저작권을 보호할 수 있는 기술로써 최근 각광받고 있는 기술이다. 본 논문에서는 전자화폐로 사용될 멀티미디어 데이터에 화폐에 대한 정보를 삽입함으로써 멀티미디어 데이터를 화폐로 사용할 수 있도록 하였고, 익명성 및 비추적성, 양도가 가능하도록 하였고, 화폐의 위•변조를 효과적으로 막을 수 있도록 하였다.

3.2.1 이미지 워터마킹

본 논문에서 제안하는 멀티미디어 전자화폐에 실제 활용되는 화폐는 이미지이다. 즉, 디지털 이미지에 워터마크로써 화폐의 ID 를 삽입함으로써 화폐로써의 가치를 만들어 내는 것이다. 이미지에 전자화폐의 ID 와 패스워드를 삽입하고, 전자화폐 이용시에는 이 이미지를 이용하여 전자화폐 ID 를 추출하도록 되어 있다. 사용자는 먼저 사용할 전자화폐를 선택하고 선택된 전자화폐에 대한 패스워드를 입력한다. 입력된 패스워드가 맞으면 삽입된 전자화폐 ID 를 추출한다.

다음 수식은 이미지 전자화폐에 사용된 간단한 워터마킹 식으로써 LSB(최하위비트)를 전자화폐 ID 의 바이너리 코드(Binary code)로 바꿔주도록 설계되었다.

$$f_{LSB}(P_{xy}) = Bin_{ID} \quad (1)$$

전자화폐의 ID 와 패스워드는 내부적으로 암호화되어 있다. 따라서 이미지로부터 직접적으로 코드를 형성했다고 하더라도 불법적으로 뽑아진 이 코드는 아무런 의미가 없는 데이터로 취급되어진다. 전자화폐의 사용을 위해서는 전자화폐에 삽입된 패스워드를 알아야 한다.

3.2.2 비디오 및 오디오 워터마킹

비디오나 오디오는 파일의 크기가 커서 화폐에 활용하기에는 약간의 무리가 따른다. 그러나 비디오나 오디오는 광고의 비중을 많이 차지 하고 있기 때문에 본 논문에서는 비디오나 오디오 데이터에 워터마크를 삽입하여 광고를 보는 사람에게도 이익을 분배할 수 있도록 함으로써 광고의 활용성을 배가시키고자 한다.

일반적인 쇼핑몰에 사용자가 접속하게 되면 아무런 절차없이 무분별한 광고가 사용자 창에 뜨게 된다. 그리고 사용자들도 아무런 생각없이 그 창을 닫는다. 이러한 행위는 광고를 하는 사람이나 사용자 모두에게 별 이익이 되지 않는다. 사용자는 필요없는 광고창을 닫는데 시간을 소비하고 광고주는 그러한 광고를 위해 돈을 투자한다.

본 논문에서는 광고를 보아준 사람에게 워터마킹 기술을 통해 일정액의 전자화폐를 지급함으로써 사용자와 광고주의 이익을 도모하고자 한다.

비디오에 워터마크로써 전자화폐의 ID 를 삽입한다. 그러나 한 프레임에 모든 ID 정보를 삽입하는 것이 아니라 마치 Time stamp 처럼 일정 또는 랜덤한 위치에 분할해서 삽입함으로써 전체 광고를 모두 본 사람에 한해서 이 광고에 삽입된 또는 새로운 전자화폐를

발행해서 보내주는 것이다.

다음 그림은 이와 같은 과정을 설명하고 있다.

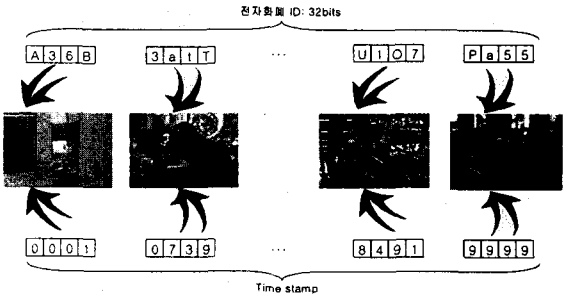

그림 3. 비디오파일에 워터마크삽입

오디오 파일에는 비디오파일과 마찬가지의 과정을 통해 광고효과와 이익분배의 효과를 가져올 수 있다.

4. 결 론

본 논문에서는 워터마킹 기술을 이용하여 현금이나 전자화폐를 대신할 수 있는 새로운 전자화폐를 소개하였다. 일반적인 전자화폐와는 달리 워터마킹 기술을 통해 현금처럼 익명성 및 양도성을 제공할 수 있도록 하였고, 위·변조를 방지할 수 있도록 하였다. 또한, IC 칩을 이용한 전자화폐보다 많은 양의 정보를 삽입할 수 있어서 전자화폐의 ID 외에도 보다 많은 정보를 삽입할 수 있었다.

5. ACKNOWLEDGEMENT

본 논문은 산업자원부-전자상거래기술개발사업(워터마킹 기법을 이용한 멀티미디어 전자화폐 구현)의 지원으로 수행되었음.

참고문헌

[1] Burr, W. E., D. Dodson, N. Nazario, and W. T. Polk, "Minimum Interoperability Specification for PKI Components, Version 1," NIST, http://csrc.nist.gov/pki, 1997

[2] 제대식, 이은철, 윤국섭, "지식경영과 특허전략", 세종서적, 2000. 9

[3] 특허청, "정보처리 및 컴퓨터 운영과제에 관한 PM 개발 최종 보고서", 2000.12

[4] 특허청 컴퓨터심사담당관실, "전자상거래와 사이버법", 2000. 4

[5] 夕田 雄之, 木下 直樹, "스마트 카드 가이드 북", 昭和情報(株), 1999

[6] Tim Dierks and Christopher Allen, "*The TLS Protocol Version 1.0*," IETF Network Working Group, RFC2246, 1999.

[7] Robert H. Deng, Yongfei Han, Albert B. Jeng, and Teow-Hin Ngair, "*A New On-Line Cash Check Scheme*," Proc. of the 4th ACM Conf. on Computer and Communications Security, pp. 111–116, ACM Press, 1997.

[8] 최형섭, 김상진, 오희국, "분할 가능한 화폐를 위한 새로운 환불방식", 한국 정보보호학회 종합학술대회논문집, pp. 177-180, 2001.

[9] 김상진, "거스름의 재사용이 가능한 전자화폐", 한양대학교 석사학위 논문, 2002.