워터마킹 기술을 활용한 이미지 전자화폐에 관한 연구

이 정 수† · 김 회 율††

요 약

본 논문에서는 이미지에 watermark를 삽입함으로써 이미지를 전자화폐로 활용할 수 있는 기술을 소개한다. 이미지에 콘텐츠ID를 부여하고 이 콘텐츠ID를 눈에 보이지 않도록 이미지에 삽입한다. 이미지 전자화폐(이후 WaterCash라 명명)를 발급하는 발급서버에서는 이 콘텐츠ID를 데이터베이스에 저장하고 전자화폐로써 관리한다. WaterCash는 익명성을 보장할 수 있고, 또한 WaterCash의 위·변조를 semi-fragile watermarking 기법을 기반으로 원천적으로 차단할 수 있다. 또한 양도가 가능하고, 워터마킹 기술을 기반으로 하기 때문에 WaterCash의 부정사용을 방지할 수 있다. 사용된 워터마킹 기술은 압축에는 강인하면서 다른 고의적, 비고의적 이미지 처리에는 연약하도록 설계되었다.

A Study on Image Electronic Money based on Watermarking Technique

JungSoo Lee† · WhoiYul Kim††

ABSTRACT

This study introduces a technology utilizing digital images as electronic money by inserting watermark into the images. Watermarking technology assign contents ID to images and inserts the contents ID into the images in an unnoticeable way. The server that manages the issue and the usage of image electronic money (called 'WaterCash' hereafter) stores issued contents ID to database and manage them as electronic money. WaterCash guarantees anonymity and prevents the forgery and modification of WaterCash based on semi-fragile watermarking technique. In addition, WaterCash is transferable and the illegal use of WaterCash can be prevented based on the watermarking technology. The watermarking technology used in this paper was designed to be robust to image compression but vulnerable to intentional or non-intentional image processing.

키워드 : 워터마킹(Watermarking), 콘텐츠ID(Content ID), 전자화폐(Electronic Money), 위·변조(Forgery and Modification)

1. 서 론

최근, 인터넷상의 거래나 정보서비스를 제공하는 사이버 비즈니스가 증가하고 전자상거래가 급속하게 부상함으로써 개인의 프라이버시를 보호하고 위·변조의 부정사용을 방지할 수 있는 지불 수단의 필요성이 부각되고 있다. 전자화폐는 은행계좌를 직접적으로 접근하지 않고 사용될 수 있는 전자적 지불 수단으로써 전자상거래에 있어 효율적인 지불수단으로 자리잡고 있다[1-4, 8].

그러나 이러한 전자화폐는 복사, 위·변조, 도난 등의 위험에 항상 노출되어 있고, 발급과 폐기 등에 많은 비용이 들어가야 한다.

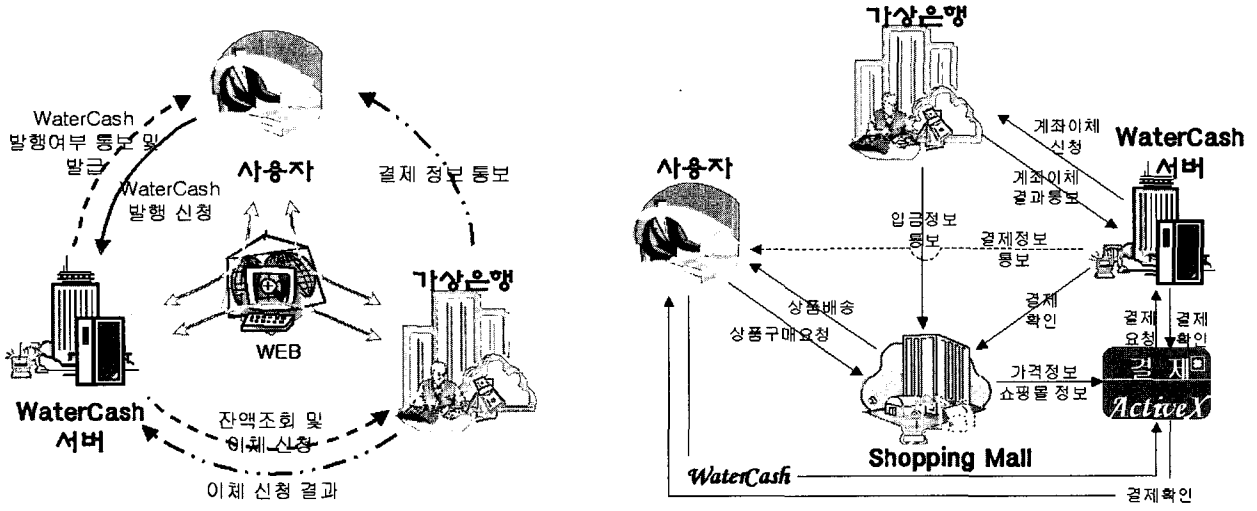
본 논문에서는 새로운 개념의 전자화폐를 소개하고자 한다. 기존의 전자화폐의 기능에 전자화폐의 위·변조를 방지하기 위해 워터마크를 삽입하였다. 또한 사용자의 프라이버시를 보호할 수 있도록 화폐사용의 익명성을 제공하고 필요에 따라 양도가 가능하다[3]. 또한 제작이 쉬운 디지털 이미지를 전자화폐로 사용함으로써 기존의 전자화폐나 일반통용화폐의 발행이나 폐기 들어가는 엄청난 비용을 절감할 수 있다. 사용된 semi-fragile watermarking기술은 또한, 이미지 전자화폐(이후 WaterCash라 명명)의 위·변조를 원천적으로 차단할 수 있게 해 주며, 위·변조를 하게 되면 WaterCash로써의 기능이 상실되도록 설계되었다[5-7].

※ 본 논문은 국가지정연구실사업(NRL-Project 2000N-NL-01-C-286)으로 지원되었음.
† 정 회 원 : ㈜ 마크애니부설연구소 책임연구원, 한양대학교 박사과정
†† 종신회원 : 한양대학교 전자전기컴퓨터공학부 교수
논문접수 : 2004년 3월 15일, 심사완료 : 2004년 8월 4일

본 논문은 다음과 같이 구성되어 있다. 2장은 WaterCash의 전체시스템에 대해서 설명한다. 시스템의 구조와 각 개체에서의 기능 및 역할을 설명한다. 3장에서는 본 논문에서 사용된 워터마킹 기술과 이미지에 삽입되는 데이터 구조를 설명하고, 4장에서는 실험을 통해 WaterCash를 실제로 위·변조했을 때 위·변조한 부위를 잘 찾아내는지를 실험했고, WaterCash가 JPEG 압축에는 얼마나 강인한가를 측정한다. 마지막으로 5장에서는 WaterCash의 개발에 대한 결론과 활용방안을 설명한다.

2. WaterCash 시스템 구조

(그림 1)은 WaterCash의 발행 및 이용방법에 대해서 설명하고 있다. WaterCash서버를 통해 WaterCash를 발급받고, 쇼핑몰을 통해 지불수단으로써 WaterCash가 이용되는 그림으로 워터마킹 기술을 통해 이미지에 삽입되는 데이터를 기반으로 한다.



(a) WaterCash의 발행 (b) WaterCash의 이용

(그림 1) WaterCash의 발행 및 이용

2.1 WaterCash의 발행 및 거래

사용자는 WaterCash 서버를 통해 WaterCash를 발급받을 수 있다. 사용자가 WaterCash를 발급받기 위해서는 먼저, 결제은행의 계좌번호를 입력해야 한다. WaterCash 서버에서는 입력된 사용자의 계좌번호를 이용하여 해당은행의 계좌에 사용자가 신청한 만큼의 잔액이 있는지 조사하고 있다면 해당금액의 WaterCash를 사용자에게 발행한다. WaterCash 서버에서는 발행된 WaterCash에 대한 콘텐츠 ID와 발행일 등의 정보를 데이터베이스에 기록한다.

발행된 WaterCash를 사용하기 위해 사용자는 WaterCash를 휴대용 저장장치에 저장하여 오프라인으로 쇼핑몰에서 구매를 하거나 온라인으로 쇼핑몰에 접속하여 물건을 구매할 수 있다. 온라인 쇼핑몰에서 구매를 위해 접속한 사용자는 결제과정에서 자신의 WaterCash를 입력하고 WaterCash에 대한 비밀번호를 입력한다. 이 과정에서 사용자는 물건을 받기 위한 자료 이외의 개인정보는 입력하지 않아도 된다. 사용자 비밀번호를 입력하게 되면 WaterCash로부터 워터마킹 기술을 이용하여 삽입된 고유한 콘텐츠ID를 추출하여 WaterCash 서버로 전송한다. WaterCash 서버에서는 입력된 WaterCash의 사용 가능성을 확인하고 사용 가능한 전자화폐에 대해서는 결제가 이루어졌음을 통보한다. 또한 WaterCash 서버는 입력받은 WaterCash에 대한 데이터베이스를 갱신하고 결제된 금액만큼 해당 쇼핑몰의 계좌로 입금시켜준다.

2.2 WaterCash의 양도

WaterCash는 위의 기능이외에도 타인에게 양도할 수 있는 기능을 가지고 있다. WaterCash는 익명성을 기반으로 하고 있기 때문에 타인에게 양도가 가능하다. WaterCash의 양도는 WaterCash 서버를 통해야 한다. 즉, 양도하고자 하는 WaterCash를 입력하면 WaterCash서버에서는 입력받은 WaterCash에 대한 고유 콘텐츠ID를 삭제하고 새로운 콘텐

츠ID를 입력하여 양도받을 사용자에게 E-메일을 통해 전송하게 된다. WaterCash를 양도 받은 사용자는 초기화 되어 있는 비밀번호를 변경하고 사용하면 된다.

3. 워터마킹 기술과 데이터 구조

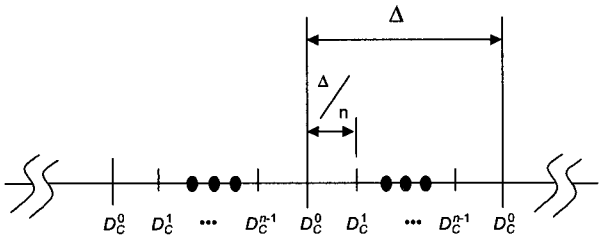
3.1 워터마킹 기술

본 연구에서 워터마킹 기술은 WaterCash에 콘텐츠ID와 부가 정보를 삽입하는 데 사용된다. 사용된 워터마킹은 Semi-fragile watermarking기법으로써 이미지의 압축에는 강인하지만 다른 악의적인 이미지 변형에는 약하도록 설계되었다. 즉, 데이터가 삽입된 WaterCash의 일부 혹은 전부를 수정하면 수정된 부분에 삽입되었던 워터마크가 깨지게 되어 결과적으로 WaterCash를 사용할 수 없게 된다.

본 논문에서는 위의 semi-fragile watermarking기법을 바탕으로 WaterCash를 설계하였고, 익명성 및 비추적성, 양도의 기능과 WaterCash의 불법적인 위·변조를 막을 수 있는 기능을 갖도록 하였다.

3.1.1 디더 변조

본 논문에서 디더 변조는 이미지에 데이터를 삽입하기 위해 사용된다. 콘텐츠ID가 입력되면 이 콘텐츠ID에 따라 디더 변조를 수행함으로써 콘텐츠ID가 이미지에 삽입되게 된다.



(그림 2) 디더 변조

그림에서 보는 바와 같이 Δ의 구간을 n 등분한다. 여기서 n은 하나의 DCT계수에 삽입할 bits수, k에 의해서 결정되는 것으로 $n=2^k$이다. 예를 들어 Δ를 4등분하여 디더 변조를 하게 되면 DCT계수 하나에 삽입할 수 있는 데이터의 양은 2bits가 된다. $D_c^i(i=0,1,\cdots,n-1)$는 디더변조했을 때의 DCT계수로써 i는 삽입된 데이터를 의미한다. 간단한 예로써 Δ구간을 두 영역으로 나누게 되면 하나의 DCT계수에 대해 디더변조를 수행하여 삽입할 수 있는 bit의 양은 1bit가 된다. 즉, 나누어진 두 영역은 각각 '0'과 '1'을 대표하는 구간으로 표시된다. Δ를 큰 수로 나누게 되면 더 많은 bits를 삽입할 수 있지만 이미지의 압축에 대한 강인성을 떨어뜨리고 이미지의 품질을 저하시키는 결과를 초래한다. 따라서 데이터의 양과 강인성, 이미지 품질과는 tradeoff 관계에 있다.

3.1.2 워터마크 삽입

본 절에서는 WaterCash에 데이터를 삽입하기 위해 사용된 이미지 워터마킹 기술을 소개한다. 워터마크로 사용되는 신호는 WaterCash에 부여되는 콘텐츠ID와 재삽입 방지코드, 그리고 사용자 패스워드이다.

먼저, 입력된 데이터를 '0'과 '1'의 이진부호로 만들고, 이미지의 8×8 픽셀을 한 블록으로 설정하여 1bit를 삽입한다. 데이터의 삽입과정을 살펴보면 다음과 같다.

① 입력된 이미지를 8×8 픽셀 단위의 블록으로 DCT 변환한다.

② 삽입될 데이터에 따라 식 (1)과 같이 DCT 계수를 디더 변조한다.

$$D_c^0(u,v)=sign(C(u,v))\times Q\left(|C(u,v)|+\frac{\Delta}{2}\right) \quad if \ d_i==0$$

$$D_c^1(u,v)=sign(C(u,v))\times Q(|C(u,v)|)+\frac{\Delta}{2} \quad if \ d_i==1$$

$$u,v=0,1,\cdots,7 \text{ and } i\geq 0\text{인 정수} \qquad (1)$$

여기서, D_c^{di}는 dither modulation된 DCT계수를 나타낸다. d_i는 삽입할 데이터로써 d_i에 따라 dither modulation 값이 달라진다. $sign(\cdot)$는 입력 값의 부호를 의미하는 것으로 다음과 같이 표현된다.

$$sign(x)=\begin{cases} x/|x| & if \ x\neq 0 \\ 1 & if \ x=0 \end{cases} \qquad (2)$$

$Q(\cdot)$는 Δ로 입력값을 양자화하는 것을 의미한다.

③ Dither modulation된 DCT 계수에 대해서 inverse DCT 변환을 수행한다.

3.1.3 워터마크 추출

워터마크의 추출과정은 워터마크의 삽입과정과 유사하다. 본 절에서는 워터마크로써 삽입된 데이터를 추출하는 과정을 설명한다.

① 입력된 이미지를 8×8 픽셀 단위로 나누고, DCT 변환을 수행한다.

② 식 (3)을 통해서 삽입된 데이터를 추출한다.

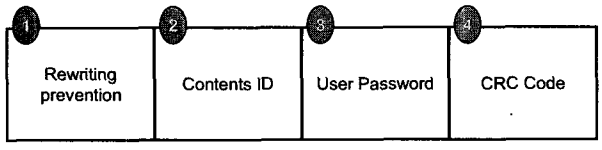
$$d_i = MOD_2\left\{\left[\frac{|C(u,v)|}{\Delta/2}\right]\right\} \quad d_i \in \{0,1\} \qquad (3)$$

여기서, $MOD_2\{\cdot\}$는 입력 값을 2로 나눈 나머지 값을 의미한다. 또한 $[\cdot]$은 입력 값에 가까운 정수 값으로 결과를 산출해 준다.

③ 추출한 데이터를 의미있는 코드로 구성한다.

3.2 삽입 데이터 구조

이미지를 전자화폐로 활용하고 전자화폐의 익명성, 양도성을 만족시키기 위해서 이미지에 콘텐츠ID를 삽입한다. 뿐만 아니라 다음 (그림 3)처럼 개인의 패스워드와 콘텐츠ID의 재삽입을 방지하는 코드를 삽입하게 된다.



(그림 3) 삽입 데이터 구조

첫 번째 영역의 재삽입 방지 코드는 일정한 규칙을 갖는 코드가 되도록 설계한다. 이미지에 콘텐츠ID를 삽입할 때, 먼저 이미지에 이전에 콘텐츠ID가 삽입되었었는지를 체크하여 한번 콘텐츠ID가 삽입된 이미지는 다른 콘텐츠ID를 삽입할 수 없도록 한다. 두 번째 영역의 콘텐츠ID 영역은 이미지에 할당된 콘텐츠ID를 삽입하는 영역이다. 이 콘텐츠ID를 통해 WaterCash가 화폐로써 활용될 수 있다. 즉, 추출된 콘텐츠ID와 동일한 콘텐츠ID를 WaterCash 서버 내에서 찾아서 WaterCash서버 내에 있는 콘텐츠ID의 데이터베이스를 확인함으로써 WaterCash의 잔액과 사용내역, 구매 등의 화폐로써의 역할을 수행하도록 한다.

세 번째 영역인 사용자 패스워드 영역은 도난이나 분실로 인한 사용자의 피해를 막아준다. 사용자 패스워드는 hash function을 거쳐서 결정되기 때문에 길이에 제한이 없다. 따라서 패스워드를 설정하면 타인이 이 전자화폐를 습득하더라도 불법적으로 사용하는 것을 막아준다. 마지막으로 CRC (Cyclic Redundancy Check) 코드를 삽입하여 삽입한 데이터를 뽑아낼 때 뽑아진 데이터가 올바른지를 판단하도록 하였다.

4. 실험결과

본 장에서는 개발된 워터마킹 기법에 대한 실험을 나타낸다. 본 연구에서 개발된 semi-fragile watermarking기법은 이미지에 많은 양의 정보를 삽입하여 전자화폐로 활용해야 하기 때문에 압축에는 강인하고 다른 악의적인 신호처리에는 삽입된 워터마크가 깨져서 나타나야 한다. 또한 이를 이용하여 사용자의 악의적인 위·변조를 효과적으로 차단할 수 있어야 한다. 만일 사용자가 자신의 WaterCash에 대한 정보를 바꾸기 위해 이미지의 일부 혹은 전부를 바꾸었다면 이 WaterCash는 사용이 불가능하게 된다. 이것은 변경된 이미지의 일부 때문에 패스워드가 맞지 않거나 콘텐츠ID를 뽑아낼 수 없게 되기 때문이다. 본 실험에서는 이미지에 임의의 데이터를 삽입하고 일부를 변경했을 때 효율적으로 변경된 부분을 찾아내는 지를 그림을 통해서 확인한다. 또한, 콘텐츠ID가 삽입된 이미지를 JPEG 압축한 후 콘텐츠ID를 뽑아내는 실험으로써 압축률을 조정해가면서 실험한다.

4.1 위·변조 검지

WaterCash로 사용된 이미지의 일부 혹은 전부를 악의를 가진 사용자가 수정하였을 때를 가정하여 이미지에 전체적

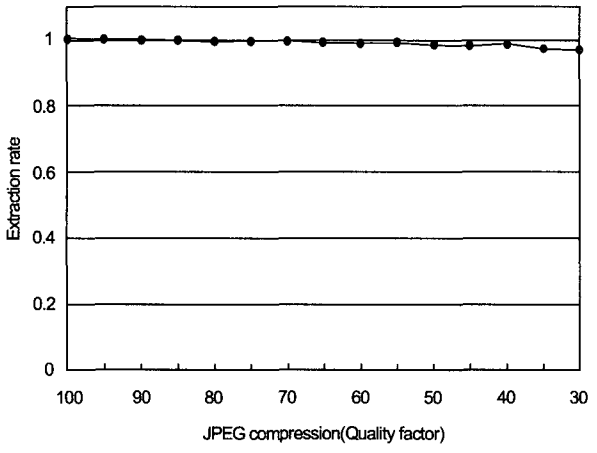
(a) 데이터가 삽입된 이미지 (b) 이미지의 일부가 수정됨 (c) 수정된 부분을 검지

(그림 4) 위·변조 검지 시스템

으로 임의의 데이터를 삽입하였다[6, 7]. 사용된 이미지는 536×240 크기의 이미지로써 8×8 블록에 1bit씩 총 2,010bits를 삽입하였다. (그림 4)(a)는 데이터가 삽입된 이미지를 보여주고 있고, (b)는 (a)의 일부를 수정한 그림이다. (c)는 (b)이미지가 입력으로 들어왔을 때 위·변조 검출 시스템을 돌려서 위조된 부분을 검출하는 그림이다.

4.2 압축에 대한 강인성

다음 그래프는 본 논문에서 제안한 semi-fragile watermarking 기법의 JPEG 압축에 대한 강인성을 실험한 것이다. 이미지에 데이터를 삽입한 후 이 이미지를 압축률을 조정해가며 압축했을 때 삽입한 데이터의 추출률을 보여준다.



(그림 5) JPEG압축에 대한 강인성 실험

추출률 R_E은 식 (4)를 이용하여 계산한다.

$$R_E = 1 - BER, \quad BER = \frac{B_{Err}}{B_{Total}} \tag{4}$$

여기서 BER은 bit error rate로써 추출했을 때 오류가 난 bits와 삽입한 전체 bits의 비율이다. 이미지의 압축률이 높아지면 추출률이 떨어지는 것을 확인할 수 있다. WaterCash 서버에서는 이미지에 삽입한 데이터를 이용하여 전자화폐의 내용을 확인하고, 결정하기 때문에 이미지로부터 추출하는 데이터는 오류가 있어서는 안된다. 따라서 본 시스템에는 데이터를 삽입할 때 오류정정부호가 함께 삽입되어 보다 안정적으로 데이터를 추출할 수 있도록 하고 있다.

5. 결 론

본 논문에서는 이미지 워터마킹 기술을 이용한 이미지 전자화폐(WaterCash)를 개발하였다. Semi-fragile watermarking 기술을 기반으로 하여 이미지를 압축했을 때는 삽입했던 데이터를 추출하고, 악의적인 공격이 있을 때는 삽입했던 데이터를 뽑아낼 수 없도록 하였다. 또한, WaterCash는 도난, 위·변조를 방지하고 익명성과 양도성을 보장함으로써 보다 안전하고 개인의 프라이버시를 보장할 수 있도록 하였다.

디지털 영상의 취득과 제작이 용이하게 바뀌어 가고 있기 때문에 일반통용화폐나 신용카드, 기존의 전자화폐에 비해 발급이나 폐기에 따른 부대비용을 절감할 수 있다. 또한 어떤 이미지라도 화폐로써 활용이 가능하기 때문에 광고효과를 거둘 수 있고 상품권으로써의 활용도 가능하다.

Reference

[1] Darius Buntinas, Eric Mazuk, "Digital Cash and Electronic Commerce," 1997.

[2] Group of Ten, "Electronic money," *http://www.bis.org/publ/gten01.htm*, ISBN 92-9131-901-5, April, 1997.

[3] G. Davida, Y. Frankel, Y. Tsiounis, M. Yung, "Anonymity Control in E-Cash Systems," *Financial Cryptography'97*, 1997.

[4] 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, ACM Press, pp.111-116, 1997.

[5] M. U. Celik, G. Sharma, E. Saber, A. M. Tekalp, "Hierarchical Watermarking for Secure Image Authentication with Localization," *IEEE Trans. Image Proc.*, Vol.11, No. 6, June, 2002.

[6] E. T. Lin, C. I. Podilchuk and E. J. Delp, "Detection of Image Alterations Using Semi-Fragile Watermarks," *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents* II, Vol.3971, Jan., 2000

[7] Qibin Sun, Shih-Fu Chang, Maeno Kurato and Masayuki Suto, "A new semi-fragile image authentication framework combining ECC and PKI infrastructure," *ISCAS02, Phoenix*, USA, May, 2002.

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

이 정 수

e-mail : jslee@markany.com

1995년 전북대학교 제어계측공학과(공학사)

1997년 전북대학교 의용생체공학과 (공학석사)

1997년~현재 한양대학교 전자전기컴퓨터 공학부 박사과정

2000년~현재 ㈜ 마크애니부설연구소 책임연구원

관심분야 : 영상처리, 디지털 워터마킹, 컴퓨터비전, 등

김 회 율

e-mail : wykim@hanyang.ac.kr

1980년 한양대학교 전자공학과(공학사)

1983년 Pennsylvania State University 전기공학과(공학석사)

1989년 Purdue University 전기공학과 (공학박사)

1989년~1994년 University of Texas 조교수

1994년~현재 한양대학교 전자전기컴퓨터 공학부 정교수

관심분야 : 영상처리, 컴퓨터비전, 패턴 인식, 머신비젼, MPEG-7 등