특집 : 멀티미디어

디지털 방송의 영상정보 보호를 위한 디지털 서명 기법

서정일*·우석훈*·원치선*·이춘**·김영길**
*동국대학교 전자공학과
**LG전자영상미디어연구소

I. 서론

TV 신호의 암호화를 위한 제한 수신 시스템(CAS, Conditional Access System)은 TV 프로그램의 상품화(유료화) 개념을 도입한 이래로 꾸준히 발전해 왔다. 초기의 제한수신 시스템은 아날로그 형태의 TV 신호 전송 체계에 맞게 표준 TV 신호에 변형을 가하는 형태로 시작되었다. 그러나 디지털 TV의 등장으로 디지털 신호처리가 가능해지면서 진정한 의미의 TV 신호의 암호화가 사용되었다. TV 신호의 암호화는 군사용 기밀이나 은행 정보의 암호화와는 달리 다음과 같은 세 가지 큰 특성을 갖는다. 첫째, 암호화를 해야할 TV신호의 정보량은 군사용 기밀이나 은행 정보에 비해 상당히 크다. 따라서, TV신호의 실시간 전송을 위해 모든 TV 신호 데이터열에 복잡한 암호화 기법을 적용하는 것은 비경제적이며 비교적 간단한 스크램블링(scrambling)을 통해 원래의 프로그램 신호형태를 변형하고, 스크램블링에 사용한 키는 복잡한 암호화 기법으로 암호화하는 이중 구조를 갖는다. 둘째, 디지털화된 TV 신호는 공간적 또는 시간적인 중복성(상관성)이 많아 스크램블링시 주의를 요한다. 셋째, TV 신호는 군사용 기밀이나 은행 정보에 비해 정보의 가치가 상대적으로 낮다. 따라서, TV 수신자들이 자신의 비밀키를 적극적으로 보호하려는 의지가 낮고 제3자에게 자신의 비밀키를 대여해 줄 가능성이 있다. 이와 같은 TV신호의 고유 특성 때문에 TV 신호는 그 특성에 알맞은 암호화 기법을 요구한다. 이런 요구는 최근 TV 방송 시스템이 TV신호의 압축 기법을 포함하는 완전 디지털 전송 방식으로 전환되고, TV 신호의 압축을 위해 국제적인 표준인 MPEG-2를 따르는 것이 보편화되면서 세계적인 규격이 갖춰지고 있다. 예를 들어 유럽의 위성, 케이블, 그리고 지상방송의 종합적 디지털 방송에 대한 규정으로 DVB(Digital Video Broadcasting) 규격을 제정하여 마무리 단계에 있다. DVB에서는 MPEG-2에 의한 디지털 압축 및 전송 규격을 따르며, TV 신호의 암호화 기법은 Simulcrypt 방식으로 제안되어 데이터의 스크램블링은 슈퍼 스크램블링(Super scrambling) 기법으로 통일하고, 이때 사용된 키의 암호화 기법은 각 방송사의 고유 암호화 기법을 인정하는 방법이다. 이와 같이 TV 방송에서 스크램블링이나 제한 수신 시스템과 같은 암호화 기술이 이용되는 것은 최근 TV 방송의 추세가 기존의 TV 방송처럼 일방적으로 일차적인 정보만 이용자에게 제공하는 것이 아니고, 이용자의 요구에 의해 다양한 부가 정보를 제공하는 경향을 띠며, 쌍방향 채널(Interactive Channel)을 이용한 고급 정보의 교환 등도 점차 다양해지고 있는 추세이기 때문이다. 이런 추세에 맞춰 정보의 제공자나 이용자 모두가 정보에 대한 신뢰성에 대한 의심을 방지하기 위해서 정보의 보호 차원이나 이용자 혹은 제공자의 권리 보호 차원에서 쌍방간에 이루어지는 정보 전송에 대한 일정한 규칙이 필요하다. 이러한 규칙을 구체화한 것이 제한 수신 시스템에서의 인증(Authentication)이다. 인증은 통신 시스템 상에서 송수신자간의 안전성의 여부를 파악하는 것이다. 디지털 신호의 경우는 비록 암호화가 되었다고 하더라도, 복제나 변조의 불법적인 정보 공격이 용이하므로 비밀유지를 위해 인증의 절차가 반드시 병행되어야 한다. 그것은 디지털 정보의 경우는 정보가 "0", "1"로만 기록되므로 통신 중에 정보 변조가 용이하고, 또 유료 TV에서 처럼 송수신이 정확하게 이루어졌는가를 확인해야 하는 경우에 대한 증거를 마련하기 위해서이다. 인증을 설명하는데 있어 디지털 서명(Digital Signature)은 필수적이다. 고전적 의미의 인증은 보통, 정보를 암호화하는데 있어, 정보의 마지막 블록에 서명된 정보 블록을 부가적으로 첨가한다. 수신단에서는 이 서명문 확인 여부에 따라 가입자의 등록 여

부, 등급, 요금 등의 모든 부가적 서비스를 제공하게 된다. 이처럼 고전적 의미의 인증은 제한 수신 시스템에서 정보의 사용자와 제공자가 서로 대화형 이용(interactive service)을 가능하게 해준다. 그렇지만, 고전적 의미의 인증 방법은 동영상에 적용하기에 몇 가지 문제점을 가지고 있다. 첫째, 고전적 인증의 방법은 인증을 위한 서명문을 원 정보에 부가적으로 첨부하여 전송하므로 전송할 정보량이 많아진다. 두 번째로, 인증을 위한 서명문은 대부분 고차 다항식 연산에 의해 서명문을 생성하므로, 실시간 처리가 중요시되는 동영상에는 적용하기가 어렵다. 이처럼 고전적 의미의 인증은 주로 문자 정보(text data)에 적용되도록 고안되었기 때문에 동영상에 적용하기는 매우 어렵다. 이런 문제점을 해결하고, 주로 영상에 대해서만 적용될 수 있는 새로운 인증 방법이 서명 문양(Watermark)을 이용한 디지털 서명(Digital signature) 이다. 디지털 서명은 디지털 영상의 여러 특성들을 이용하여 영상 정보에 인증을 위한 서명 문양을 삽입하고, 삽입된 서명 문양을 필요한 경우 검출하므로써 인증을 수행하는 방법이다. 서명 문양을 이용하는 디지털 서명의 경우는 고전적인 인증과는 달리 별도의 서명문을 전송하지 않으므로 전송되는 정보량의 변화가 없으며, 영상의 저작권만을 보호하는 수단이므로 영상의 이용자를 제한하는 것이 아니고 이용은 누구나 할 수 있도록 하며, 정보의 제공자는 그 이용을 관리하는 것이 가장 큰 차이점이다. 예를 들어, TV 프로그램의 일부 장면을 이용자가 복제나 편집하여 이용한다면 그 이용 자체를 방지하는 것이 아니고, 영상 이용에 대한 경제적 또는 법적인 권리를 정보의 소유자가 차후에 주장할 수 있도록 하는 것이다. 디지털 서명의 경우 서명 문양을 영상에 직접 처리하므로 전송이나 저장할 때 정보량의 변화가 없고, 이미 계산된 서명 문양을 영상에 삽입하는 것으로 서명이 되므로 동영상의 실시간 처리도 가능하다. 그러나, 서명 문양을 이용한 디지털 서명에도 몇 가지 단점이 있다. 첫째는 원영상에 임의로 변화를 주므로 영상 화질에 훼손이 있을 수 있다. 두 번째로는 디지털 영상의 경우 정보량이 매우 크므로 전송이나 저장을 위해서는 영상을 압축 해야 하는데, 압축률을 높이기 위해서는 손실 압축(lossy compression)의 방법을 이용하게 된다. 물론 손실 압축의 결과로 영상의 화질이 시각적으로 크게 손상되지는 않지만, 영상 정보의 작은 변화를 이용하여 인증을 하는 디지털 서명의 경우에는 매우 큰 약점이 된다. 때문에 일차적으로 디지털 서명은 압축 환경을 고려해야 한다는 전제 조건이 있어야 한다. 물론 경우에 따라서는 무손실(lossless compression) 압축의 방법을 이용할 수도 있지만 이것은 매우 특수한 경우로 일반적인 디지털 방송에 적용되기 위해서는 압축 환경에 대한 고려가 있어야 한다. 본 고에서는 고전적 의미인 제한 수신 시스템에서의 인증과 서명 문양(Watermark)을 이용하는 디지털 서명에 대해서 각각의 의미와 대표적인 기법들을 소개하고, 실제 디지털 방송에 적용하기 위해 고려해야 할 사항들을 살펴본다.

II. 유료 방송을 위한 제한 수신 시스템

TV 신호를 위한 제한 수신 기술은 기능면에서 다음과 같이 양분될 수 있다. 첫째는 원래의 프로그램 신호의 형태를 변형하는 스크램블링(scrambling) 기술이고, 두 번째 기술은 변형된 신호를 복원하는 디스크램블링(descrambling)에 필요한 관련키와 각 수신자들의 시청 권리를 관리하는 자격(entitlement)기술이다. 자격기술은 스크램블링에 사용한 키와 프로그램의 취득 조건을 자격 통제 메시지(ECM, Entitlement Checking Message) 내에 포함시켜 전송하는 자격통제 기능과 자격의 유효기간 등을 자격관리 메시지(EMM, Entitlement Management Message) 내에 포함하여 전송하는 자격관리 기능으로 구분할 수 있다. 자격통제 및 자격관리 메시지 내에는 디스크램블링에 필요한 관련키가 적당한 암호화 알고리즘에 의해 암호화(encryption)되어 각 수신자에게 전송된다. 이러한 기능 블록을 포함한 제한수신 시스템의 기본 구성은 그림 1과 같다[1].

스크램블링(scrambling)은 스크램블링된 신호의 형태만으로는 원래의 신호를 추정할 수 없도록 원 신호에 변형을 가하는 것으로 신호의 종류 즉, 영상, 음성, 일반 데이

디지털 서명(Digital signature) : 원래 의미는 인증을 위해 사용되는 서명문이다. 그러나 본 논문에서는 고전적인 의미의 서명문과 구별하기 위해 서명 문양을 이용하는 방법만을 디지털 서명이라 한정한다.

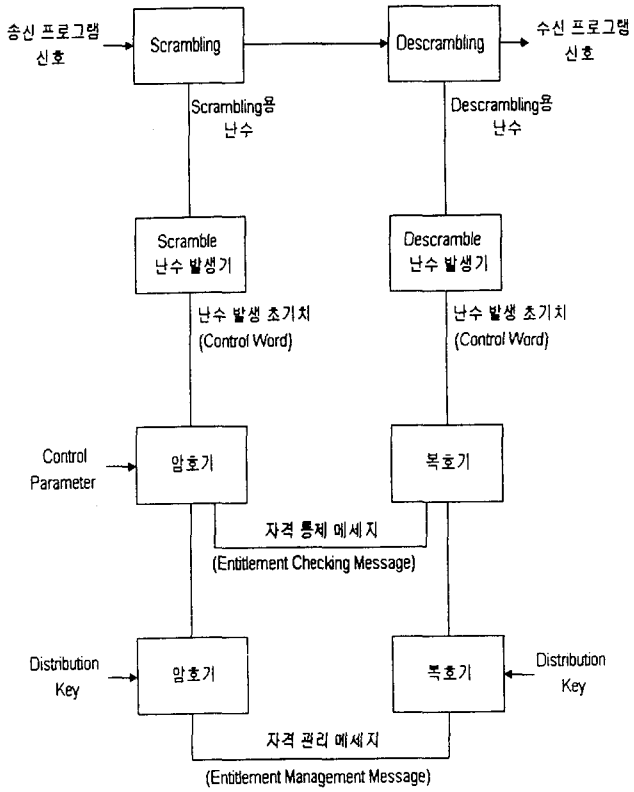


그림 제한 수신 시스템 구성도
Fig 1. Diagram of CAS

터 등에 따라 다르고, 신호의 형태가 디지털이냐 아날로그냐에 따라 달라진다. 일반적으로 제한 수신 시스템을 위한 스크램블링 방식이 갖추어야할 조건은 우선 스크램블링과 디스크램블링 과정 중 원 신호가 열화되지 않고, 영상과 음성이 스크램블링되는 제한수신 모드와 함께 스크램블링 없이 가입자뿐만이 아니라 미가입자도 원신호를 수신할 수 있는 공개모드도 갖추어야 한다. 또한, 스크램블링의 방식을 결정할 때 고려되어야할 조건으로 디스크램블러의 가격이 가능한 저렴해야 한다는 것이다. 그러나, 디스크램블러의 가격과 스크램블링 방식의 비화도는 서로 상보관계(trade-off)에 있으므로 적절한 수준의 비화도를 유지하면서 가격도 합당한 스크램블링 방식이 채택되어야 한다[2][3]. 제한 수신 시스템을 위한 비디오 신호의 스크램블링은 음성 신호와 영상 신호에 각기 다른 방법을 사용한다. 음성 신호의 스크램블링(암호화)은 발생된 의사 난수와 디지털화된 음성 신호를 $GF\{2\}$상의 가산 방식을 대부분 채택하고 있다. 영상 신호의 스크램블링은 비디오 신호 변형, 동기(sync) 신호 변형 및 이들의 혼합된 방식으로 나눌 수 있고 변형될 신호의 형태에 따라 아날로그 및 디지털 방식으로도 구분된다. 하지만, 최근 대부분의 정보가 디지털로 저장 또는 전송되어 이용되므로 본 절에서는 디지털 스크램블링 방식에 대해서만 논의하도록 한다.

디지털 영상 신호는 그 신호만이 갖는 특성에 의해 신호처리에 있어 몇 가지 제약을 가지고 있다. 먼저 영상 정보는 그 정보량이 너무 크기 때문에 그 정보를 제대로 저장하거나 전송하기에는 매우 어렵다. 예를 들어, 1시간 분량의 TV 영상 신호의 정보는 대략적으로 360GB의 메모리를 차지한다. 이 정도 분량의 정보를 저장하거나 전송한다는

것은, 그것도 실시간 처리를 위해서는 극히 어려운 문제인 것이다. 따라서, 디지털 영상을 다루는데 있어 반드시 필요한 것이 영상 압축이다. 즉, MPEG-2와 같은 압축 방식에 의해서만 동영상의 실시간 처리가 가능한 것이다. 그런데, 이런 압축 환경은 영상에 대한 다른 처리를 하는데 많은 제약을 가한다. 미리 압축된 영상을 스크램블링하는 방법은 실시간 처리가 가능한 반면, 스크램블링의 비화도에 많은 약점을 가지고 있다. 그래서 우리가 먼저 살펴보아야 할 관점은 압축 환경에서의 영상 스크램블링을 위한 순서일 것이다. 압축된 영상 신호를 스크램블링하기 위해서는 몇 가지의 고려 사항이 있다. 우선 전송 채널이 단일 채널이 아니고 여러 채널을 거쳐 정보가 전송된다고 가정한다면, 각 채널에서의 압축 환경이 틀리므로 채널이 바뀔 때마다 압축을 풀고 새로 압축을 해야 한다. 이때, 정보의 스크램블링 역시 채널이 변경될 때마다 디스크램블링과 스크램블링을 반복해야 하는 문제가 발생한다. 이것이 전송률 호환성(Transcodability)의 문제다. 이 경우 중간 사업자 또는 중계소에서 모두 해독키를 가지고 있어야 하므로, 해독키의 관리에 대한 비도를 떨어뜨릴 수 있다. 그러면, 이 문제를 해결하기 위해서 압축 전에 영상 정보에 스크램블링을 가하는 방법에 대해 살펴보자. 이 경우 위에서 발생한 전송률 호환성(transcodability)의 문제나 이로 인해 발생할 수 있는 비화도의 약화는 피할 수 있지만, 이것과는 또 다른 문제가 발생할 수 있다. 그것은 바로 투명성(Transparency)의 문제다. 유료 TV의 경우 비가입자들에게 불법적인 정보의 이용을 제지하는 차원과 동시에 향후 가입을 유도하기 위한 투명성(Transparency)이 보장되어야 한다. 하지만, 스크램블링된 영상을 압축하는 경우에는 이런 투명성을 보장하기 어렵다. 그렇다면 어떤 방법으로 전송률 호환성(transcodability)과 투명성(Transparency)을 동시에 해결할 수 있겠는가 ? 이 질문에 대한 가장 적절한 답변은 안정된 스마트 카드를 활용하는 것이다. 즉 스마트 카드 내에 전송률 호환성(transcodability)을 위해 키 저장과 Transcoding Node를 동시에 보관하게 하는 것이다. 이런 시스템을 IC 카드나 Set-Top Box에 내장하여 각 채널의 중계소와 가입자에게 보관하도록 하면 전송률 호환성(transcodability)과 투명성은 동시에 해결될 수 있을 것이다[4].

Ⅲ. TV 프로그램의 저작권 보호를 위한 인증 기법

3.1 키 암호화를 위한 인증 방법

인증(Authemtication)은 향후 요구되는 쌍방향 부가서비스(interactive service)를 제공하기 위한 것으로 스크램블링을 위한 키의 관리나 TV 프로그램의 저작권 보호를 위해 필요한 개념이다. 본 절에서는 고전적인 인증 방법과 특히 영상 정보의 인증을 위한 디지털 서명에 대해 소개하도록 한다.

3.1.1 대칭적(공통키) 암호화 기법에서의 인증 방식

대칭적 암호화 기법(DES)에서는 인증의 방법으로 MDC나 MAC의 방법을 이용한다. 이때 암호화는 보통 CBC(Cipher Block Chaining) 방법을 기본으로 하고 있다[5]. MDC(Manipulation Detection Codes)는 메세지를 $M_i(1 \le i \le n)$라고 할 때, $MDC(=M_1 \oplus M_2 \oplus \cdots \oplus M_{n-1})$를 메세지에 첨가한 후, 암호화하여 전송한다. 그러나, MDC의 경우 암호화된 메세지에 임의의 블록을 삽입 또는 재배열의 공격이 가능한 단점이 있다. 만약, 제3자가 임의의 암호문 C'를 알고 있다면, 송신되는 암호문 $C(=C_1, C_2, C_3, \cdots\cdots, C_n)$에 대하여 임의의 메세지를 쌍으로 삽입할 경우에는 MDC에는 변화가 생기지 않아 인증의 결과가 틀려진다.

예를 들어, $C' = E_k(M'_i \oplus C'_{i-1})$를 마지막 블록을 제외한 임의의 위치에 쌍으로 삽입하면, 전체 암호문 C는 다음과 같이 된다.

$$C = C_1, C_2, C', C_3, \cdots\cdots, C', C_{n-2}, C_{n-1}, C_n$$

이 경우 평문은 다음과 같이 복호화 된다.

$$M = M_1, M_2, C_2 \oplus D_k(C'), C' \oplus D_k(C), \cdots\cdots, C_{n-3} - \oplus D_k(C'), C' \oplus D_k(C'_{n-2}), M_{n-1}, N$$

위 평문의 MDC를 구하면 다음과 같다.

$$MDC = M_1 \oplus M_2 \oplus D_k(C') \oplus C' \oplus \cdots \oplus D_k(C') \oplus C' \oplus D_k(C_2) \oplus X_{n-1} = M_1 \oplus M_2 \oplus \cdots\cdots \oplus M_{n-2} \oplus M_{n-1}$$

이와 같이 수신단에서 확인하는 MDC는 변화가 생기지 않는다. 따라서 정확한 인증이 이루어지지 않는 단점이 있다. MAC(Message Authentication Codes)의 경우도 MDC와 거의 유사한 과정을 수행한다. 단지 서명값이 조금 다를 뿐이다. MAC에서는 서명값을 CBC에 의해 암호화된 암호문의 최종값 Cn으로 취한다.

$$MAC=E_k(M_n \oplus C_{n-1})=C_n$$

MAC나 MDC를 이용하는 공통키 방식의 인증은 불법적인 공격에 노출이 심한 약점을 가지고 있어, 실제 인증의 역할을 수행하기에는 많은 단점이 있다.

3.1.2 비대칭적(공개키) 암호화에 따른 인증 방식

공개키 암호화 방식에 의한 인증 방법은 암호화 방식마다 제 각기 특징을 지니고 있다. 즉, 공개키 암호화 방식의 특징 중의 하나로서 디지털 서명을 위한 인증의 개념이 부가되어 있다. 때문에 공통키 방식의 암호화에서 처럼 어떤 특별한 부가적인 알고리즘을 첨가하여 인증을 수행하는 것이 아니고, 공개키 암호화 방법 자체만으로 인증의 역할을 수행한다.

가. RSA 인증 방법

RSA 서명은 공개키 암호화 시스템에서 사용되는 기본적인 인증 방식이다[6]. 이 방법은 기밀보호기능과 디지털 서명 기능을 동시에 수행하며, 다른 공개키 방식의 인증 방법과는 달리 유일하게 서명문만을 전송하는 특징을 가지고 있다. 그 인증을 위한 과정은 그림 2에 나타내었다.

RSA 암호화 시스템은 송신자가 보내고자 하는 서명문을 송신자의 비밀키로 암호화한 후, 수신자의 공개키로 암호화하여 이 결과를 송신한다. 수신자는 전송된 정보를 받아 자신의 비밀키로 복호화한 후, 그 결과를 송신자의 공개키로 암호화하여 별도로 전송된 정보와 계산의 결과가 같은 경우 인증은 정당한 것으로 판단된다. 그림 2에서 Dk는 비밀키를 Ek는 공개키를 나타내고, A는 송신자, B는 수신자, M은 전송 정보를 나타낸다.

나. Shamir의 고속 서명 방식

Shamir의 서명 시스템은 서명 및 인증 동작이 간단하여 송신자의 서명문 생성 과정과 수신자의 서명문 인증 과정을 소프트웨어로 구현될 수 있을 정도로 고속으로 실현될 수 있다. 서명 시스템 구성을 위한 시스템 파라미터는 다음과 같은 과정을 통해 구해진다[6][7].

① 송신자는 임의로 선택된 원소 $k_{ij} \in GF(2)(i=1, \cdots\cdots, n, j=1, \cdots\cdots, 2n)$로 구성된 행렬 K를 생성한 후, 송신자의 비밀키로 보관한다.

② $p \geq 2n-1$의 관계를 만족하는 소수 p를 선택한다.

③ 사용자는 벡터 $A=(a_1, a_2, \cdots\cdots, a2_n)$, $a_i \in GF(p)$, $(i=1,2, \cdots\cdots, 2n)$를 계산한다. 생성가능한 방정식의 개수가 n이므로 송신자는 A의 요소중 n개의 요소 $(a_1, a_2, \cdots\cdots, a_n)$를 임의로 선택한다.

만약 송신자가 자신의 서명문을 수신자에게 전달하고 싶을 경우, 송신자는 자신의 비밀키 K를 이용하여 서명문 $S(=M \times K)$를 계산한 후, 수신자에게 전송한다. 서명문 S를 수신하면, 공개키 디렉토리에서 송신자의 공개키 (A,

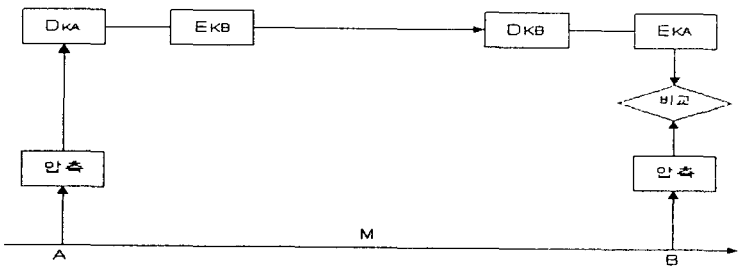


그림 2. RSA 서명 기법
Fig 2. RSA Signature

p)를 가져온 후 평문 M(=S×A)을 복구한다.

라. Ong-Schnorr-Shamir(OSS)의 서명 방식

OSS 서명 방식은 큰 정수에 대한 소인수 분해 문제와 다음과 같은 평방근 문제(quadratic congruence problem)에 기반을 두고 있다[8]. OSS 서명 방식을 실현하기 위한 주요 시스템 파라미터는 다음과 같다.

① 두개의 큰 소수 p, q를 선택한 후, 합성수 N = p×q 를 계산한다.

② gcd(k, N) = 1을 만족하는 임의의 정수 k를 선택한다.

③ k, N을 이용하여 사용자의 공개키 $K \equiv -k^{-2} \bmod N$을 계산한다.

OSS 서명시스템에서의 서명문은 RSA 서명 시스템과는 달리 한 쌍의 서명문 (S_1,S_2)으로 구성된다. 만약 송신자가 gcd(M, N)=1을 만족하는 메세지 M(0<M<n)에 대한 서명문을 수신자에게 전달하고 싶은 경우, 다음과 같은 과정을 통해 수행할 수 있다.

① 송신자는 gcd(r, N)=1인 난수 r을 선택한다.

② 송신자는 메세지 M, 비밀키 k를 이용하여 서명문 쌍을 계산한다.

③ 송신자는 메세지 M과 서명문 쌍(S_1, S_2)을 수신자에게 전달한다.

④ 수신자는 전송 받은 M과 서명문 쌍을 아래의 식을 통해 인증을 검사한다.

$$
\begin{aligned}
S_1^2+K\cdot S_2^2 &= [1/2\cdot(M/r+r)]^2+K\cdot[1/2\cdot(M/r-r)]^2 && \bmod N\\
&= 1/4[M/r+r)^2+K\cdot k^2\cdot(M/r-r)^2] && \bmod N\\
&= 1/4(M/r+r)^2-(M/r-r)^2] && \bmod N\\
&= 1/4[4M] && \bmod N\\
&= M
\end{aligned}
$$

마. ID 기본 서명 시스템

ID 기본 서명 시스템은 지금까지 공개키 암호화 시스템이 공개키 저장을 위한 키 디렉토리를 유지함으로써 통신개시시 키 센터와의 과도한 트랙픽과 메모리가 요구되는 단점을 보완하여 통신상대의 공개키를 상대방의 이름, 망주소, 또는 성별 등의 조합으로 구성된 함수로부터 도출하므로써 망내의 별도의 키센터의 지속적인 유지를 요구하지 않는 것을 특징으로 하고 있다. 그러므로 ID 기본 암호시스템에서의 키 센터는 새로운 사용자가 처음으로 망에 가입할 때만 동작하여 사용자의 비밀키 및 망 관련 공개 정보를 부여하는 기능만을 수행한다. 공개키 암호 시스템을 이용한 서명방식에서는 자신의 비밀키를 이용하여 서명문을 생성하고, 수신자측에서는 송신자의 공개키를 이용하여 서명문의 유효여부를 결정하는 반면, ID 기본 서명 방식에서는 망가입시 암호키 생성센터로부터 받은 비밀키를 이용하여 서명문을 생성하고, 수신자는 송신자의 ID로부터 상대방의 공개키를 계산하여 서명문의 유효 여부를 가린다. 따라서 본 시스템에서는 별도의 암호키 디렉토리가 요구되지 않는 특징이 있다[6][7][8].

지금까지 본 절에서는 각각의 암호화 방식에 대한 디지털 서명 또는 인증의 방법을 알아보았다. 지금까지 개발된 이러한 인증 알고리즘은 영상 정보를 전제로 한 것이 아니라 평문(text) 정보를 대상으로 하고 있다는 취약성을 공통적으로 지니고 있다. 때문에, 이들 알고리즘을 그대로 유료 TV나 영상 화상 통신과 같은 디지털 영상 통신에 적용하기에는 몇 가지 해결해야 할 문제점을 가지고 있다. 우선 영상 압축 환경을 고려하지 않았기 때문에 발생할 수 있는 정보의 보존성 문제와 과연 이런 알고리즘을 통한 인증의 과정이 실시간에 처리될 수 있느냐에 관한 의문점이 바로 그것이다. 따라서, 다음절에서 설명하는 서명 문양을 이용한 디지털 서명 방법은 이러한 문제에 어떻게 대응하는지 살펴보자.

3.2 서명 문양을 이용한 저작권 보호

지금까지는 인증(authentication)을 위한 별도의 서명문(고전적인 의미)을 생성하여 이 서명문을 원정보와 함께 전송하므로써 사용자와 제공자의 권익을 동시에 보호하였다. 하지만 정보량이 매우 크고, 실시간 처리가 중요시되는 디지털 영상의 경우는 고전적 의미의 서명문을 이용할 경우 전송 정보량이 더욱 커지고 서명문 관리가 어렵다는 단점이 있다. 또한 점차 일반화되어 가는 멀티미디어와 네트워크 환경에서 어느 특정 이용자를 전제로 정보를 제공한다는 것은 무의미하다. 최근 대두되는 새로운 의미의 디지털 서명은 네트워크 상에 존재하는 모든 이용자가 곧 정보의 사용자가 된다는 전제로 누구나 자유롭게 정보를

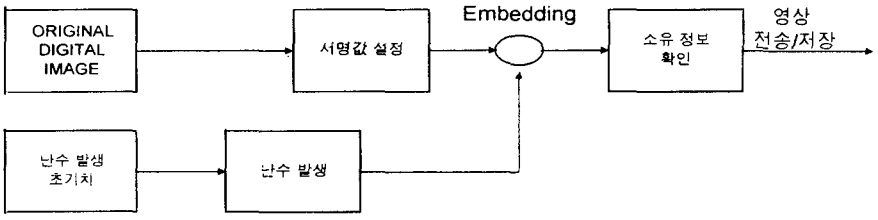
이용할 수 있도록 하면서 정보 제공자가 차후에 정보 이용에 대한 권리를 주장할 수 있도록 제안된 방법이다[4]. 이것은 이미 스크램블링을 소개하면서 언급했던 투명성(transparency)을 더욱 강화한 방법이다. 새로운 의미의 디지털 서명 방법은 영상의 시각적인 특성을 이용하여 영상에 직접 임의의 변화를 주고, 저작권의 확인이 필요할 때는 서명 문양(watermark)이라고 불리는 이 변화를 검출하므로써 영상의 저작권 또는 소유권을 주장할 수 있는 근거를 마련할 수 있도록 하였다. 이 서명 문양 방법은 정보량이 증가하지 않고, 실시간 처리가 보다 용이한 장점을 갖는다. 서명 문양 방법은 인증을 위한 서명과는 달리 정보의 소유자와 이용자의 권리를 동시에 보호하는 차원이 아니고, 일반 대다수의 이용자를 전제로 정보의 소유권만을 보호하는 것이다. 즉, 서명 문양은 인증에 비해 협소한 의미를 가지는 디지털 서명의 한 방법이라고 할 수 있다[4][9][10]. 서명 문양(watermark)은 정보에 가해지는 임의의 변화 모두를 나타내지만, 대체로 두 가지의 형태로 나타난다. 그 중 하나는 서명값을 이용하는 것이고, 나머지 하나는 스탬프(seal or stamp)를 사용하는 것이다. 이 두 종류의 서명 문양은 모두 다음과 같은 전제 조건을 만족해야 한다[4][9][10].

- 삽입된 문양은 시각적으로 구별되지 않아야 한다.
- 영상의 저작권자 및 소유권자는 서명 문양을 쉽고 안전하게 검출할 수 있어야 한다.
- 손실 압축(Lossy compression)이나 필터링(Filtering)과 같은 디지털 영상 처리 기법 등에 대하여 서명 문양이 영향을 받지 않아야 한다.
- 서명 영상(Signed image)에 대해 제 3의 디지털 서명 공격에 강해야 한다.

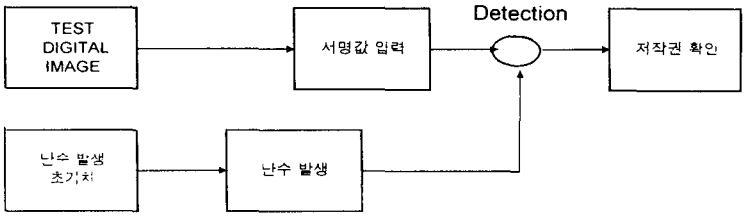
서명 문양에 대한 연구는 최근 다방면에서 많은 발전을 하고 있다. 지금까지의 추세는 안정된 서명 문양의 생성과 검출에 연구 목적을 두고 있다. 본 절에서는 지금까지 소개된 디지털 서명 방법 중에서 대표적인 몇 가지 예를 들어 구체적으로 서명 문양에 대한 내용을 소개한다.

3.2.1 서명 문양의 삽입

서명 문양은 두 가지의 종류가 있다. 그 중 하나는 정수를 이용하는 서명값이고, 나머지 하나는 이진 영상을 이용하는 스탬프(stamp, seal)이다. 두 종류의 서명 문양은 각기 서로 다른 특성을 갖는다. 서명값의 경우는 매 영상마다 다르게 삽입할 수 있어 보다 안정적인 서명 구조를 갖지만, 검출할 때는 대부분 확률적인 접근에 의해 저작권 주장



(a) 서명 문양 삽입 과정



(b) 서명 문양 검출 과정

그림 3. 서명 문양 삽입/검출 과정
Fig 3. The Flowchart of embedding/detection watermarks

(a) 서명 문양

(b) 서명 영상

(c) 검출 서명 문양

그림 4. Stamp를 이용한 서명 문양
Fig 4. A watermark with stamp

을 위한 신뢰도가 낮다는 단점이 있다. 반면, 이진 영상을 이용하는 스탬프의 경우는 서명값에 비해 삽입되는 서명 문양의 종류가 한정적인 단점이 있지만, 검출에 있어서는 서명값보다는 상대적으로 신뢰도가 높은 특성이 있다. 따라서, 각 사용자의 특성에 따라 서명값 또는 스탬프를 이용하여 서명할 수 있다.

서명값을 이용하는 디지털 서명은 서명 문양의 생성이 매우 다양하다. 일반적으로 공통적인 알고리즘을 소개하면 그림 3과 같은 알고리즘으로 구성된다. 먼저, 그림 3. (a)에서 처럼 서명 문양 생성을 위한 이진 의사 난수(pseudo random number)를 발생한다. 이진 의사 난수는 여러 가지 방법으로 생성할 수 있는데, 그 중 대표적인 것이 원시 다항식(primitive polynomial) 연산에 의한 것이다[9][10]. 이진 의사 난수를 생성하는 목적은 한정된 서명값으로 다양한 서명 패턴을 확보하는데 있다. 즉, 원영상이 열화되지 않기 위해서는 서명값의 범위가 클 수 없다. 따라서, 비도가 높고 다양한 서명 패턴을 만들기 위해서는 이진 난수에 의해 원영상에 삽입되는 위치를 변화하는 방법밖에 없다. 따라서 서명값을 이용하는 대부분의 디지털 서명 방법들은 일차적으로 의사 난수를 발생한다. 두 번째로, 발생된 이진 의사 난수에 따라 서명값을 원영상에 삽입한다. 삽입하는 방법은 대부분이 XOR의 연산자를 이용한다[9][11][12]. 한편, 스탬프는 그림 4. (a)와 같은 이진 영상을 이용하는 경우이다. 이진 영상의 스탬프를 S라 하고, 원영상을 I라고 하면, 그림 4. (b)와 같은 서명 영상 Is는 아래와 같이 얻어진다[13].

$$I_s = I \oplus S$$

이렇게 얻어진 서명 영상 I_s를 이용자에게 전송하고, 필요한 경우는 다시 스탬프를 서명 영상에서 추출하여 인증을 하게 된다.

$S=I_s \oplus I=(I \oplus S) \oplus I$

3.2.2 서명 문양의 검출

디지털 영상은 그 정보량이 매우 크므로 영상의 저장이나 전송을 위해서는 반드시 압축 과정을 거친다. 압축 방법은 사용자의 목적과 정보의 중요도에 따라 다양한 방법을 이용할 수 있지만, 일반적으로 압축률이 높은 손실 압축(Lossy compression)의 방법을 가장 널리 이용한다. 손실 압축 방법은 영상을 압축(Compression)/신장(Decompression) 과정에서 원영상 정보에 필연적인 손실을 준다. 압축 손실은 영상 데이터 자체에는 많은 변화를 가져오지만 낮은 압축률에서는 실제 시각적으로 구별되지 않는다. 하지만, 영상 데이터의 미세한 변화를 이용하는 서명 문양 방법에서는 매우 치명적인 약점이 된다. 때문에, 서명값을 이용하는 디지털 서명은 압축 환경에 대응하기 위해 서명값 검출을 위해 확률적 방법을 사용한다. 그 대표적인 예가 가설 검증 (Hypothesis Testing) 이론을 이용하는 경우다[9][10]. 또는, 서명값 발생시 자기 상관성(auto-correlation)을 갖는 서명값을 만들어 압축에 의해 손상되는 서명값을 복구하는 방법을 사용하는 경우다[11]. 이처럼 서명값을 이용하는 디지털 서명은 압축 환경에 대한 대비책을 가지고 있다. 그림 3. (b)는 삽입된 서명값을 검출하는 일반적인 알고리즘이다. 그림에서 Test Digital Image는 서명 영상(Signed image)을 의미한다. 한편, 스탬프를 이용하는 경우도 물론 압축 환경에 많은 영향을 받지만, 서명값을 이용하는 경우와는 달리 스탬프의 형태로 서명 확인을 하므로 압축 손실의 영향에 좀 덜 민감하다고 할 수 있다. 그림 4. (b)는 스탬프가 삽입된 서명 영상을, 그림 4. (c)는 검출된 스탬프를 보여준다.

3.2.3 동영상에서의 서명 문양

일반적으로 현재까지 소개된 서명 문양은 정지 영상을 대상으로 검증된 방법들이다. 하지만, 서명 문양은 동영상에 적용도 큰 어려움 없이 가능하다. 즉, 매 프레임마다 연산된 서명 문양을 삽입하고, MPEG-2와 같은 압축 방법으로 압축하여 전송하거나 저장하게 된다. 동영상의 경우 고전적인 디지털 서명에 비해 서명 문양에 의한 디지털 서명 방법은 연산 과정이 단순하므로 실시간 처리가 가능하고, 투명성(transparency)이나 전송률 호환성(transcodability)에 대해서도 큰 문제가 없다. 즉, 고전적인 디지털 서명 기법들은 주로 문자 정보를 대상으로 하여 동영상에 적용하기에는 단점이 있었지만, 서명 문양에 의한 디지털 서명은 영상 정보를 목적으로 만들어진 서명 방법으로 동영상과 같은 실시간 처리가 중요시되는 환경에서 매우 바람직한 서명 방법이다.

Ⅳ. 결론

지금까지 본 고에서는 제한 수신 시스템에서 정보 보호를 위한 스크램블링, 인증과 암호화 기법에 따른 디지털 서명 기법을 살펴보았다. 또한, 새로운 디지털 서명 방법으로 서명 문양을 이용하는 방법에 대해서도 간략히 살펴보았다. 기존의 암호화 방식에 의한 디지털 서명 기법을 디지털 방송에서 이용하기에는 이미 설명하였듯이 실시간 처리 문제, 또는 투명성과 전송률 호환성 문제 등 때문에 어려움이 있다. 하지만 차세대 서명 방법인 서명 문양을 이용하면 이와 같은 어려움은 해결할 수 있을 것이다. 물론, 서명 문양에 의한 서명 방법에도 몇 가지 해결해야할 문제점이 남아있다. 그 중 하나가 압축 환경에서 발생되는 압축 또는 양자화 손실을 어떻게 극복하는가 하는 문제이다. 이 문제의 해결책으로 제시된 것은 확률적인 서명 문양의 검출[9][10]이나, 자기 상관성의 이용[11], 또는 영상의 블록 특성을 이용하는 방법[10] 등 여러 가지 해결책이 제시되고 있다. 이 밖에 나타나는 문제점은 서명 문양의 비화도이다. 삽입된 서명 문양이 시각적으로 드러나지 않아야 한다는 조건 때문에 서명 문양은 다양한 서명 패턴을 이룰 수 없다. 하지만, 이와 같은 문제 역시 서명 삽입을 위한 난수 발생[9][10]이나, 스탬프와 같은 또 다른 이진 영상을 이용하면 충분히 해결할 수 있는 문제이다.

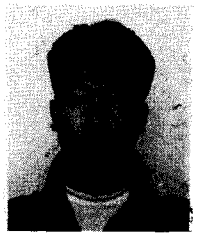
지금까지 살펴본 서명 문양에 의한 디지털 서명 방법은 차후 멀티미디어 네트워크 환경이나 디지털 방송 환경에서 영상의 저작권을 보호하는 방법으로 이용하기에 충분하다고 할 수 있다.

참고 문헌

1 D. Angebaud, J-L Giachetti, "Conditional Access Mechanisims for All Digital Broadcast Signals", IEEE Trans. on Consumer Electronics, Vol38, No.3, pp.88-194, 1992

2. F. Baylin, R. Maddox, J. McCornac, "World Satelite TV and Scrambling Methods", Baylin Publication, 1991
3. 권 정익, 원 치선, "다기능을 갖는 영상 스크램블링", 제7회 신호처리 합동 학술대회 논문집, Vol.7, No. 1, pp.638-641, 1994
4. Benoit M. Macq, Jean Jacques Quisquater, "Cryptology for digital TV broadcasting", Proceedings of IEEE, Vol.83, No.6, pp.944-957, 1995
5. 안 효범, 박 창성, "메세지 체인 방식에 의한 인증 알고리즘", 통신정보보호학회지, Vol.3, No.4, pp.24-37, 1993
6. 이 아란, 송 주석, "디지털 서명에 관한 고찰", 통신정보보호학회지, Vol.3, No.1, pp.32-41, 1993
7. 강 찬구, 김 대영, "디지털 다중 서명 방식", 통신정보보호학회지, Vol.2, No.4, pp.7-17, 1992
8. Man Young Rhee, "Cryptography and Secure Communications", McGraw-Hill Book Co., 1994
9. N. Nikolaidis, I.Pitas, "Copyright protection of images using robust digital signatures", Proc. pf ICASSP-96, pp.2168-2171, May 7-10, Atlanta, GA
10. 서 정일, 우 석훈, 원 치선, "영상 블록 특성을 이용한 디지털 서명 기법", 제9회 신호처리 합동학술대회 논문집, Vol.9 Part 1, pp.653-656, 1996
11. Raymond B. Wolfgang, Edward J. Delp, "A watermark for digital images", ICIP-96, Vol. 3, pp.219-222, 1996
12. Steve Walton, "Image authentication for a slippery new age", Dr. Dobb's Journal, pp.18-26, April, 1995
13. Chiou-Ting Hsu, Ja-Ling Wu, "Hidden signatures in images", ICIP-96, Vol.3, pp.223-226, 1996

필자소개



서 정 일

1996. 1 동국대학교 전자공학과 학사
1996. 3 ~ 현재 동국대학교 전자공학과(석사 과정)
주관심분야 : 영상 정보 보호, 암호화, 디지털 방송 등

우 석 훈

1995. 2 동국대학교 전자공학과 학사
1996. 3 ~ 현재 동국대학교 전자공학과(석사 과정)
주관심분야 : 영상 정보 보호, 암호화, 디지털 방송 등

원 치 선

1982. 2 고려대학교 전자공학과 학사
1986. 매사추세츠대학 석사
1990. 매사추세츠대학 전기 컴퓨터공학과 박사
1989 ~ 1992 금성사 선임연구원
1992 ~ 현재 동국대학교 전자공학과 부교수
주관심분야 : 영상 분할 기반 영상 압축, 비디오 정보 보호 및 전송 시스템

이 춘

1981. 2 연세대학교 전자공학과 학사
1986. 8 미국 Virginia. 석사
1990. 12 미국 Virginia. 박사
1991. 1 ~ 현재 LG 전자 근무
현재 LG 멀티미디어 연구소 BDS 팀장(책임연구원)
주관심분야 : HDTV, DBS, Digital VCR 및 영상 압축 관련 기술

김 영 길

1974. 2 한양대학교 전자공학과 학사
1976. 2 한국 과학원 전기/전자공학과 석사
1988. 2 한국 과학원 전기/전자공학과 박사
1976. 2 ~ 현재 LG 전자 근무
현재 LG 멀티미디어 연구소 New AV Group 장(연구위원)
주관심분야 : VCR, HDTV, DBS, Digital VCR 및 디지털 방송 관련 기술