通信情報保護學會論文誌
第 7 卷 第 2 號, 1997. 6

FAX 문서에 대한 DM 합성 알고리즘을 이용한 디지털 서명의 제안

박 일 남*, 이 대 영**

A Proposal On Digital Signature For FAX Document Using DM Algorithm

Il-Nam Park, Dae-Young Lee

요 약

본 논문에서는 FAX문서에 직접 서명을 실행하는 디지털 서명 방식을 제안한다. 서명 비트를 합성하기 위해 기주사된 복수개의 참조 주사선중 키에 의해 선택된 주사선의 변화화소와 부호화 주사선의 변화화소의 거리의 우기성을 이용하여 합성 비트열에 따라 거리를 신축조작하는 합성 알고리즘을 제안한다. 앞서 제시한 방식에 비해 서명의 확산이 가능하므로 부분 서명에 의해 문서 전체에 대한 서명이 구현되어 서명 속도가 개선되며 합성 전제조건의 제거로 합성 가능량이 증가한다. 또한 제안하는 디지털 서명구조에 의해 디지털 서명의 제 3 조건인 송신 부인 봉쇄를 구현한다. 디지털 서명된 송신 문서는 원 문서와 시각적으로 구분이 어려워 제 3자에게는 통상의 문서 교환으로 인식될 것이다.

Abstract

This paper presents a digital signature scheme for facsimile document which directly embeds a signature onto the document. We use multiple reference lines which have been scanned just before and modify each distance of changing pels both on the reference line specified by key and on the coding line with a single bit of the signature data. The time to take in signature is reduced by spreading of signature. Non-repudiation in origin, the 3rd condition of digital signature is realized by proposed digital signature scheme. The transmitter embeds the signature secretly and transfers it, and the receiver makes a check of any forgery on the signature and the document. This scheme is compatible

* 경희대학교 박사과정, 충남전문대학 조교수

* * 경희대학교 교수

with the ITU-T.4(CCITT G3 or G4 facsimile standards). The total amount of data transmitted and the image quality are about the same to that of the original document, and thus a third party notices that no signature is embedded on the document.

1. 서 론

최근 FAX 통신으로 대표되는 문서화상 통신이 상업용 뿐 아니라 가정용으로 까지 광범위하게 보급되고 보급율 또한 급속히 증가하고 있으며, 통신량의 증가 뿐 아니라 이용목적도 다양화되고 있고 내용 자체도 단순 문서교환에 머물지 않고 부가가치가 높고 비밀을 요구하는 정보의 교환에까지 이르고 있다.[1]

이와 같이 폭넓은 정보전달 수단으로써 필수불가결한 FAX 통신이지만 송수신 문서의 정당성을 인증하기가 곤란하다는 단점이 있다. 예를 들어, 본래의 아날로그 패턴인 자필의 사인이나 도장에 의해서 날인한 중요문서를 단순히 MH(Modified Huffman), MR(Modified Read)혹은 MMR(Modified Modified Read)부호화하여 FAX 송신할 경우 불법적인 제3자에 의한 문서의 위조에 의해 문서의 정당성을 인증(Authentication)할 수 없다.[3, 4] 또한 송수신자의 이해 관계가 걸려있는 민감한 문서의 경우 수신자가 문서를 받은 사실을 부인하는 수신자 부인봉쇄(Non-repudiation,Delivery)나 송신자가 문서의 송신 사실을 부인하는 송신자 부인봉쇄(Non-repudiation,Origin)[3]등도 해결할 수 없다. 이와같은 데이타의 무결성을 확인하는 정보의 인증(Data authentication)과, 정보를 교환하는 상대방을 확인하는 사용자의 인증(User authentication)을 위해 디지털 서명(Digital signature)이 사용되고 있으며 그 실현 방법으로 RSA(Rivest Shamir & Adleman) 암호 기법(cryptographic scheme)등이 효과적으로 이용된다.[12]

그러나 FAX 문서의 경우 데이터량이 많아 문서 전체에 RSA 알고리즘등을 적용해 서명을 시행할 경우 속도상에 문제가 있고 암호화된 사실을 확인할 수 있어 공격의 대상이 될 수 있으며 해쉬(Hash)함수를 적용해 문서의 축약부분에 대해 서명을 시행한다해도 FAX 문서의 특성상 이를 전송 문서와 별도로 전송할 수 없기 때문에 이를 해결할 수 있는 방법이 요구된다. 종래의 데이타 통신에 있어서는 그 인증방식으로써 다수의 서명 방법이 제안되어 있으나,[2, 3, 4] FAX 문서에 대한 서명은 데이터 통신의 인증법을 그대로 적용할 수도 없고 그 특수성으로 인해 연구가 미비한 상태이다. 우리는 앞서 이에 대한 연구의 일환으로 부호장의 우기성을 이용한 디지털 서명법을 제안한 바 있다.[7, 8]그러나 이 방식은,

1) 문서 전체에 대한 인증을 위해 전체 문서에 서명문을 합성하여야 하며
2) 문서 전체를 스크램블하기 위해 문서량만큼의 메모리가 필요하고
3) 디지털 서명의 3 조건중 S 조건을 해결할 수 없어 부득이 중재자(Arbitrator)서명 방식[11]의 적용이 불가피하다는 단점을 갖고 있다.

따라서 본 논문에서는 이러한 문제점을 해결하는데 초점을 맞추어 비트 합성 알고리즘을 개선하고 서명 시스템을 수정 보완하였다. 비트 합성 알고리즘은 부호화 주사선(Coding Scan Line : 이하 CSL)과 키에 의해 선택된 참조 주사선(Reference Scan Line : 이하 RSL)의 변화화소사이의 거리(Distance)의 우기성(Even-Odd Feature)을 이용하여 서명 비트를 합성하는 것으로 이를 이용하면,

1) 문서의 일부분에의 서명이 문서 전체에 확산되고

2) 스크램블 과정이 불필요하여 논문[7, 8]의 방식보다 고속의 서명이 가능하며
3) 비도(Crypto-degree)면에서 개선되어 보다 안전성을 확보할 수 있다.

또한 앞의 3)을 해결하기 위해 본 논문에서 제안하는 DM 알고리즘과 함께 DES 알고리즘 및 RSA 알고리즘을 적용한 디지털 서명 구조를 제안한다.

2. FAX 문서의 특징 및 DM 알고리즘

2.1 FAX 문서의 특징 및 디지털 서명의 조건

ITU-T Recommendation T.4, T.6(종전에는 "CCITT Recommendation T.4, T.6)[5, 6, 9, 10]에 의하면 ISO A4, ISO B4, ISO A3 규격의 표준 모드에서의 수직방향의 해상도는 3.85 line/mm ±1%이고 선택적 고해상도의 경우 7.7 line/mm ±1%이다. 또한 표준 모드의 경우 수평 방향으로 215mm±1%의 주사선에 1728개의 화소가 있어서 약 8 pel/mm의 수평해상도를 갖고 고해상도의 경우 약 2배 가까이 된다. 따라서 표준 모드의 경우 1화소가 차지하는 길이는 약 0.12-0.13mm정도로 극히 미세하다. 따라서 1비트 정도의 증감에 의해 문서의 화질이 그리 저하되지 않아 문서상에 어떠한 변화가 있음을 판독하기는 어렵다. 따라서 이를 이용하면 시각적인 차이 없이 문서상에 디지털 서명을 시행할 수 있다. 이때 디지털 서명은 안전성(Security)의 관점에서 다음과 같은 3가지 조건을 만족하여야 한다.

- [T]조건[11, 12] : 서명문의 제 3자(Third party)에 의한 위조 방지
- [R]조건[11, 12] : 서명문의 수신자(Reciever)에 의한 위조 방지
- [S]조건[11,12] : 송신자(Sender)의 송신 부인 봉쇄

여기서 [T]조건은 악의의 제3자가 송신 문서를 도청해 이를 해독하여 내용을 바꾸거나 삭제하는 것을 방지하는 것이고 [R]조건은 문서를 수신한 수신자가 자신에게 유리하도록 수신 문서의 내용을 위조하는 것이며 [S]조건은 문서를 송신한 송신자가 자신의 불이익을 막기위해 문서를 송신한 사실을 부인하는 것을 방지하는 것이다. 이러한 조건을 전제로 FAX문서에 서명을 시행할 경우 동일 매체상에 서명이 이루어져야 하는 특수성이 있다. 만일 FAX문서와 서명이 분리되어 전송된다면 제3자나 수신자에 의한 문서의 위조를 피할 수 없다.

따라서 상기한 FAX문서의 특징과 상기조건 그리고 FAX문서의 서명의 특수성을 고려하여 문서상에 서명을 시행하는 방법을 제안한다.

2.2 디지털 서명을 위한 비트합성 알고리즘

2.2.1 RM 합성 알고리즘(Runlength Mixing Algorithm : 이하 RM 알고리즘)[7, 8]

그림1의 부호화 주사선의 변화화소에 대해 다음과 같이 정의한다.

a_0 : 부호화 주사선의 개시 변화화소. 즉, 부호화 RL 최초의 화소
a_1 : 부호화 주사선에서 a_0의 우측에 있는 다음의 변화 화소
a_2 : 부호화 주사선의 a_1의 우측에 있는 다음의 변화 화소

이들 변화화소를 이용해서 a_2, a_j간의 부호장을 RL(a_i, a_j)로 쓰기로 하고 그림2의 백RL과 흑RL이 짝수인가 홀수인가에 따라 전송하고자하는 서명데이타의 비트열을 합성부호화한다. RL이 짝수일 경우 서명문으로부터 1비

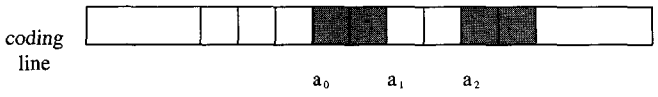


그림 1. 변화화소의 정의

트를 취해 그 값이 "1"이라면 화소 a_1을 1화소 우측으로 이동하고 "0"이라면 그대로 둔다. RL이 홀수라면 합성할 데이타 1비트를 취해 그 값이 "0"이라면 a_1을 1화소분 좌로 이동하고 "1"이라면 그대로 둔다. 위의 방법으로 합성된 비트를 수신측에서는 다음과 같이 복호화한다. RL(a_0, a_1)이 짝수라면 합성비트 "0"을 추출하고 RL(a_0, a_1)이 홀수라면 합성비트 "1"을 추출한다.

RM 합성 및 추출 알고리즘을 정리하면 다음과 같다.

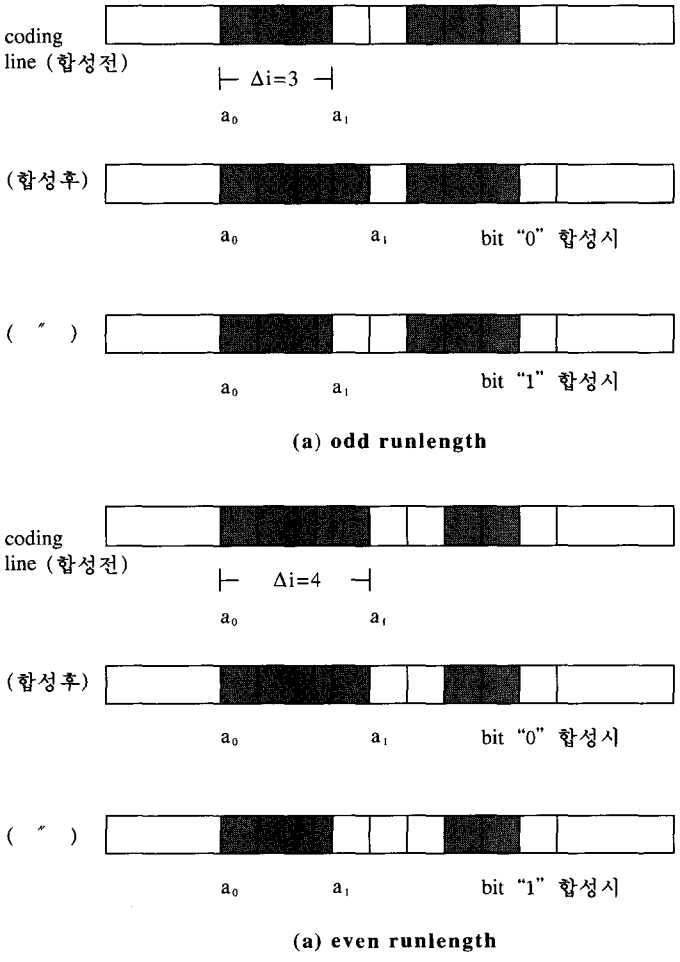


그림 2. 서명데이타 합성 방법

합성 알고리즘

```
START:
    S=Acquire 1 bit from signatures
      if(RL(a0, a1)=even)
          then if(S=1)
              then
                  a1<-(one pel left)
            else if(S=0)
                  NO OPERATION
      else if (RL(a0 ,a1)=odd)
          then if (S = 0)
              then
                  a1->(one pel right)
            else if(S=1)
                  NO OPERATION
```

추출 알고리즘

```
if(RL(a0, a1)=even)
    OUTPUT SIGNATURE BIT "0"
else
    OUTPUT SIGNATURE BIT "1"
```

예외 조건(그림 3)

i) $RL(a_0, a_1)=1$일때 a_1을 합성에 의해 좌측으로 이동시키는 것은 불가
(따라서 $RL(a_0, a_1)>1$)

ii) $RL(a_0, a_1)$이 우수일때 $RL(a_1, a_2)=1$이라면, 합성에 의해 a_1을 우로 이동하는 것은 불가(따라서 $RL(a_1, a_2)>1$)

RM 알고리즘은 제3자가 알고리즘을 알고 있을 경우 단순히 우기성을 판별하여 서명문을 추출할 수 있고 서명문에 따라 합성을 전체적으로 확산시키기 위해 원문서를 스크램블해야 하므로 문서 데이터량 만큼의 메모리가 소요되고 문서정보 전체를 인증하기 위해 문서 전체에 서명을 합성해야 하므로 서명속도가 느리다는 단점이 있다.

2.2.2 DM 알고리즘(Distance Mixing Algorithm : 이하 DM 알고리즘)[15]의 제안

DM알고리즘은 RSL상의 변화화소와 CSL상의 변화화소와의 거리(Distance)의 우기성

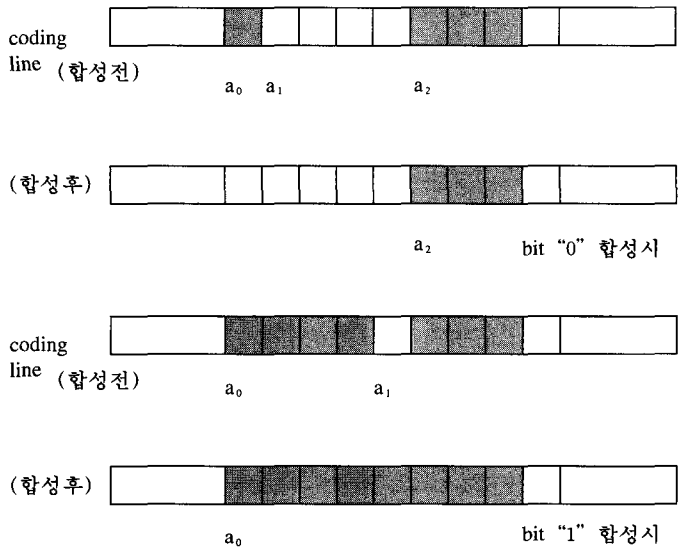


그림 3. 예외 조건

(Even-Odd Feature)을 이용해서 그 우기성과 서명 데이타의 비트열에 따라 그 거리를 신축 조작함으로써 합성을 시행한다.[15] 이때 CSL은 기주사된 n_{ab}개의 주사선을 이용하고 그 선택은 송수신자간의 비밀 공통키에 의해 이루어짐으로써 서명의 확산과 서명의 보안을 구현할 수 있다. 주사가 끝난 n_{ab}개의 주사선을 메모리에 저장해 놓고 이중에서 비밀키에 의해 i 번째의 주사선을 선택한다. 결국 이 RSL상의 변화화소와 CSL상의 변화화소간의 거리의 우기성으로 서명 데이타를 합성하는 것이다.

우선, CSL과 n_{ab}개의 RSL의 변화화소, 변화화소간의 거리 및 그 우기성에 관해서 다음과 같이 정의한다.

a_1 : CSL상의 주목 RL(Runlength) 최초의 변화 화소

$b_1^{(i)}$: 제 i RSL상의, a_1에 대응한 a_1과 동일한 색의 변화화소. 즉 a_1 좌측에 있는 RL의 최초의 화소

Δi : 변화화소 a_1과 $b_1^{(i)}$ 사이의 거리

ϕi : Δ_i의 우기성을 나타내며, Δ_i가 짝수라면 0, Δi가 홀수라면 1로 한다.

DM 알고리즘을 이용한 합성 예는 그림 4와 같다.

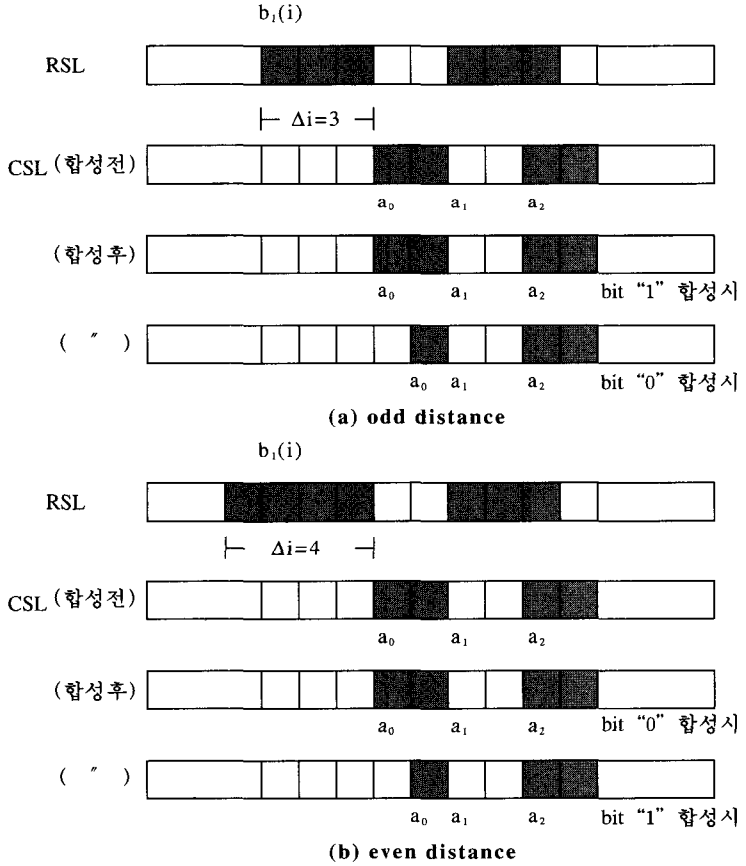


그림 4. 비트 합성 방법

DM알고리즘을 유도하기 위해 각 처리기능을 다음과 같이 정의한다.

f_1 : distance를 그대로 유지

f_2 : distance를 반전 → a_0 위치를 한화소 우측으로 이동

f_3 : distance를 반전 → a_1 위치를 한화소 우로 이동후 a_0를 한 화소 우로 이동

Δ_i의 우기성 ϕ_i와 합성 비트 S의 각각의 경우에 대한 처리를 진리표로 보면 표 1과 같다.

DM 알고리즘의 경우 f_2, f_3 처리후 실행전후의 RSL상의 직상화소가 바뀌어 $b_1(i)$의 위치가 수신측에서 오판되어 합성 비트 추출시 오류가 발생한다. 이 경우 그림 5와 같이 보정처리를 시행한다.

ϕ_i	s	ϕ_i	비 고	f
0	0	0	ϕ_i를 그대로	f_1
0	1	1	ϕ_i를 반전	f_2
1	0	0	ϕ_i를 반전	f_2
1	1	1	ϕ_i를 그대로	f_1

표 1. 각 경우의 처리에 대한 진리표

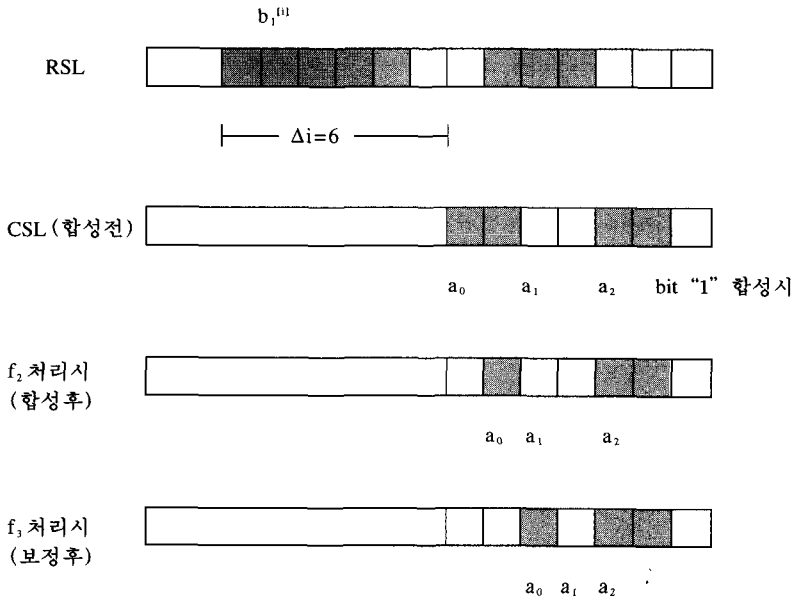


그림 5. 예외 보정처리

DM 합성 및 추출 알고리즘을 정리하면 다음과 같다.

합성 알고리즘

```
START :
    if(RL(a0, a1)≠1)
      then
          if(φi⊕S=0)
                process f1(no operation)
      elseif(φi⊕S=1)
                process f2(a0->)
                goto   REV
       elseif(RL(a0, a1)=1)
          if(φi⊕S=0)
                process f1(no operation)
       elseif(φi⊕S=1)
                process f3(a1->, a0 ->)
                goto   REV
REV :
    if(φi'=0 AND S=1)
      then
                process f3(a1->, a0->)
      else
                NO OPERATION
END:
```

추출 알고리즘

```
START :
    if(φi=0)
      OUTPUT SIGNATURE BIT "0"
    elseif(φi=1)
      OUTPUT SIGNATURE BIT "1"
END:
```

이와 같이 n_{ab}개의 주사선에 의존하도록 서명 데이타를 합성하면, 1개의 변화화소 a_0에 n_{ab}개의 우기성 계열 $\psi(\phi_1, \phi_2, \cdots, \phi n_{ab})$이 존재하게 되어서 만일 제3자나 수신자가 문서를 위조한 때, 문서상의 변화화소 a_0에 대해 계열 ψ를 만족시키는 것은 극히 곤란하게 된다.

DM 알고리즘은 합성시 전제조건이 없어 합성 가능량이 저하되지 않으며 문서의 일부분에의 서명 합성이 문서상의 다른 영역으로 확산되어 문서의 일부분에만 합성하면 족하므로 서명 속도가 개선된다.

3. DM 알고리즘을 이용한 디지털 서명 알고리즘

3.1 디지털 서명 알고리즘

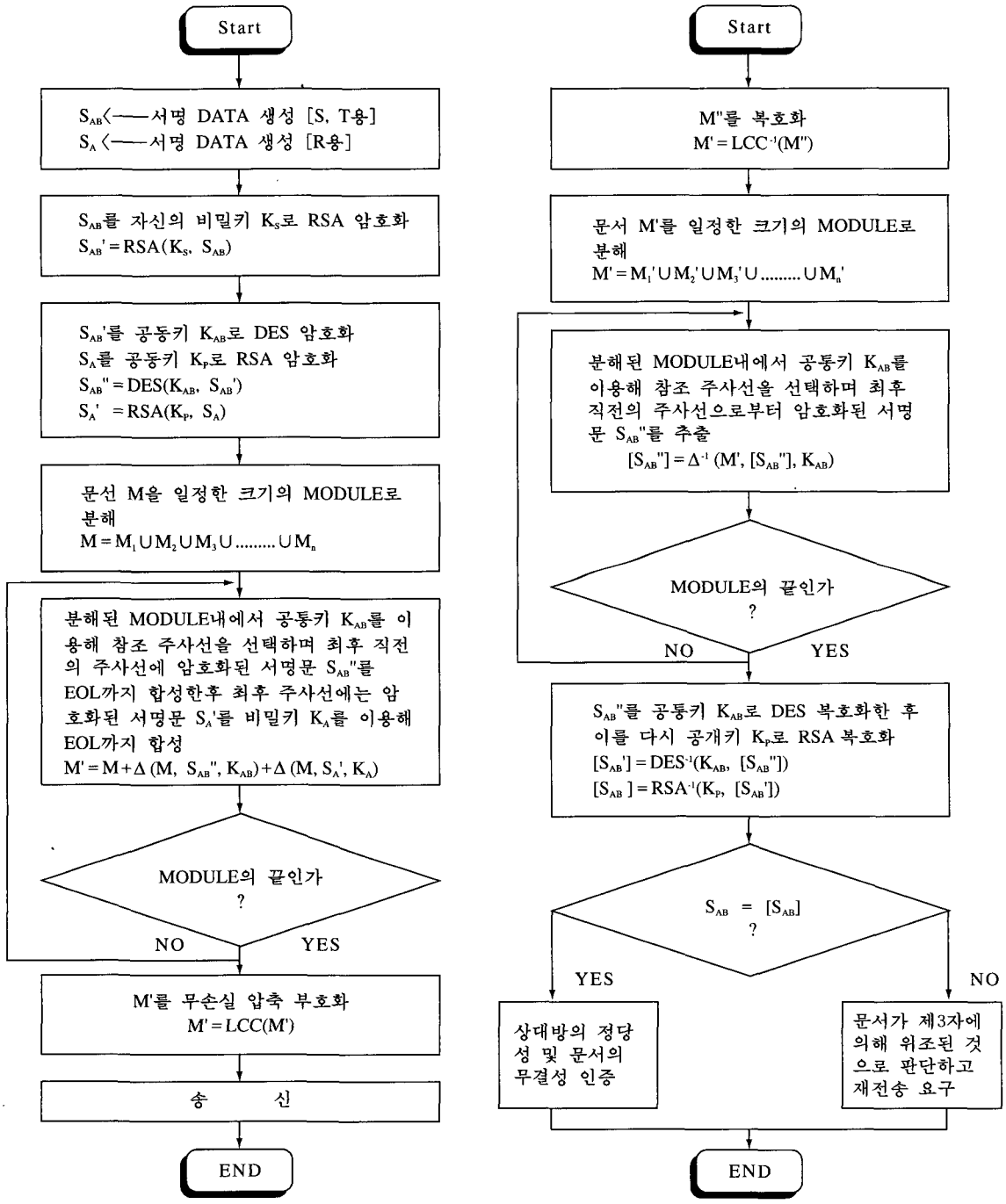
2.1절에 제시된 디지털 서명의 조건을 만족하는 DM 알고리즘을 이용한 서명 알고리즘을 그림 6에 제안한다. 이는 DM 알고리즘의 특성을 이용하여 문서의 일부분에만 서명을 시행하여 서명 속도를 높였고 RSA 알고리즘을 적용하여 논문 [7, 8]의 문제점인 디지털 서명의 [S]조건을 해결하였다.

우선 송신자 A는 S, T용의 서명 데이타 S_{AB}와 R용의 서명 데이타 S_A를 생성하여 이의 보안을 위해 각각 키(Key) K_S와 , K_{AB} 및 K_P를 이용해 암호화한다.

$$S'_{AB} = RSA(K_S, S_{AB})$$
$$S''_{AB} = DES(K_{AB}, S'_{AB})$$
$$S'_A = RSA(K_P, S_A) \quad \text{----------(3-1)}$$

여기서 RSA(Rivest Shamir & Adleman) 암호[12, 16]는 공개키 암호 방식이고 DES(Data Encryption Standard)[12, 13, 14]는 공통키 암호 방식이다. K_{AB}는 A, B간 비밀 공통키(Secret Common Key)이고 K_S는 RSA방식에서의 A의 비밀키(Secret Key), K_P는 A의 공개키(Public Key)이다. 그후 A는 문서 M을 B와 사전에 약속된 크기의 모듈(Module)로 분해한다.

$$M = M_1 \cup M_2 \cup M_3 \cup \cdots \cup M_n \quad \text{-----(3-2)}$$



a) 송신측 처리 b) 수신측 처리

그림 6 DM 알고리즘을 이용한 디지털 서명 알고리즘

분해된 모듈 단위로 각 모듈의 최후주사선 직전의 주사선을 찾아 DM 알고리즘(이하 수식에서는 Δ로 표기)을 이용해 그 주사선의 처음부터 끝까지(EOL) 암호화된 S, T용의 서명 데이타 S''_{AB}를 키 K_{AB}를 이용해 합성한 후 최후 주사선에는 EOL까지 암호화된 R용의 서명 데이타 S'_A를 자신의 비밀키 K_A를 이용해 합성한다.

$$M'=[M_1+\Delta(M_1, S''_{AB}, K_{AB})+\Delta(M_1, S'_A, K_A)] \cup [M_2+\Delta(M_2, S''_{AB}, K_{AB})+\Delta(M_2, S'_A, K_A)] \cup \cdots\cdots + \cdots\cdots \cup [M_n+\Delta(M_n, S''_{AB}, K_{AB})+\Delta(M_n, S'_A, K_A)] \quad (3\text{-}3)$$

송신자 A는 디지털 서명된 문서 M'를 MH, MR, 또는 MRR로 무손실 압축부호화(Lossless Compression Coding : 이하 LCC)하여 이를 수신자 B에게 송신한다.

$$M''=LCC(M') \quad (3\text{-}4)$$

수신자 B는 M''를 수신하여 복호화하여 디지털 서명된 문서 M'를 구한다.

$$M'=LCC^{-1}(M'') \quad (3\text{-}5)$$

다음은 디지털 서명된 문서 M'을 송신자 A와 사전에 약속된 크기의 모듈로 분해한다.

$$M'=M'_1 \cup M'_2 \cup M'_3 \cup \cdots \cup M'_n \quad (3\text{-}6)$$

이어 분해된 모듈단위로 각 모듈의 최후 주사선 직전의 주사선을 찾아 그 주사선의 처음부터 EOL까지 합성되어 있는 암호화된 S, T용의 서명 데이타 $[S''_{AB}]$를 추출한다.

$$[S''_{AB}]_1=\Delta^{-1}(M_1, [S''_{AB}]_1, K_{AB})$$
$$[S''_{AB}]_2=\Delta^{-1}(M_2, [S''_{AB}]_2, K_{AB})$$
$$\vdots$$
$$[S''_{AB}]_n=\Delta^{-1}(M_n, [S''_{AB}]_n, K_{AB}) \quad (3\text{-}7)$$

그 후 추출된 $[S''_{AB}]_1, [S''_{AB}]_2, \cdots, [S''_{AB}]_n$을 공통키 K_{AB}를 이용해 복호화한다.

$$[S_{AB}']_1=DES^{-1}(K_{AB}, [S''_{AB}]_1)$$
$$[S_{AB}']_2=DES^{-1}(K_{AB}, [S''_{AB}]_2)$$
$$\vdots$$
$$[S_{AB}']_n=DES^{-1}(K_{AB}, [S''_{AB}]_n) \quad (3\text{-}8)$$

이를 다시 A의 공개키 K_p로 RSA복호화하여 $[S_{AB}]$를 구한다.

$$[S_{AB}]_1=RSA^{-1}(K_p, [S_{AB}']_1)$$
$$[S_{AB}]_2=RSA^{-1}(K_p, [S_{AB}']_2)$$
$$\vdots$$
$$[S_{AB}]_n=RSA^{-1}(K_p, [S_{AB}']_n) \quad (3\text{-}9)$$

수신자 B는 추출된 서명 $[S_{AB}]$와 본래의 서명 S_{AB}에 대해 다음의 경우 상대방을 인증함과 동시에 문서의 무결성을 인증한다.

$$(S_{AB}=[S_{AB}]_1) \text{ AND } (S_{AB}=[S_{AB}]_2) \text{ AND } \cdots \text{ AND } (S_{AB}=[S_{AB}]_n) \quad (3\text{-}10)$$

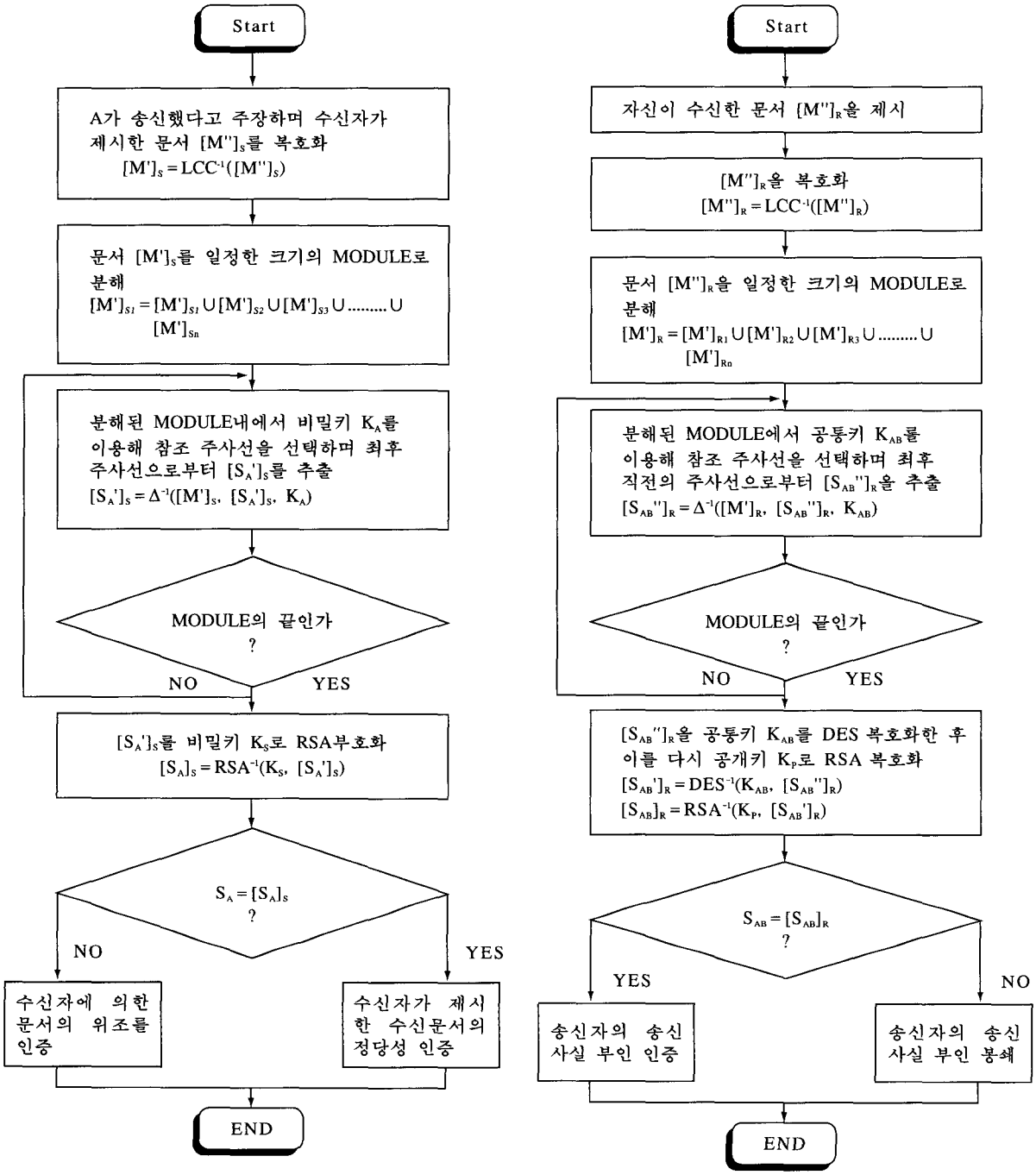
그러나 다음과 같은 경우 위조 부분을 검출함과 동시에 송신측에 재전송을 요구한다.

$$(S_{AB} \neq [S_{AB}]_1) \text{ OR } (S_{AB} \neq [S_{AB}]_2) \text{ OR } \cdots \text{ OR } (S_{AB} \neq [S_{AB}]_n) \quad (3\text{-}11)$$

3.2 분쟁시 처리

한편 송신자 A는 수신자 B가 문서를 위조하는 등의 문제 발생시 다음의 절차를 실행한다.(그림 7) B가 제시한 문서($[M'']_S$)에 대해 식(3-5), 식(3-6)을 시행한후 모듈의 최후 주사선에서 비밀키 K_A로 복호를 실행하여 R용의 서명 데이타 $[S'_A]_S$를 추출한다.

$$[S'_A]_{S1}=\Delta^{-1}([M']_{S1}, [S'_A]_{S1}, K_A)$$
$$[S'_A]_{S2}=\Delta^{-1}([M']_{S2}, [S'_A]_{S2}, K_A)$$
$$\vdots$$
$$[S'_A]_{Sn}=\Delta^{-1}([M']_{Sn}, [S'_A]_{Sn}, K_A) \quad (3\text{-}12)$$



a) 수신자 위조 인증 절차

b) 수신자 부인 봉쇄 절차

그림 7 분쟁시 처리 절차

추출된 $[S'_A]_{S1}$, $[S'_A]_{S2}$, · · · , $[S'_A]_{Sn}$를 A의 비밀키 K_S를 이용해 RSA 복호한다.

$$[S_A]_{S1}=RSA(K_S, [S'_A]_{S1})$$
$$[S_A]_{S2}=RSA(K_S, [S'_A]_{S2})$$
$$\vdots$$
$$[S_A]_{Sn}=RSA(K_S, [S'_A]_{Sn}) \quad \text{----------(3-13)}$$

송신자 A는 다음과 같은 경우 수신자 B의 위조를 인증한다.

$$(S_A \neq [[S_A]_{S1}) \text{ OR } (S_A \neq [S_A]_{S2}) \text{ OR}$$
$$\cdots \text{ OR } (S_A \neq [S_A]_{Sn}) \quad \text{-----(3-14)}$$

수신자는 수신 문서에 대해 송신자가 송신 사실을 부인할 경우 다음과 같은 절차를 밟는다.

우선 수신자는 자신이 송신자 A로 부터 수신했다고 주장하는 문서 $[M'']_R$을 제시하고 이로부터 디지털 서명된 문서 $[M']_R$을 복호한다.

$$[M']_R=LCC^{-1}([M'']_R) \quad \text{----------(3-15)}$$

다음은 디지털 서명된 문서 $[M']_R$을 송신자 A와 사전에 약속된 크기의 모듈로 분해한다.

$$[M']_R=[M']_{R1} \cup [M']_{R2} \cup [M']_{R3} \cup \cdots \cup [M']_{Rn} \text{---(3-16)}$$

이어 분해된 모듈단위로 각 모듈의 최후 주사선 직전의 주사선을 찾아 그 주사선의 처음부터 EOL까지 DM 알고리즘을 이용해 합성되어 있는 암호화된 S, T용의 서명 데이타 $[S''_{AB}]_R$을 추출한다.

$$[S''_{AB}]_{R1}=\Delta^{-1}([M']_{R1}, [S''_{AB}]_{R1}, K_{AB})$$
$$[S''_{AB}]_{R2}=\Delta^{-1}([M']_{R2}, [S''_{AB}]_{R2}, K_{AB})$$
$$\vdots$$
$$[S''_{AB}]_{Rn}=\Delta^{-1}([M']_{Rn}, [S''_{AB}]_{Rn}, K_{AB}) \text{----(3-17)}$$

그 후 추출된 $[S''_{AB}]_{R1}$, $[S''_{AB}]_{R2}$, · · · , $[S''_{AB}]_{Rn}$을 공통키 K_{AB}를 이용해 DES복호화한다.

$$[S_{AB}']_{R1}=DES(K_{AB}, [S''_{AB}]_{R1})$$
$$[S_{AB}']_{R2}=DES(K_{AB}, [S''_{AB}]_{R2})$$
$$\vdots$$
$$[S_{AB}']_{Rn}=DES(K_{AB}, [S''_{AB}]_{Rn}) \quad \text{----------(3-18)}$$

이를 다시 A의 공개키 K_p로 RSA복호화하여 $[S_{AB}]_R$을 구한다.

$$[S_{AB}]_{R1}=RSA(K_p, [S_{AB}']_{R1})$$
$$[S_{AB}]_{R2}=RSA(K_p, [S_{AB}']_{R2})$$
$$\vdots$$
$$[S_{AB}]_{Rn}=RSA(K_p, [S_{AB}']_{Rn}) \quad \text{----------(3-19)}$$

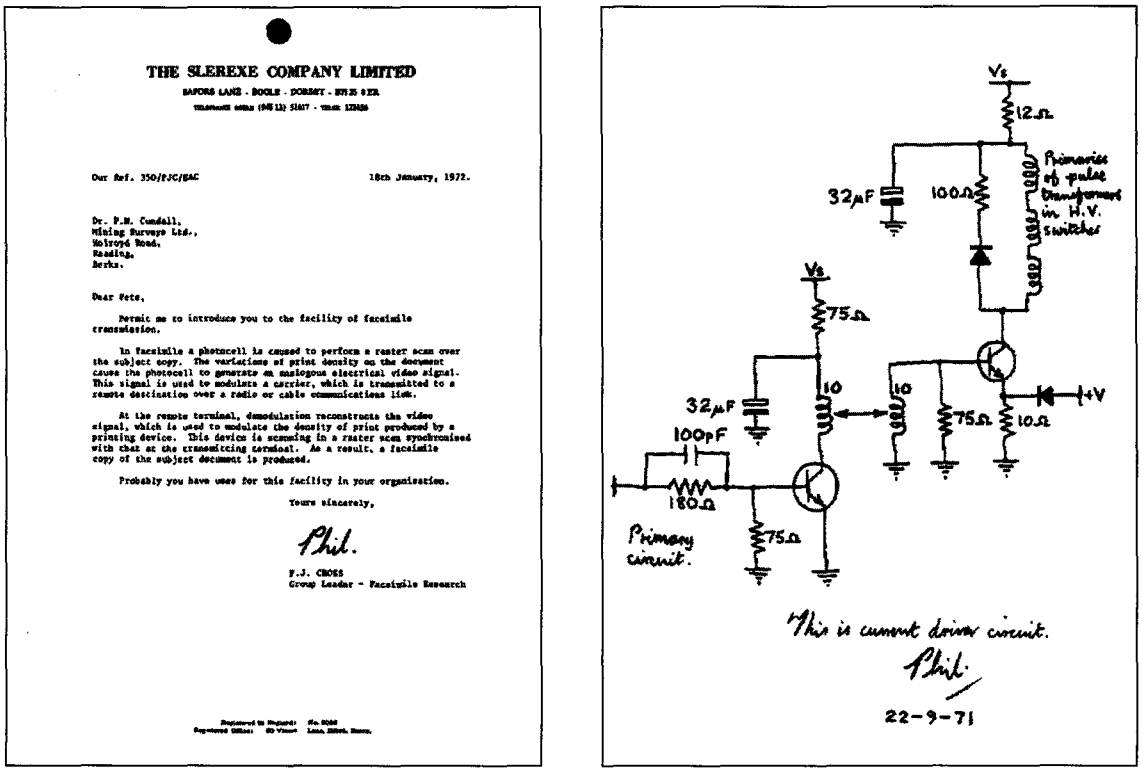
이때 $[S_{AB}']_R$은 송신자 A 자신의 비밀키에 의해 RSA 암호화된 것으로 A의 공개키 K_p에 의해서만 해독되므로 복호내용이 ,정상적인 경우 수신자가 제시한 문서 $(M'')_R$의 송신 사실을 부인할 수 없게 된다. 즉, 다음과 같은 경우 송신자의 송신 부인을 봉쇄할 수 있다.

$$(S_{AB})_1=[S_{AB}]_{R1} \text{ AND } (S_{AB})_2=[S_{AB}]_{R2} \text{ AND}$$
$$\cdots \text{ AND } (S_{AB})_n=[S_{AB}]_{Rn} \text{ -------(3-20)}$$

4. 실험 및 고찰

본 논문에서 제안된 알고리즘에 대한 모의실험은 ITU의 FAX용 TEST화상(1024×723)[8]인 CHART No1, No2 를 선택하여 PC상에서 실험을 행하였다. 실험 결과는 다음과 같다.

그림 10에서 보는 바와같이 원 문서 화상과 서명이 합성된 문서화상간의 시각적인 차이를 느낄 수 없어 비밀 서명이 가능한 것을 확인할 수 있었으며 그림 11에서 RM 알고리즘을 적용한 문서와 DM알고리즘을 적용한 문서중 RM을 적용한 쪽이 약간 화질이 나아 보이나 이는 확대 화상이므로 통상의 문서 교환시에는 차이가 거의 없을것이다. 표 2에서와 같이 앞서 발표한 RM 서명문 합성 방법과 비교하였을 때에 합성가능 데이터량이 NO1문서의 경우 약 45% NO2의 경우 약 4.5% 증가함을 확인하였다. 즉 문서가 복잡할수록 DM 알고리



THE SLEREXE COMPANY LIMITED

Our Ref. 350/PJC/EAC 18th January, 1972.

Dr. P.M. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROES
Group Leader - Facsimile Research

Vs
12Ω
Primaries of pulse transformer in H.V. switcher
32μF
100Ω
75Ω
10
+V
100pF
180Ω
Primary circuit.
This is current drive circuit.
Phil.
22-9-71

a) CHART No1 b) CHART No2

그림 8. ITU.T4 문서화상

서명 데이타 : DIGITAL SYSTEM LAB							
01000100	01001001	01000111	01001001	01100011	01000001	01010011	01100010
01101000	01100010	01100011	01000101	01010100	01010011	01000001	01000010

DES 암호화된 데이타							
11010110	01001011	00011101	00101101	00001001	11011111	01111100	10000111
01010111	00110110	01111110	01010100	10011111	11001001	01001011	10011111

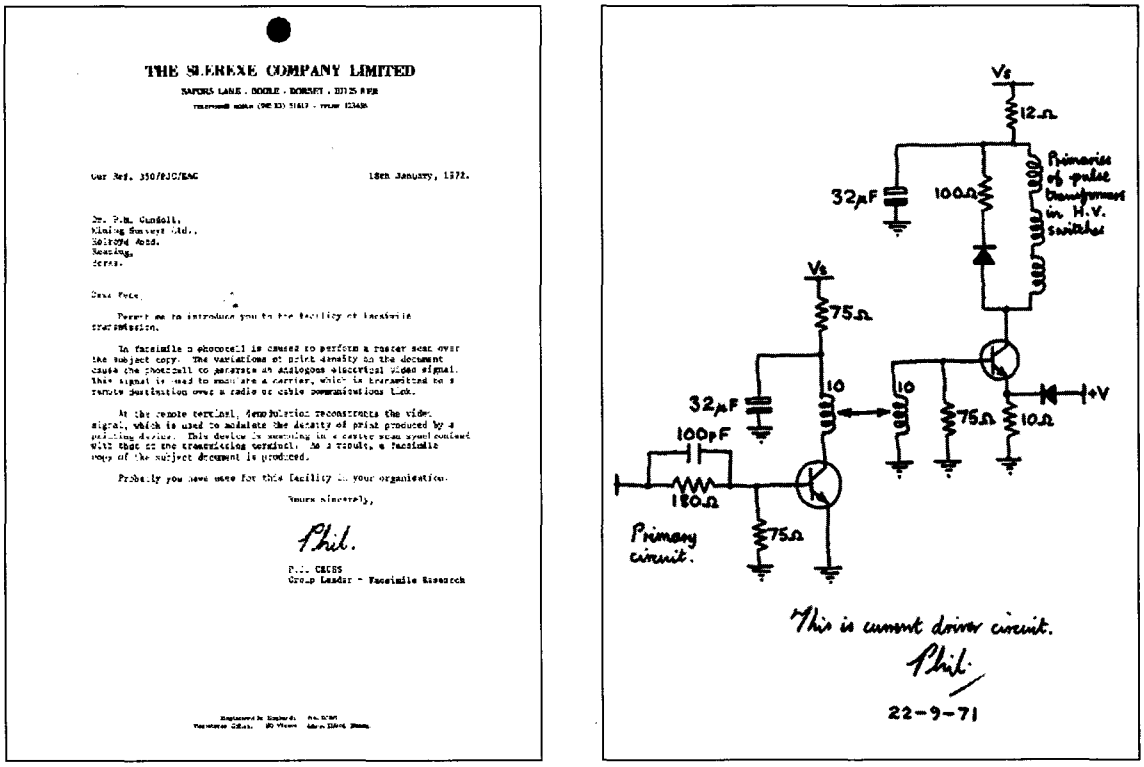
a) S, T용의 서명 데이타 및 암호화

서명 데이타 : PARK IL NAM
01010000 01000001 01010010 01001011 01001001
01001100 01001110 01000001 01001101

00001010 01001100 10000010 11000011 01001100
00001100 11101010 10111010 01010100

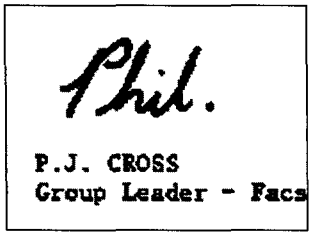
b) R용의 서명 데이타 및 암호화

그림 9. 서명 데이타의 암호화

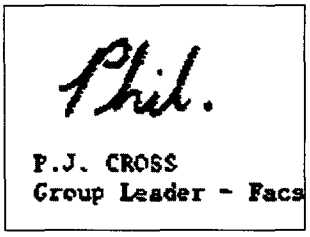


a) CHART No1 b) CHART No2

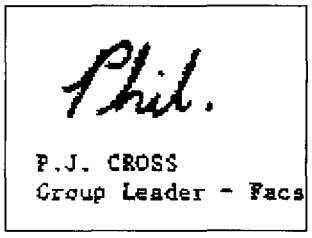
그림 10. 서명 데이타가 합성된 T.4 문서화상



(a) 원 문서 화상



(b) Paper[7, 8] 서명 문서



(c) DM 서명 문서

그림 11. 합성된 문서와의 비교

단위 : BIT

오동간적 / 합성알고리즘	M=1	M=3	M=5	M=10	M=20	M=40	평균 증가율
[No1] RM 합성법[7, 8]	6,188	2,082	1,264	716	353	210	
제안된 DM 합성법	9,243	3,110	1,855	1,065	556	300	45.%
[No2] RM 합성법[7, 8]	5,102	1,702	1,011	504	244	133	
제안된 DM 합성법	5,359	1,793	1,051	525	253	139	4.5%

표 2. 문서화상의 합성가능데이타량 비교(CHART No1, No2)

단위 : BIT

오동간적 / 합성알고리즘	M=1	M=3	M=5	M=10	M=20	M=40
RM 합성법 [No1]	178,812 (24.15%)	178,805 (24.15%)	178,803 (24.15%)	178,800 (24.15%)	178,802 (24.15%)	178,802 (24.15%)
제안된 DM 합성법 [No1]	181,374 (24.45%)	179,847 (24.29%)	179,308 (24.21%)	179,089 (24.18%)	179,008 (24.17%)	178,905 (24.16%)
RM 합성법 [No2]	107,625 (14.537%)	107,606 (14.534%)	107,612 (14.535%)	107,602 (14.533%)	107,592 (14.532%)	107,597 (14.533%)
제안된 DM 합성법 [No2]	107,886 (14.572%)	107,672 (14.543%)	107,633 (14.538%)	107,609 (14.535%)	107,602 (14.533%)	107,597 (14.533%)

원문서 : No1 FAX 문서화상 : 178.802 (24.15%)
No2 FAX 문서화상 : 107.597 (14.533%)
(1024×723=740,352)

표 3. MH 부호량의 변화

증의 합성량이 더욱 증가함을 확인하였다. 또한 표 3에 보인 바와같이 합성 전후의 전송 부호량의 변화가 약 0.3% 이내로 부호량의 증대에 따른 부하가 거의 없음을 확인하였다. 문서상의 서명이 해독될 확률을 비도(Crypto-degree)로 평가하면 다음과 같다. 문서 화상의 해상도를 (ixj)로 하고 모듈 수를 m이라하면 1개의 모듈내에는 i/m개의 주사선이 존재하게 되므로 1개의 모듈이 해독될 확률 P_{DM}은 다음과 같다.

$$(P_{DM})_m = i^{-(j+1)} * m^j \quad \text{----------(4-1)}$$

따라서 문서 전체가 해독될 확률 P_{DM}은 다음과 같다.

$$P_{DM} = (i^{-(j+1)} * m^j)^m \quad \text{----------(4-2)}$$

이때 보통 i>>m이므로 DM알고리즘을 해독하기 위한 시간 복잡도는 $O(n^k)$로 볼 수 있다. 반면 RM 알고리즘의 경우 해독을 위한 시간 복잡도는 O(n!)로 DM 알고리즘이 비도상에서 개선됐으므로 보다 안전함을 알 수 있다.

5. 결 론

FAX 문서 자체에 어떠한 수단으로 서명을 시행하여 제3자의 눈에는 보통의 문서와 다름없게 전송하는 디지털 서명방식은 상대방 및 문서에 대한 정당성을 인증할 수 있는 방법이다. 본 논문에서는 참조 주사선과 부호화 주사선의 변화화소의 거리의 우기성을 이용한 DM 합성 알고리즘을 제안하고 이를 이용하여 FAX 문서에 디지털 서명의 3 조건인 [T], [R], [S]조건을 만족하는 디지털 서명을 시행하는 알고리즘을 제안하였다. ITU의 TEST CHART를 대상으로 실험한 결과, DM 알고리즘은 기존의 RM 알고리즘에 비해 합성량을 증가시키고 비도상에서 시간 복잡도가 $O(n^k)$으로 매우 안전함을 확인하였다. 합성 전후 부호량의 변화가 거의 없어 합성에 따른 부하가 거의 없었고 합성 전후의 문서상에서의 뚜렷한 시각적 차이를 느낄 수 없어 제 3자에게는 통상의 문서 교환으로 인식될 것이다. 앞으로 디지털 서명 뿐아니라 비밀문서를 일반문서에 합성할 경우에 대한 연구가 필요할 것이며 이를 위해서는 보다 다량의 데이터를 합성할 수 있는 알고리즘을 개발해야할 것이다.

참 고 문 헌

[1] 小野, 浦野 : "アルチメデイア通信", 情報處理, Vol.24, No.10,pp.1227-1232 (昭 58-10)

[2] 池野, 小山 : 現代暗號理論, 電子通信學會, 第 12章, pp.217-239(昭 61)

[3] R. R. Jueneman, C. H. Meyer, and S.M.Matyas, "Message Authentication", IEEE Communications Magazine, vol.23, no.9, pp.29-40,Sept.1985

[4] Robert R.Jueneman, "Eletronic Document Authentication" , IEEE Network Magazine, vol.1, no.2, pp.17-23, April.1987

[5] CCITT Recommendation T.4 : Standardization of Group 3 facsimile apparatus for document transmission,Red Book.1984

[6] CCITT Recommendation T.6 : Facsimile coding schemes and coding control functions for Group 4 facsimile apparatus, Red Book.1984

[7] 박일남외, "MH부호화를 사용하는 FAX 문서에 대한 다중화 서명법 연구", 신호처리 학회 발표 논문집.1995

[8] 김한상, "MH부호화를 사용하는 FAX 문서에 대한 계층적 디지털 서명법 연구", 경희대학교 석사 학위 논문, 1995

[9] ITU-T Recommendation T.4, 1993

[10] R. Hunter and A. H. Robinson, "International digital facsimile coding standards", Proc.IEEE, 68, 7, pp.854-867, 1980

[11] Selim G.Aki, "Digital Signatures : A Tutorial Survey",IEEE Computer, pp.15-24, Feb. 1983

[12] 한국전자통신연구소, "현대암호학", 1991, 8

[13] "Data Encryption Standard", FIPS Pub. 46, NSA, U.S. Dep. of Commerce, Washington, DC, Jan. 1977.

[14] A.Shimizu and S. Miyaguchi, "Fast Data Encryption Algorithm", Abstructs of EUROCRYPT '87.

[15] 박일남외, "변화화소간의 차분치를 이용한 FAX문서에서의 디지털 서명법", 한국통신학회 추계 종합 학술 발표회 논문집, 1995

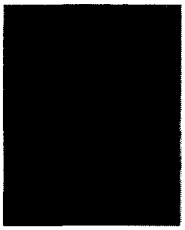
[16] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems", Comm. ACM, Vol. 21, No.2, Feb. 1978, pp.120-126.

□ 著者紹介

박 일 남

1985년 2월 : 경희대학교 공과대학 전자공학과 졸업(공학사)
1988년 8월 : 경희대학교 대학원 전자공학과 졸업(공학석사)
1993년 2월 : 경희대학교 대학원 전자공학과 박사과정 수료
1992년 ~ 현재 : 충남전문대학 사무자동화과 재직(조교수)

※ 주관심 분야 : 디지털 시스템, 영상처리, 암호학



이 대 영

1970년 3월 : 캘리포니아 주립대학원 졸업(공학석사)
1979년 9월 : 연세대학교 대학원 전자공학과 졸업(공학박사)
1971년 9월 : 경희대학교 공과대학 전자공학과 조교수
1977년 3월 : 경희대학교 공과대학 전자공학과 부교수
1982년 3월 ~ 현재 : 경희대학교 공과대학 전자공학과 교수
한국통신학회 수석 부회장
경희대학교 공과대학 학장 역임
경희대학교 산업정보대학원장 역임

※ 주관심 분야 : 디지털 시스템, 컴퓨터 네트워크, 영상처리