論文 96-21-12-4

문서화상에 대한 RDM 합성 알고리즘 및 디지틀 서명에의 응용

正會員 朴 一 男*, 李 大 寧*

A Sutdy on RDM Algorithm for Document Image and Application to Digital Signature

Il-Nam Park*, Dae-Young Lee* *Regular Members*

요 약

본 논문에서는 문서 화상에 비트를 합성하는 방법으로 RDM 알고리즘을 제안한 후 이를 이용하여 FAX 문서에 직접 서명을 실행하는 디지틀 서명 방식을 제안한다. 본 알고리즘은 비트를 합성하기 위해 기주사된 복수개의 참조 주사선중 키에 의해 선택된 주사선의 변화화소와 부호화 주사선의 변화화소의 거리의 우기성과 부호화 주사선의 부호장의 우기성을 이용하여 합성 비트열에 따라 거리와 부호장을 신축조작하는 방법으로 한 번에 2 비트씩 합성을 실행한다. 이는 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 디지틀 서명구조에 의해 디지틀 서명의 제 3조건인 송신자 부인 봉쇄를 구현한다. 디지틀 서명된 송신 문서는 원 문서와 시각적으로 구분이 어려워 제 3자에게는 통상의 문서 교환으로 인식될 것이다.

ABSTRACT

This paper presents the RDM algorithm for composition of bit. After this, We propose a digital signature scheme for facsimile document using RDM algorithm. We modify the even-odd feature in distance of changing pel between coding line and multiple reference line which have been scanned before, and run-length in coding line. 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 with the ITU-T.4(G3 or G4 facsimile standards). The total amount of data transmitted and the quality of image are about the same to that of the original document, thus a third party does not notice signature embeded on the document.

*慶熙大學校 電子工學科
Dept. of Electronic Engineering, Kyunghee Univ.
論文番號:96305-0930
接受日字:1996年 9月 30日

Ⅰ. 서 론

최근 FAX 통신으로 대표되는 문서화상 통신이 상업용 뿐아니라 가정용으로 까지 광범위하게 보급되고 보급율 또한 급속히 증가하고 있으며, 통신량의 증가 뿐아니라 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 이해관계가 걸려있는 민감한 문서의 경우 수신자가 문서를 받은 사실을 부인하는 수신자 부인봉쇄(Non-repudiation, Delivery)나 송신자가 문서의 송신사실을 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 디지틀 서명(Digital signature)이 사용되고 있으며 그 실현 방법으로 암호 기법(cryptographic scheme)이 효과적으로 이용된다.[9]

그러나 일반 데이타통신과 달리 FAX의 경우 원문서와 서명문을 분리전송할 수 없어 이를 해결할 수 있는 방법이 요구된다. 종래의 데이타 통신에 있어서는 그 인증방식으로써 다수의 서명방법이 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 디지틀 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) 디지틀 서명의 3 조건중 S 조건을 해결할 수 없어 부득이 중재자(Arbitrator)서명 방식[10]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 복수개의 참조 주사선(Reference Scan Line: 이하 RSL)의 변화화소사이의 거리(Distance)의 우기성(Even-Odd Feature)과 부호화 주사선의 부호장(Run-Length: 이하 RL)의 우기성을 이용하여 서명 비트열을 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 RDM 알고리즘과 함께 DES 알고리즘 및 RSA 알고리즘을 적용한 디지틀 서명 방식을 제안한다.

Ⅱ. FAX 문서의 특징 및 RDM 알고리즘

2.1 FAX 문서의 특징 및 디지틀 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 역 2배 가까이 된다. 따라서 표준 모드의 경우 1화소가 차지하는 길이는 약 1.2-1.3mm정도로 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 디지틀 서명을 시행할 수 있다. 이때 디지틀 서명은 안전성(Securacy)의 관점에서 다음과 같은 3가지 조건을 만족하여야 한다.[11, 12]

[T]조건: 서명문의 제3자(Third party)에 의한 위조 방지

[R]조건 : 서명문의 수신자(Reciever)에 의한 위조 방지
[S]조건 : 송신자(Sender)의 송신 부인 봉쇄

이러한 조건을 전제로 FAX문서에 서명을 시행할 경우 동일 매체상에 서명이 이루어져야 하는 특수성이 있다. 만일 FAX문서와 서명이 분리되어 전송된다면 제 3자나 수신자에 의한 문서의 위조를 피할 수 없다.

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

2.2 디지틀 서명을 위한 비트합성 알고리즘

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

그림 1의 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

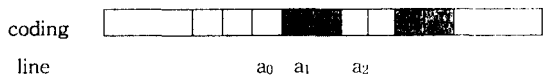
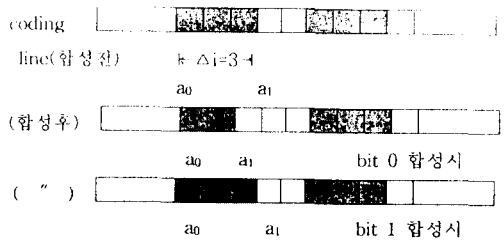
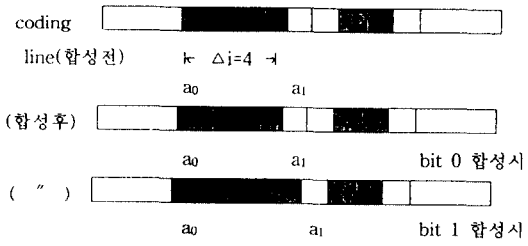


그림 1. 변화화소의 정의
Fig. 1 Definition of changing pel

이들 변화화소를 이용해서 a_i, a_j간의 부호장을 RL(a_i, a_j)로 쓰기로 하고 그림 2의 백RL과 흑RL이 짝수인가 홀수인가에 따라 전송하고자하는 서명데이타의 비트열을 합성부호화한다. RL이 짝수일 경우 서명문으로부터 1비트를 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 복호한다. RL(a_0, a_1)이 짝수라면 합성비트 "0"을 추출하고 RL(a_0, a_1)이 홀수라면 합성비트 "1"을 추출한다.



(a) odd runlength



(b) even runlength

그림 2. 서명데이타 합성 방법
Fig. 2 Mixing Method of Signature data

RM 합성 및 추출 알고리즘을 정리하면 다음과 같다.

합성 알고리즘

```
S1 = ACQUIRE 1 BIT FROM SIGNATURES
  IF RL(a0, a1) = even
     then if S1 = 1
        MOVE position of a1 to 1 pel RIGHT
     else
        NO OPERATION
  else if S1 = 0
        MOVE position of a1 TO 1 pel LEFT
  else
        NO OPERATION
```

추출 알고리즘

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

예외 조건 (그림 3)

i) RL(a_0, a_1) = 1일때 a_1을 합성에 의해 좌측으로 이

동 시키는 것은 불가(따라서 $RL(a_0, a_1)>1$)

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

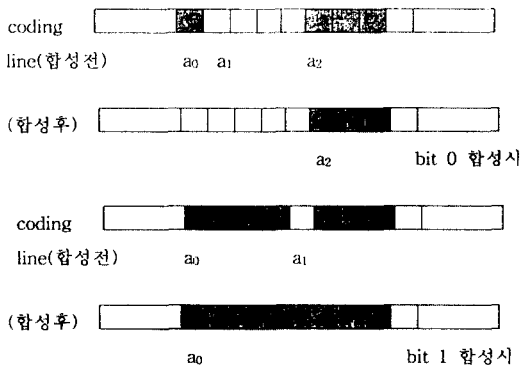


그림 3. 예외 조건
Fig. 3 Exceptional condition

RM 알고리즘은 제삼자가 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 제안 합성 알고리즘(Run-Length & Distance Mixing Algorithm : 이하 RDM 알고리즘)[15]

RDM알고리즘은 키에 의해 선택된 RSL상의 변화화소와 CSL상의 변화화소와의 거리(Distance)의 우기성(Even-Odd Feature)과 CSL상의 RL의 우기성을 이용해서 그 우기성과 서명 데이타의 비트열에 따라 그 거리 및 부호장을 신축조작함으로써 합성을 시행한다. 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 저장해 놓고 이중에서 비밀키에 의해 i 번째의 주사선을 선택한다.

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

a_0 : CSL상의 부호화 혹부호장 최초의 변화화소로 CSL상의 최초의 화소가 백화소인 경우 run 1의 가상의 혹 run을 최초의 화소 직전에 설정

$b_0^{(i)}$: 기주사된 RSL중 i 주사선 상에서 CSL의 변화화소 a_0 직전의 동색의 변화화소

a_1 : CSL에서 a_0의 우측에 있는 다음의 변화 화소

$RL(a_0, a_1)$: 화소 a_0, a_1사이의 부호장(run-length)

RL : $RL(a_0, a_1)$의 우기성(even-odd feature)

∇_i : 변화화소 a_0와 $b_0^{(i)}$ 사이의 거리(distance : 이하 수식에서는 ∇)

φi : ∇_i의 우기성, 즉 ∇_i가 우수이면 0이고 기수이면 1

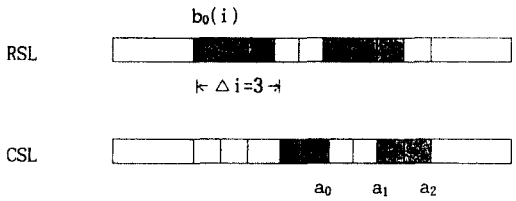


그림 1. RDM알고리즘의 각 화소의 정의
Fig. 1 Definition of each pel in RDM algorithm

본 알고리즘은 RL과 φi를 고려한 수신측에서의 복호를 고려하여 송신측에서 합성 BIT s_0, s_1에 따라 부호화 주사선의 RL과 CSL과 RSL간 φi를 신축조작함으로써 합성을 실현한다.

합성을 실현하기 위한 각 처리기능(PROCESSING FUNCTION)을 다음과 같이 정의한다.

f_1 : 현 상태 유지

$RL' \leftarrow RL$, $\varphi i' \leftarrow \varphi i$

f_2 : RL과 φi를 반전

f_2' : $RL(a_0, a_1)=1$인 경우의 처리로 a_1의 위치를 두 화소 우로 이동 후 a_0위치를 한 화소 우로 이동

f_2'' : $RL(a_0, a_1)\geq 2$인 경우의 처리로 a_0위치를 한 화소 우로 이동

$RL' \leftarrow (RL+1)MOD2$, $\varphi i' \leftarrow (\varphi i+1)MOD2$

f_3 : RL만 반전시키기 위해 a_1의 위치를 한 화소 우로 이동

$RL' \leftarrow (RL+1)MOD2$, $\varphi i' \leftarrow \varphi i$

f_4 : φi만 반전시키기 위해 a_1의 위치를 한 화소 우로 이동후 a_0 위치를 한 화소 우로 이동

$RL' \leftarrow RL$, $\varphi i' \leftarrow (\varphi i+1)MOD2$

이를 이용해 각각의 경우에 따른 처리를 종합하면 표 1과 같다.

표 1. 각 경우의 처리에 대한 진리표
Table 1. Truth Table in each case

RL	φi	S_1	S_0	RL′	$\varphi i'$	f_1	f_2	f_3	f_4
0	0	0	0	0	0	1	0	0	0
0	0	0	1	0	1	0	0	0	1
0	0	1	0	1	0	0	0	1	0
0	0	1	1	1	1	0	1	0	0
0	1	0	0	0	0	0	0	0	1
0	1	0	1	0	1	1	0	0	0
0	1	1	0	1	0	0	1	0	0
0	1	1	1	1	1	0	0	1	0
1	0	0	0	0	0	0	0	1	0
1	0	0	1	0	1	0	1	0	0
1	0	1	0	1	0	1	0	0	0
1	0	1	1	1	1	0	0	0	1
1	1	0	0	0	0	0	1	0	0
1	1	0	1	0	1	0	0	1	0
1	1	1	0	1	0	0	0	0	1
1	1	1	1	1	1	1	1	0	0

이를 처리기능 f에 대해 논리적의 합(Sum of Product)의 형태로 표현한 후 논리식을 정리하면 다음과 같다.

$$\begin{aligned}f_1 &= \overline{RL}\cdot\overline{\varphi i}\cdot\overline{S_1}\cdot\overline{S_0}+\overline{RL}\cdot\varphi i\cdot\overline{S1}\cdot S_0\\ &\quad+RL\cdot\overline{\varphi i}\cdot S_1\cdot\overline{S_0}+RL\cdot\varphi i\cdot S_1\cdot S_0\\ &=\overline{RL}\cdot\overline{S_1}(\overline{\varphi i}\cdot\overline{S_0}+\varphi i\cdot S_0)+RL\cdot S_1(\overline{\varphi i}\cdot\overline{S_0}+\varphi i\cdot S_0)\\ &=(\overline{RL}\cdot\overline{S_1}+RL\cdot S_1)\cdot(\overline{\varphi i}\cdot\overline{S_0}+\varphi i\cdot S_0)\\ &=\overline{(RL\oplus S_1)}\cdot\overline{(\varphi i\oplus S_0)}\end{aligned}$$

$$\begin{aligned}f_2 &= \overline{RL}\cdot\overline{\varphi i}\cdot S_1\cdot S_0+\overline{RL}\cdot\varphi i\cdot S1\cdot\overline{S_0}\\ &\quad+RL\cdot\overline{\varphi i}\cdot\overline{S_1}\cdot S_0+RL\cdot\varphi i\cdot\overline{S_1}\cdot\overline{S_0}\\ &=\overline{RL}\cdot\overline{S_1}(\overline{\varphi i}\cdot S_0+\varphi i\cdot\overline{S_0})+RL\cdot\overline{S_1}(\overline{\varphi i}\cdot S_0+\varphi i\cdot\overline{S_0})\\ &=(\overline{RL}\cdot S_1+RL\cdot\overline{S_1})\cdot(\overline{\varphi i}\cdot S_0+\varphi i\cdot\overline{S_0})\\ &=(RL\oplus S_1)\cdot(\varphi i\oplus S_0)\end{aligned}$$

$$\begin{aligned}f_3 &= \overline{RL}\cdot\overline{\varphi i}\cdot S_1\cdot\overline{S_0}+\overline{RL}\cdot\varphi i\cdot S1\cdot S_0\\ &\quad+RL\cdot\overline{\varphi i}\cdot\overline{S_1}\cdot\overline{S_0}+RL\cdot\varphi i\cdot\overline{S_1}\cdot S_0\\ &=\overline{RL}\cdot S_1(\overline{\varphi i}\cdot\overline{S_0}+\varphi i\cdot S_0)+RL\cdot\overline{S_1}(\overline{\varphi i}\cdot\overline{S_0}+\varphi i\cdot S_0)\\ &=(\overline{RL}\cdot S_1+RL\cdot\overline{S_1})\cdot(\overline{\varphi i}\cdot\overline{S_0}+\varphi i\cdot S_0)\\ &=(RL\oplus S_1)\cdot\overline{(\varphi i\oplus S_0)}\end{aligned}$$

$$\begin{aligned}f_4 &= \overline{RL}\cdot\overline{\varphi i}\cdot\overline{S_1}\cdot S_0+\overline{RL}\cdot\varphi i\cdot\overline{S1}\cdot S_0\\ &\quad+RL\cdot\overline{\varphi i}\cdot S_1\cdot S_0+RL\cdot\varphi i\cdot S_1\cdot\overline{S_0}\\ &=\overline{RL}\cdot\overline{S_1}(\overline{\varphi i}\cdot S_0+\varphi i\cdot\overline{S_0})+RL\cdot S_1(\overline{\varphi i}\cdot S_0+\varphi i\cdot\overline{S_0})\\ &=(\overline{RL}\cdot\overline{S_1}+RL\cdot S_1)\cdot(\overline{\varphi i}\cdot S_0+\varphi i\cdot\overline{S_0})\\ &=(\overline{RL\oplus S_1})\cdot(\varphi i\oplus S_0)\end{aligned}$$

그림 2와 같은 경우의 처리예는 다음과 같다.

이 경우 합성BIT $s_1=1$, $s_0=0$이고 $RL=0$, $\phi_i=1$이므로 $(RL\oplus s_1)$ $(\varphi i\oplus s_0)=1$이 경우에 해당되므로 f_2 처리를 시행하여 $RL'=1$, $\varphi i'=0$으로 만들어 합성시켜야한다. 그런데 $RL(a_0, a_1)\geq 2$이므로 f_2''처리한다. 즉, a_0의 위치를 한 화소 우로 이동한다.

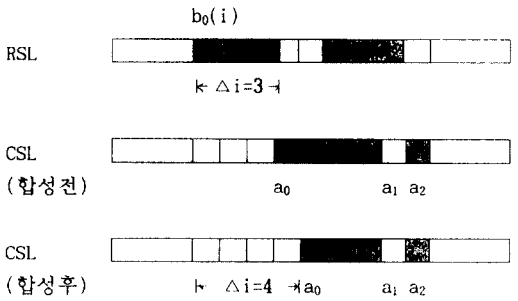
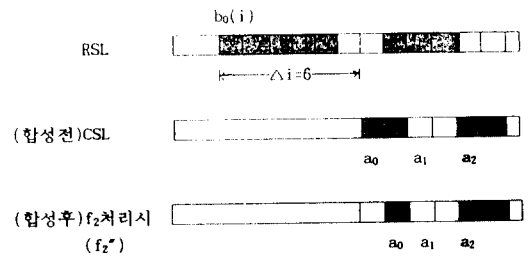


그림 4. 합성처리 예
Fig. 4 Example of Mixing

본 알고리즘의 예외처리는 다음과 같다.

RDM알고리즘중 f_2, f_4 적용시 실행전후의 참조주사선상의 직상화소의 위치가 바뀌어 $b_0^{(i)}$의 위치가 수신측에서 오판되어 합성 BIT 추출시 오류가 발생 할 수 있다. 즉 f_2, f_4 처리후 ϕ_i가 반전되어야 하나 반전되지 않고 $\varphi i'=\varphi i$인 경우 이에 대한 보정이 요구된다. 이 경우 그림 3과 같이 f_2나 f_4처리 후 보정을 위해 다시한번 f_4처리(a_1을 한 화소 우로 이동후 a_0를 한 화소 우로 이동)를 추가로 시행한다.



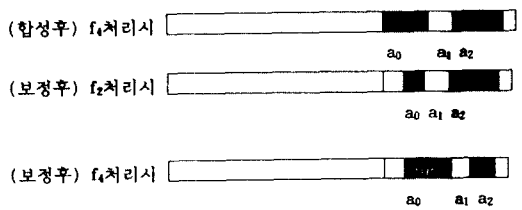


그림 5. RDM 알고리즘의 예외 보정처리
Fig. 5 Exceptional revision processing in RDM algorithm

전체적인 RDM합성 및 추출 알고리즘은 다음과 같다.

<RDM합성 알고리즘>

```
While(not end of page) {
NEXT: While(not end of line)
        {
        Determine reference line i by key
        Set a0,a1 in coding line
        Compute RL(a0,a1) and ∇i
        RL = RL(a0,a1) MOD2
        φi = ∇i MOD2
        Acquire two bits pair(s1,s0) from document
        /* Excute composition of two bits pair */
        if((RL ⊕ s1) (φi ⊕ s0)=1)
              process  f1(no operation)
              goto  NEXT
        elseif((RL ⊕ s1) (φi ⊕ s0)=1)
              if(RL(a0,a1)=1)
                    process  f2'(a1->->,a0->)
              elseif(RL(a0,a1)≥2)
                    process  f2''(a0->)
                    goto  REV
        elseif((RL ⊕ s1) (φi ⊕ s0)=1)
              process  f3(a1->)
              goto  NEXT
        elseif((RL ⊕ s1) (φi ⊕ s0)=1)
              process  f4(a1->,a0->)
              goto  REV
REV:    if(φi'=φi)
              process  f4(a1->,a0->)
        else
              goto  NEXT
        }
}
```

<RDM 추출 알고리즘>

```
While(not end of page) {
NEXT: While(not end of line)
        {
        Determine reference line i by key
        Set a0,a1 in coding line
        Compute RL(a0,a1) and ∇i
        RL = RL(a0,a1) MOD2
        φi = ∇i MOD2
        /* excute extraction of two bits pair */
        s1 = RL
        s0 = φi
        }
}
```

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 제 3자나 수신자가 문서를 위조한 때, 문서상의 변화화소 a_0에 대해 계열 Ψ를 만족시키는 것은 극히 곤란하게 된다.

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

Ⅲ. RDM 알고리즘을 이용한 디지틀 서명 알고리즘

3.1 디지틀 서명 알고리즘

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

우선 송신자 A는 S, T용의 서명 데이타 SAB와 R용의 서명 데이타 SA를 생성하여 이의 보안을 위해 각각 키(Key) K_S와 K_{AB}를 이용해 암호화한다.

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

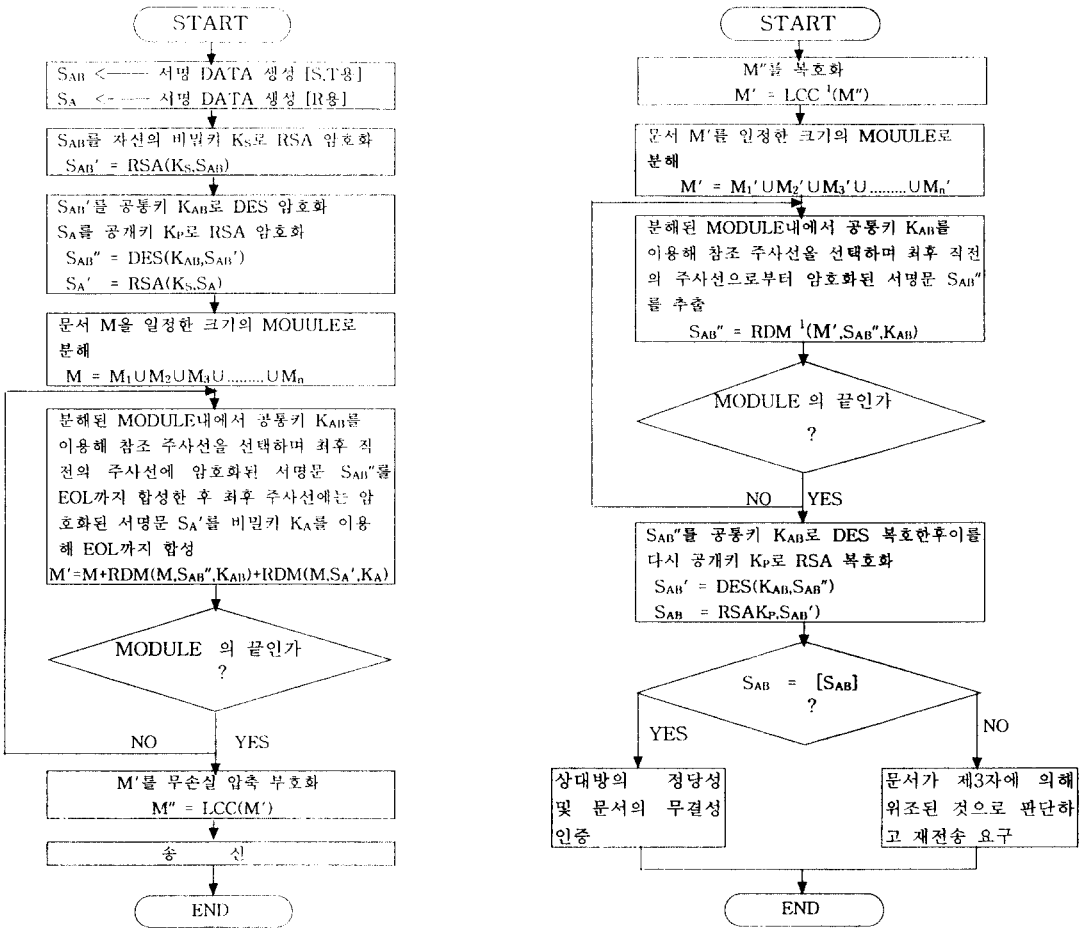


그림 6. DM 알고리즘을 이용한 디지틀 서명 알고리즘
Fig. 6 Digital signature algorithm using DM algorithm

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)이다. 그후 A는 문서 M을 B와 사전에 약속된 크기의 모듈(Module)로 분해한다.

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

분해된 모듈 단위로 각 모듈의 최후주사선 직전의 주사선을 찾아 RDM 알고리즘을 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.

$$\begin{aligned} M' = {} & [M_1 + RDM(M_1, S''_{AB}, K_{AB}) + RDM(M_1, S'_A, K_A)] \\ & \cup [M_2 + RDM(M_2, S''_{AB}, K_{AB}) + RDM(M_2, S'_A, K_A)] \\ & \cup \cdots\cdots + \cdots\cdots \\ & \cup [M_n + RDM(M_n, S''_{AB}, K_{AB}) + RDM(M_n, S'_A, K_A)] \end{aligned} \qquad (3\text{-}3)$$

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

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

수신자 B는 M″를 수신하여 복호화(이하 LCC^{-1})하여 디지틀 서명된 문서 M′를 구한다.

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

다음은 디지틀 서명된 문서 M′을 송신자 A와 사전에 약속된 크기의 모듈로 분해한다.

$$M' = M'_1 \cup M'_2 \cup M'_3 \cup \cdots \cup M'_n \tag{3-6}$$

이어 분해된 모듈단위로 각 모듈의 최후 주사선 직전의 주사선을 찾아 그 주사선의 처음부터 EOL까지 합성되어 있는 암호화된 S, T용의 서명 데이타 S''_{AB}를 RDM 추출 알고리즘(이하 RDM^{-1})으로 추출한다.

$$\begin{aligned}
[S''_{AB}]_1 &= RDM^{-1}(M_1, [S''_{AB}]_1, K_{AB}) \\
[S''_{AB}]_2 &= RDM^{-1}(M_2, [S''_{AB}]_2, K_{AB}) \\
&\vdots \\
[S''_{AB}]_n &= RDM^{-1}(M_n, [S''_{AB}]_n, K_{AB})
\end{aligned} \tag{3-7}$$

그 후 추출된 $[S''_{AB}]_1$, $[S''_{AB}]_n$, …, $[S''_{AB}]_n$을 공통키 K_{AB}를 이용해 DES복호한다.

$$\begin{aligned}
[S_{AB}']_1 &= DES(K_{AB}, [S''_{AB}]_1) \\
[S_{AB}']_2 &= DES(K_{AB}, [S''_{AB}]_2) \\
&\vdots \\
[S_{AB}']_n &= DES(K_{AB}, [S''_{AB}]_n)
\end{aligned} \tag{3-8}$$

이를 다시 A의 공개키 K_p로 RSA복호하여 S_{AB}를 구한다.

$$\begin{aligned}
[S_{AB}]_1 &= RSA(K_p, [S_{AB}']_1) \\
[S_{AB}]_2 &= RSA(K_p, [S_{AB}']_2) \\
&\vdots \\
[S_{AB}]_n &= RSA(K_p, [S_{AB}']_n)
\end{aligned} \tag{3-9}$$

수신자 B는 다음의 경우 상대방을 인증함과 동시에 문서의 무결성을 인증한다.

$$\begin{aligned}
&(S_{AB} = [S_{AB}]_1) \text{ AND } (S_{AB} = [S_{AB}]_2) \text{ AND} \\
&\qquad \cdots \text{ AND } (S_{AB} = [S_{AB}]_n)
\end{aligned} \tag{3-10}$$

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

$$\begin{aligned}
&(S_{AB} \neq [S_{AB}]_1) \text{ OR } (S_{AB} \neq [S_{AB}]_2) \text{ OR} \\
&\qquad \cdots \text{ OR } (S_{AB} \neq [S_{AB}]_n)
\end{aligned} \tag{3-11}$$

3.2 분쟁시 처리

한편 송신자 A는 수신자 B가 문서를 위조 하는등의 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.

$$\begin{aligned}
[S'_A]_{S1} &= RDM^{-1}([M']_{S1}, [S''_A]_{S1}, K_A) \\
[S'_A]_{S2} &= RDM^{-1}([M']_{S2}, [S''_A]_{S2}, K_A) \\
&\vdots \\
[S'_A]_{Sn} &= RDM^{-1}([M']_{Sn}, [S''_A]_{Sn}, K_A)
\end{aligned} \tag{3-12}$$

추출된 $[S'_A]_{S1}$, $[S'_A]_{S2}$, …, $[S'_A]_{Sn}$를 A의 공개키 K_P를 이용해 RSA 복호한다.

$$\begin{aligned}
[S_A]_{S1} &= RSA(K_P, [S'_A]_{S1}) \\
[S_A]_{S2} &= RSA(K_P, [S'_A]_{S2}) \\
&\vdots \\
[S_A]_{Sn} &= RSA(K_P, [S'_A]_{Sn})
\end{aligned} \tag{3-13}$$

송신자 A는 다음과 같은 경우 수신자 B의 위조를 인증한다.

$$\begin{aligned}
&(S_A \neq ([S_A]_{S1}) \text{ OR } (S_A \neq [S_A]_{S2}) \text{ OR} \\
&\qquad \cdots \text{ OR } (S_A \neq [S_A]_{Sn})
\end{aligned} \tag{3-14}$$

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

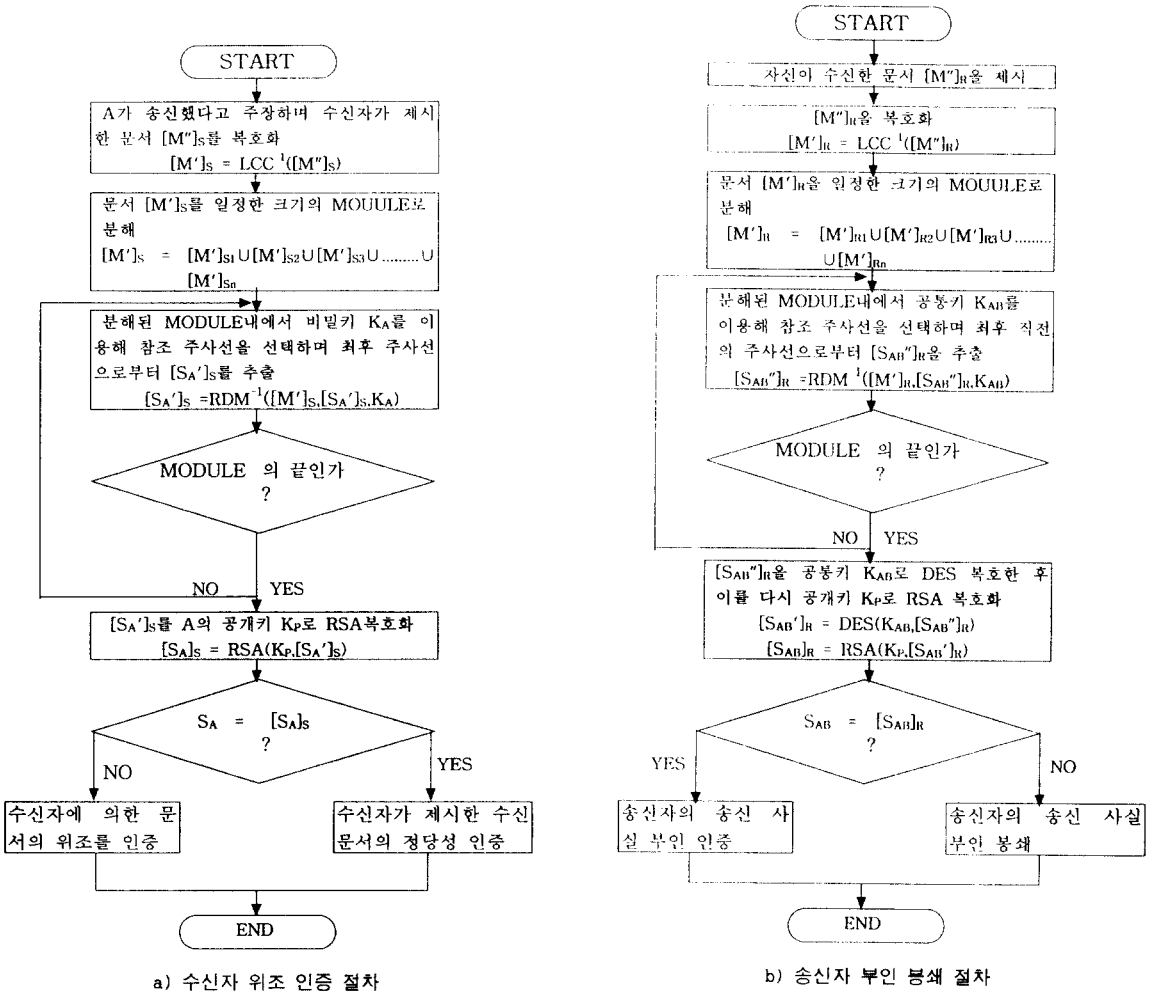


그림 7. 분쟁시 처리 절차

Fig. 7 Processing Procedure in trouble

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

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

다음은 디지틀 서명된 문서 $[M^{'}]_R$을 송신자 A와 사전에 약속된 크기의 모듈로 분해한다.

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

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

$$\begin{aligned}
[S^{''}_{AB}]_{R1} &= RDM^{-1}([M^{'}]_{R1}, [S^{''}_{AB}]_{R1}, K_{AB}) \\
[S^{''}_{AB}]_{R2} &= RDM^{-1}([M^{'}]_{R2}, [S^{''}_{AB}]_{R2}, K_{AB}) \\
&\vdots \\
[S^{''}_{AB}]_{Rn} &= RDM^{-1}([M^{'}]_{Rn}, [S^{''}_{AB}]_{Rn}, K_{AB})
\end{aligned} \tag{3-17}$$

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

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

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

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

이때 $[S_{AB}']_R$은 송신자 A 자신의 비밀키에 의해 공개키 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.

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

Ⅳ. 실험 및 고찰

본 논문에서 제안된 알고리즘에 대한 모의 실험은 ITU의 FAX용 TEST화상(1024×723)[8] 두개를 선택하여 PC상에서 실험을 행하였다. 실험 결과는 다음과 같다.

그림 10과 그림 11에서 보는 바와같이 원 문서 화상과 서명이 합성된 문서화상간의 시각적인 차이를 느낄 수 없어 비밀 서명이 가능한 것을 확인할 수 있었으며 표 2에서와 같이 앞서 발표한 RM 서명문 합성 방법과 비교하였을 때에 합성가능 데이터량이 NO1 문서의 경우 약 45% NO2 문서의 경우 약 4.5% 증가함을 확인하였다. 즉 문서가 복잡할수록 RDM 알고리즘의 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

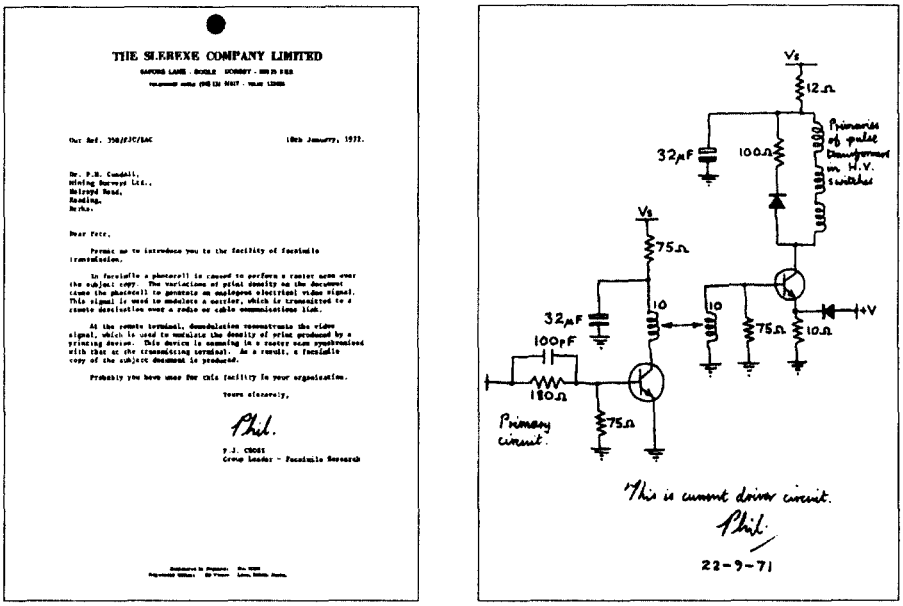


그림 8. ITU.T4 문서화상
Fig. 8 ITU.T4 TEST CHART

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

이 름 : R K H NAME
01010000 01000001 01010010 01001011 01001001
01001100 01001110 01000001 01001101

SA 암호화된 데이타
00001010 01001100 10000010 11000011 01001100
00001100 11101010 10111010 01010100

b)R용의 서명 데이타 및 암호화

그림 9. 서명 데이타의 암호화
Fig. 9 Encryption of signature data

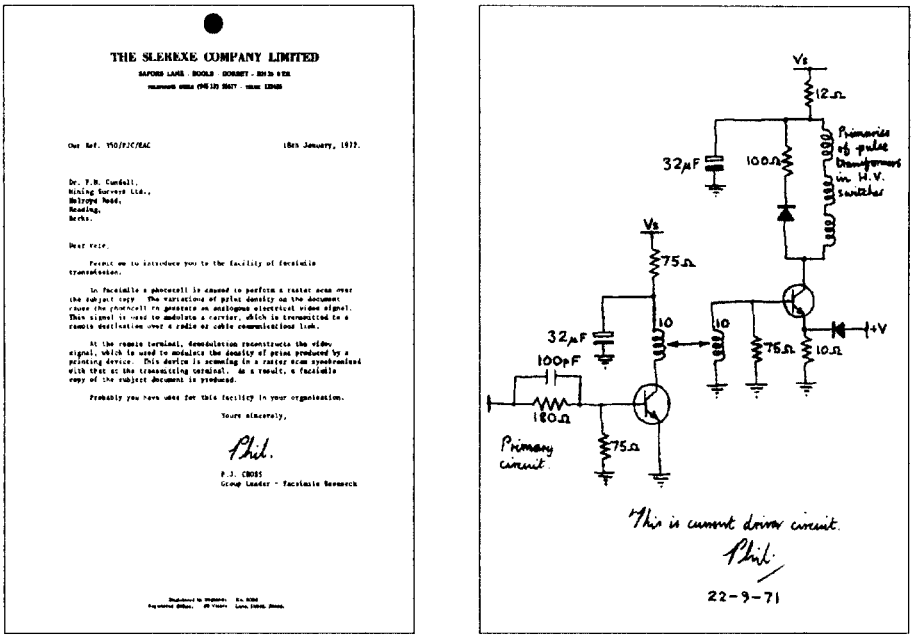
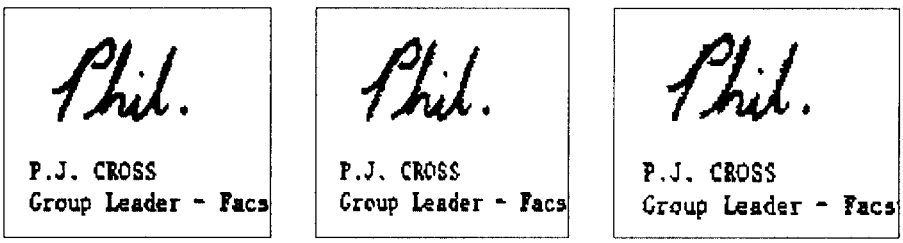


그림 10. 서명데이타가 합성된 T.4 문서화상
Fig. 10 T.4 test chart mixed by signature data



(a)원 문서 화상 (b)Paper[7, 8] 서명 문서 (c)DM 서명 문서

그림 11. 합성된 문서와의 비교
Fig. 11 Comparison between mixing test chart and original test chart

표 2. 문서화상의 합성가능데이타량 비교
Table 2. Comparison of mixing capability on test chart

단위 : BIT

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

표 3. MH 부호량의 변화
Table 3. Change in MH code length

단위 : BIT

모듈간격	M = 1	M = 3	M = 5	M = 10	M = 20	M = 40
RM 합성법의 NO1 FAX 문서화상	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 합성법의 NO1 FAX 문서화상	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 합성법의 NO2 FAX 문서화상	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 합성법의 NO2 FAX 문서화상	107,886 (14.572%)	107,672 (14.543%)	107,633 (14.538%)	107,609 (14.535%)	107,602 (14.533%)	107,597 (14.533%)

MH 부호량(압축률)

원문서 : NO1 FAX 문서화상 : 178.802(24.15%)
NO2 FAX 문서화상 : 107.597(14.533%) (1024×723 = 740,352)

비도(Crypto-degree)로 평가하면 다음과 같다. 문서화상의 해상도를 (ixj)로 하고 모듈 수를 m이라 하면 1개의 모듈내에는 i/m개의 주사선이 존재하게되므로 1개의 모듈이 해독될 확률 $(P_{RDM})_m$은 다음과 같다.

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

따라서 문서 전체가 해독될 확률 P_{RDM}은 다음과 같다.

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

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

V. 결 론

FAX 문서 자체에 어떠한 수단으로 서명을 시행하여 제 3자의 눈에는 보통의 문서와 다름없게 전송하는 디지틀 서명은 상대방 및 문서에 대한 정당성을 인증할 수 있는 방법이다. 본 논문에서는 참조 주사선과 부호화 주사선의 변화 화소의 거리의 우기성을 이용한 RDM 합성 알고리즘을 제안하고 이를 이용하여 FAX 문서에 디지틀 서명의 3 조건인 T, R, S조건을 만족하는 디지틀 서명을 시행하는 알고리즘을 제안하였다. ITU의 TEST CHART를 대상으로 실험한 결과, RDM 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 교환으

로 인식될 것이다. 앞으로 디지틀 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 디지틀 서명법 연구", 경희대학교 석사 학위 논문, 1995.
9. ITU-T Recommendation T.4, 1993.
10. ITU-T Recommendation T.6, 1993.
11. R. Hunter and A. H. Robinson, "International digital facsimile coding standards", Proc. IEEE, 68, 7, pp.854-867, 1980.
12. Selim G. Aki, "Digital Signatures:A Tutorial Survey", IEEE Computer, pp.15-24, Feb. 1983.
13. 한국전자통신연구소, "현대암호학", 1991, 8.
14. "Data Encryption Standard", FIPS Pub. 46, NSA, U.S. Dep. of Commerce, Washington, DC, Jan. 1977.
15. A. Shimizu and S. Miyaguchi, "Fast Data Encryption Algorithm", Abstructs of EUROCRYPT '87.
16. 박일남외, "변화화소간의 차분치를 이용한 FAX 문서에서의 디지틀 서명법", 한국통신학회 추계 종합 학술 발표회 논문집, 1995.
17. R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-keyCryptosystems", Comm. ACM, Vol.21, No.2, Feb. 1978, pp.120-126.

朴 一 男(Il-Nam Park) 정회원

1985년 2월:경희대학교 공과대학 전자공학과 졸업(공학사)

1988년 8월:경희대학교 대학원 전자공학과 졸업(공학석사)

1993년 2월:경희대학교 대학원 전자공학과 박사과정 수료

1992년 3월~현재:충남전문대학 사무자동화과 재직 (조교수)

※주관심분야:디지틀 시스템, 영상처리, 암호학

李 大 寧(Dae-Young Lee) 정회원