정보학연구 제5권 제1호 2002년 3월(pp.1-11)
The Journal of Information Technology, Vol.5, No.1

문서화상에 대한 차분부호장 혼합 합성 알고리즘

박일남*

요 약

본 논문에서는 문서화상에 대한 차분 부호장 혼합 알고리즘을 제안한다. 본 알고리즘을 사용할 경우 RL과 DM 알고리즘에 비해 동일 문서에 2배의 정보를 합성할 수 있다. 본 알고리즘을 사용할 경우 비 보안 문서상에 디지털 서명 뿐 아니라 보안 문서도 합성 가능하다. 이 경우 제 3자가 보안 전송 사실을 감지 할 수 없어 문서의 보안 전송이 구현된다.

Ⅰ. 서론

근래들어 여러 형태의 정보통신에 있어서 보안에 대한 요구가 급격히 증가하고 있음은 주지의 사실이다. 따라서 이에 대한 연구도 매우 활발해지고 있다.[1,2] 화상의 경우도 예외는 아니어서 이의 보안방식에 대한 연구가 다소 진전되어 있다. 그러나 이들 연구는 대개 기존의 데이터통신에서 연구되어온 각종의 암호화기법을 그대로 적용하는데 머물고 있다. 특히 문서 화상의 경우 타 화상에 비해 중요 정보를 갖고 있는 경우가 대부분이며 기존의 암호화 방식을 그대로 적용할 경우 제 3자가 문서의 암호화 여부를 쉽게 판독할 수 있어 매우 강한 암호를 적용하지 않는 한 암호해독자의 암호해독(Cryptanalysis)으로 인해 문서의 안전성(Secrecy)을 보장받을 수 없다. 문서 화상의 정보량을 고려할 때 강한 암호의 적용은 속도상에서 큰 문제를 야기시킨다. 따라서 본 논문은 이와같은 점을 고려해 문서의 보안 전송 여부를 제 3자가 판독할 수 없게 하여 1차적으로는 공격(Attack)의 가능성을 줄이고 2차적으로는 공격이 가해진다해도 스크램블(Scramble)에 의해 해독이 용이하지 않도록 하는 BIT합성에 의한 문서의 보안 기법으로 차분부호장 혼합(Runlength & Distance Mixing) 알고리즘을 제안하다. 이는 앞서 제시한 방식[3,4,5]에 비해 동일한 문서 공간에 약 2배의 합성이 가능하므로 송수신 부호량을 반감시킬 수 있으며 합성 속도가 개선된다. 본 알고리즘은 부호화 주사선(Coding Scan Line:이하 CSL)의 흑부호장(Black Runlength:이하 BR)의 우기성과 참조주사선(Reference Scan Line:이하 RSL)과 CSL의 변화화소간 거리의 우기성을 합성 비트에 따라 신축조작함으로써 2비트의 동시 합성을 구현한다. 실험을 통해 앞서 제안한 알고리즘과 차분부호장 혼합 알고리즘을 합성 가능량 및 합성 전후의 부호량의 변화와 비도의 측면에서 비교 분석한다.

* 대덕대학 컴퓨터정보통신계열

II. FAX 문서의 특징 및 차분 부호장혼합 알고리즘

2.1 FAX 문서의 특징

ITU-T Recommendation T.4,T.6(종전에는 "CCITT Recommendation T.4,T.6)[6,7,8,9]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 문서상에 비밀을 요하는 정보를 비밀리에 합성할 수 있다.

2.2 문서화상에 대한 비트합성 알고리즘

2.2.1 RM 알고리즘(Runlength Mixing Algorithm:이하 RM 알고리즘)[3,4]

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

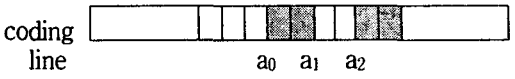
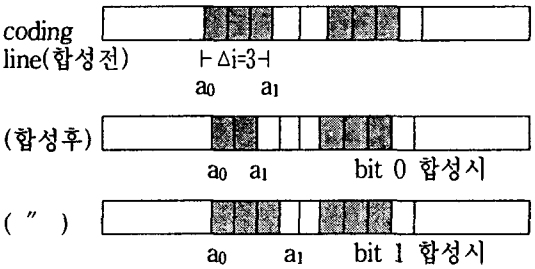


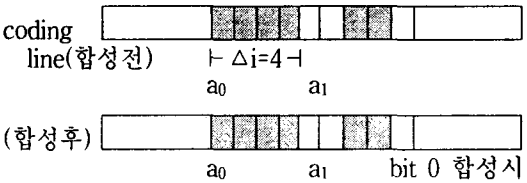
그림 1. 변화화소의 정의

[Fig 1] Definition of changing pel

이들 변화화소를 이용해서 a_i, a_j간의 부호장을 $RL(a_i,a_j)$로 쓰기로 하고 그림2의 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) $RL(a_0,a_1)=1$일때 a_1을 합성에 의해 좌측으로 이동 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 이동하는 것은 불가(따라서 $RL(a_1,a_2) > 1$)

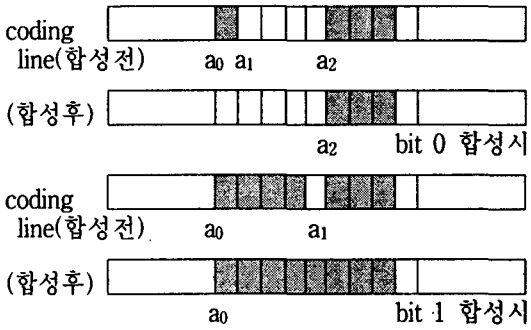


그림 3. 예외 조건

[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)

차분부호장 혼합 알고리즘은 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 저장

해 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 흑부호장 최초의 변화화소로 CSL상의 최초의 화소가 백화소인 경우 run 1의 가상의 흑 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 변화화소

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

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

∇_i : 변화화소 a_0 와$b_0^{(i)}$ 사이의 거리(distance: 이하 수식에서는 ∇)

φi : ∇_i 의 우기성,즉 ∇_i 가 우수이면 0이고 기수이면 1

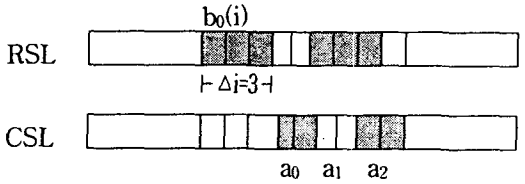


그림 4. 차분부호장 혼합 알고리즘의 각 화소의 정의

〔 Fig 4 〕 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(Prccessing Function)을 다음과 같이 정의한다.

f_1 : 현 상태 유지

RL′ <- RL , $\varphi i'$ <- φi

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′ <- (RL+1)MOD2, $\varphi i'$ <- (φ i+1)MOD2

f_3 : RL만 반전시키기 위해 a_1의 위치를 한 화소 우로 이동

RL′ <- (RL+1)MOD2, $\varphi i'$ <- φi

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

RL′ <- RL, $\varphi i'$ <- (φi+1)MOD2

이를 이용해 각각의 경우에 따른 처리를 종합하면 <표 1>과 같다.

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

$$f_1 = \overline{RL}\cdot\overline{\varphi i}\cdot\overline{S_1}\cdot\overline{S_0} + \overline{RL}\cdot\overline{\varphi i}\cdot S1\cdot S_0 + \overline{RL}\cdot\varphi i\cdot\overline{S_1}\cdot\overline{S_0} + RL\cdot\overline{\varphi i}\cdot S_1\cdot S_0$$

$$= \overline{RL}\cdot\overline{S_1}(\overline{\varphi i}\cdot\overline{S_0}+\varphi i\cdot S_0) + RL\cdot S_1(\varphi i\cdot\overline{S_0} + \overline{\varphi i}\cdot S_0)$$

$$= (\overline{RL}\cdot\overline{S_1} + RL\cdot S_1)\cdot(\overline{\varphi i}\cdot\overline{S_0} + \varphi i\cdot S_0)$$

$$= \overline{(RL \oplus S_1)}\cdot\overline{(\varphi i \oplus S_0)}$$

표 1 각 경우의 처리에 대한 진리표

〔Table 1〕 Truth Table in each case

RL	φi	S1	S0	RL'	φi'	f1	f2	f3	f4
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

$$f_2 = \overline{RL} \cdot \overline{\varphi i} \cdot S_1 \cdot S_0 + \overline{RL} \cdot \varphi i \cdot S1 \cdot \overline{S_0}$$
$$+RL \cdot \overline{\varphi i} \cdot \overline{S_1} \cdot S_0 + RL \cdot \varphi i \cdot \overline{S_1} \cdot \overline{S_0}$$
$$= \overline{RL} \cdot S_1(\overline{\varphi i} \cdot S_0 + \varphi i \cdot \overline{S_0}) + RL \cdot S_1$$
$$(\overline{\varphi i} \cdot S_0 + \varphi i \cdot \overline{S_0})$$
$$= (\overline{RL} \cdot S_1 + RL \cdot \overline{S_1}) \cdot (\overline{\varphi i} \cdot S_0 + \varphi i \cdot \overline{S_0})$$
$$= (RL \oplus S_1) \cdot (\varphi i \oplus S_0)$$

$$f_3 = \overline{RL} \cdot \overline{\varphi i} \cdot S_1 \cdot S_0 + \overline{RL} \cdot \varphi i \cdot S1 \cdot S_0$$
$$+RL \cdot \overline{\varphi i} \cdot S_1 \cdot S_0 + RL \cdot \varphi i \cdot \overline{S_1} \cdot S_0$$
$$= \overline{RL} \cdot S_1(\overline{\varphi i} \cdot S_0 + \varphi i \cdot S_0) + RL \cdot S_1$$
$$(\varphi i \cdot S_0 + \overline{\varphi i} \cdot S_0)$$
$$= (\overline{RL} \cdot S_1 + RL \cdot \overline{S_1}) \cdot (\overline{\varphi i} \cdot S_0 + \varphi i \cdot S_0)$$
$$= \overline{(RL \oplus S_1) \cdot (\varphi i \oplus S_0)}$$

$$f_4 = \overline{RL} \cdot \varphi i \cdot S_1 \cdot S_0 + RL \cdot \varphi i \cdot S1 \cdot S_0$$
$$+RL \cdot \overline{\varphi i} \cdot S_1 \cdot S_0 + RL \cdot \varphi i \cdot S_1 \cdot \overline{S_0}$$
$$= \overline{RL} \cdot S_1(\varphi i \cdot S_0 + \overline{\varphi i} \cdot \overline{S_0}) + RL \cdot S_1$$
$$(\varphi i \cdot S_0 + \overline{\varphi i} \cdot S_0)$$
$$= (\overline{RL} \cdot S_1 + RL \cdot S_1) \cdot (\varphi i \cdot \overline{S_0} + \overline{\varphi i} \cdot S_0)$$
$$= \overline{(RL \oplus S_1)} \cdot (\varphi i \oplus S_0) \text{------식(2-1)}$$

그림 5와 같은 경우의 처리예는 다음과 같다.

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

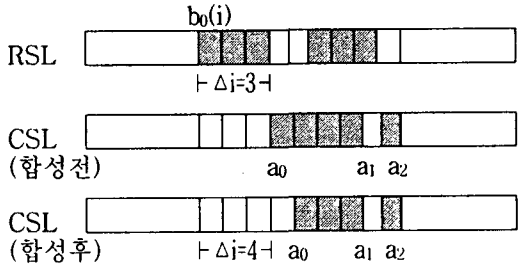


그림 5 합성처리 예

〔 Fig 5 〕 Example of Mixing

본 알고리즘의 예외처리는 다음과 같다.

RDC알고리즘 중 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_i 가 반전되어야 하나 반전되지 않고 $\varphi i' = \varphi i$인 경우 이에 대한 보정이 요구된다. 이 경우 그림 6과 같이 f_2,나 f_4처리 후 보정을 위해 다시한번 f_4처리(a_1을 한 화소 우로 이동후 a_0를 한 화소 우로

이동)를 추가로 시행한다.

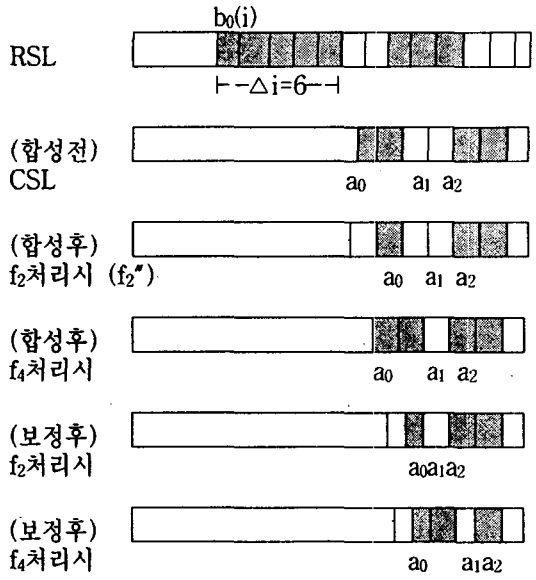


그림 6 차분부호장 혼합 알고리즘의 예외 보정처리

〔 Fig 6 〕 Exceptional revision processing in RDM algorithm

전체적인 차분부호장 혼합 합성 및 추출 알고리즘은 다음과 같다.

<차분부호장 혼합 합성 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
      } }
```

<차분부호장 혼합 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. 차분부호장 혼합 알고리즘은 합성시 전제조건이 없어 합성 가능량이 저하되지 않으며 앞서 제안한 RM 알고리즘에 비해 두 배의 합성이 가능하므로 전송 부호량의 감소와 서명 속도의 개선이 가능하다.

Ⅲ. 실험 및 고찰

본 논문에서 제안된 알고리즘에 대한 모의 실험은 ITU의 FAX용 TEST화상(1024×723)[8] [8,9] 두 개를 선택하여 PC상에서 실험을 행하였다. 실험 결과는 다음과 같다.

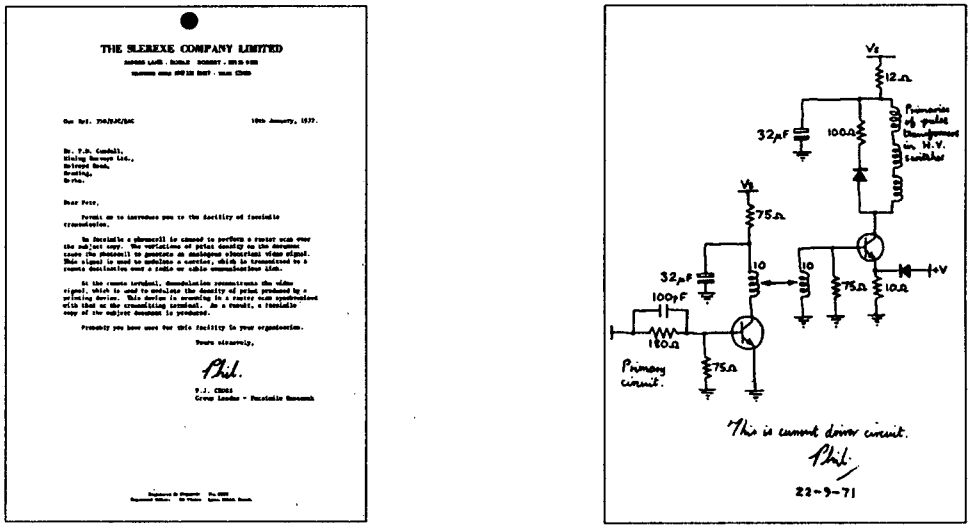


그림 7. ITU.T4 문서화상
〔 Fig 7 〕 ITU.T4 TEST CHART

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

그림 8. 합성할 데이터
〔 Fig 8 〕 Data mixed in document

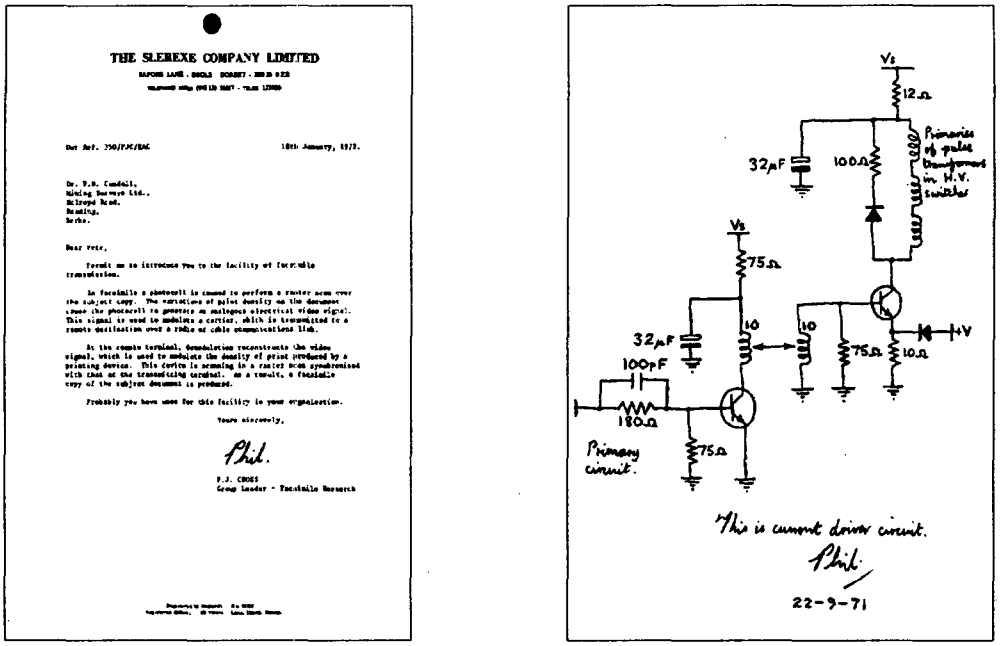
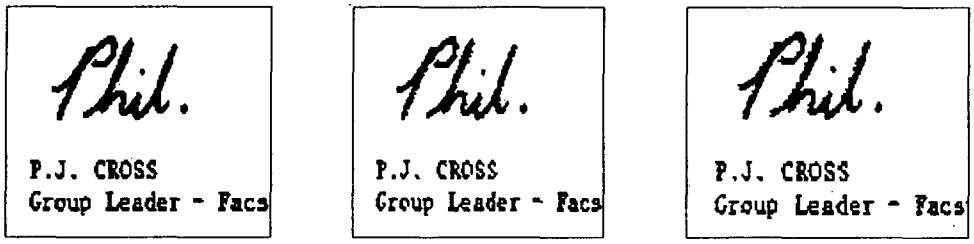


그림 9. 데이타가 합성된 T.4 문서화상

[Fig 9] T.4 test chart mixed by data



(a) 원 문서 화상 (b) Paper[7,8] 합성 문서 (c)차분부호장혼합 합성 문서

그림 10. 합성된 문서와의 비교

[Fig 10]. 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)

그림 10과 그림 11에서 보는 바와같이 원 문서 화상과 데이타가 합성된 문서화상간의 시각적인 차이를 느낄 수 없어 비밀 합성이 가능한 것을 확인할 수 있었으며 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 차분부호장혼합 알고리즘의 합성량이 더울 증가함을 확인하였다. 또한 표 3에 보인 바와같이 합성 전후의 전송 부호량의 변화가 약 0.3% 이내로 부호량의 증대에 따른 부하가 거의 없음을 확인하였다.문서상의 해독될 확률을 비도(Crypto-degree)로 평가하면 다음과 같다. 문서 화상의 해상도를 (ixj)로 하고 모듈 수를 m이라 하면 1개의 모듈내에는 i/m개의 주사선이 존재하게되므로 1개의 모듈이 해독될 확률 $(P_{RDM})_1$은 다음과 같다.

$$(P_{RDM})_1 = i^{-(j-1)} * m^j \quad \text{----------식(3-1)}$$

따라서 문서 전체가 해독될 확률 P_{RDM}은 다음과 같다.

$P_{RDM} = (i^{-(j+1)} * m^j)^m$ ----------식(3-2)

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

Ⅳ. 결론

본 논문에서는 참조 주사선과 부호화 주사선의 변화 화소의 거리의 우기성을 이용한 차분부호장혼합 합성 알고리즘을 제안하였다. ITU의 TEST CHART를 대상으로 실험한 결과, 차분부호장혼합 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 본 논문에서 제안한 차분부호장 혼합 알고리즘을 이용하여 디지틀 서명 뿐 아니라 비밀문서를 일반문서에 합성할 경우에 대한 연구가 필요할 것이다.

참고문헌

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] 박일남외, "MH부호화를 사용하는 FAX 문서에 대한 다중화서명법 연구", 신호처리학회 발표논문집, 1995

4] 김한상, "MH부호화를 사용하는 FAX 문서에 대한 계층적 디지틀서명법 연구", 경희대학교 석사학위논문, 1995

5] 박일남외, "변화화소간의 차분치를 이용한 FAX 문서에서의 디지틀 서명법", 한국통신학회 추계 종합 학술 발표회 논문집, 1995

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

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

8] ITU-T Recommendation T.4, 1993

9] ITU-T Recommendation T.6, 1993

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

11] 한국전자통신연구소, "현대암호학", 1991. 8

A Sutdy On Runlength Distance Mixing Algorithm For Document Image

Il-Nam Park*

Abstract

This paper presents a composition method for document image using RDM algorithm. It is possible to compose about double quantity of document image in same document space compared with RL or DM algorithm, if it used. RDM algorithm is available to compose secret document as well as digital signatures onto non-secure document. In this case, secure transmissin of document will be realize because the third party do not recognize secure transmission.

* Dept. of Computer & Information Communication, Taeduk college