정보학연구 제2권 제2호 1999년 11월(pp.89-105)
The Studies of Information Technology, Vol.2, No.2

합성 방식을 이용한 문서 화상의 보안 체계 연구

허윤석*/김일경**/박일남***

요 약

본 논문은 컴퓨터를 이용한 문서 화상의 보안 통신에서 요구되는 문서 화상의 보안, 위조, 인증 등의 제반 분쟁에 대처하기 위한 연구이다. 문서 화상의 보안을 위해서 기존에 연구되어온 각종 암호화 방식 및 스크램블 방식과 같이 정보의 보안 여부를 노출시키고 비도에 의지하는 방식과 달리 정보의 보안여부를 제3자가 판독하기 어렵도록 하여 일상의 문서 교환으로 인식하게 함으로써 1차적으로 이의 해독에 따른 위험을 감소시키고 2차적으로는 해독이 가해진다 하여도 알고리즘 자체의 비도에 의해 해독을 용이하지 않도록 하는 방식의 보안 체계를 제안한다.

Ⅰ. 서론

근래 들어 여러 형태의 정보통신에 있어서 보안에 대한 요구가 급격히 증가하고 있음은 주지의 사실이다. 따라서 이에 대한 연구도 매우 활발해지고 있다. 이는 컴퓨터 통신망이 컴퓨터 자원의 공동 이용과 컴퓨터 시스템의 신뢰성 향상을 위해 지리적으로 분산되어 있는 각 컴퓨터들을 통신 회선으로 결합하고 있다는 데에서 출발한다. 즉, 이러한 정보와 자원의 공유는 안전성(Securacy)이 확보되지 않은 통신채널을 통해 이루어지기 때문에 권한을 부여받지 못한 불법 사용자들이 통신 채널 등을 통해 정보를 도청하여 정보를 위조하거나 악용하는 위협이 대두되었기 때문이다. 이와 같은 통신상에서 상존 하는 정보의 보안에 대한 위협을 막기 위해 혼돈(Confusion)과 확산(Diffusion)에 의해 정보의 보안을 구현하는 암호화(Cryptography)기법이 오래 전부터 연구되어 왔으며 근래에 와서 통신량과 질의 급속한 확대에 힘입어 보다 심도 있는 연구가 계속되고 있다.[1,2,3,4,5]

본 연구는 문서의 보안 전송 여부를 제 3자가 판독할 수 없게 하여 1차적으로는 암호화 여부의 시각적 확인에 따른 공격(Attack) 대상으로써의 가능성을 줄이고 2차적으로는 해독자가 전문에 대해 암호문 단독 공격(Ciphertext only attack)등 여타 방법으로 공격을 가한다 해도 합성 알고리즘 자체의 비도에 의해 해독이 용이하지 않도록 합성 방식을 이용한 문서화상의 보안 체계에 대한 것이다. 합성 방식으로는 디지털 서명을 위한 DM(Distance Mixing)알고리즘 및 디지털 서명뿐 아니라 보안 문서(Secret Document: 이하 SD)를 합성하기 위해 bit 합성량을 배가시킨 RDM(Runlength & Distance Mixing)

* 충청대학 전자공학과 전임강사
** 대덕대학 정보통신과 조교수
*** 대덕대학 사무자동화과 조교수

알고리즘에 대해 논한 후 이를 이용한 보안 방식에 대해 기술한다.

II. 합성 알고리즘

2.1 거리의 우기성을 이용한 합성 알고리즘(Distance Mixing Algorithm:이하 DM 알고리즘)[6.7]

참조 주사선(RSL: Reference Scan Line)상의 변화화소와 부호화 주사선(CSL: Coding Scan Line)상의 변화화소와의 거리(Distance)의 우기성(Even-Odd Feature)을 이용해서 그 우기성과 서명 데이타의 비트열에 따라 그 거리를 신축 조작함으로써 합성을 시행한다. 이때 CSL은 기주사된 n개의 주사선을 이용하고 그 선택은 송수신자간의 비밀 공통키에 의해 이루어짐으로써 서명의 확산과 서명의 보안(Security)을 구현할 수 있다. 주사가 끝난 n개의 주사선을 메모리에 저장해 놓고 이중에서 비밀키에 의해 i 번째의 주사선을 선택한다. 결국 이 RSL상의 변화화소와 CSL상의 변화화소간의 거리의 우기성에 따라 서명 데이타를 합성하는 것이다.

우선, 그림 2-1에서 CSL과 n개의 RSL의 변화화소, 변화화소간의 거리 및 그 우기성에 관해서 다음과 같이 정의한다.

a_1: CSL상에서 부호화될 부호장(Runlength)의 최초의 변화 화소

$b_1^{(i)}$: 제 i번 RSL상의 a_1에 대응되는 a_1과 동일한 색의 변화화소.

즉 a_1 좌측에 있는 흑부호장의 최초의 화소

Δ_i: 변화화소 a_1과 $b_1^{(i)}$ 사이의 거리(Distance)

ϕ_i: Δ_i의 우기성을 나타내며 Δ_i 가 짝수라면 0, Δ_i가 홀수라면 1로 한다.

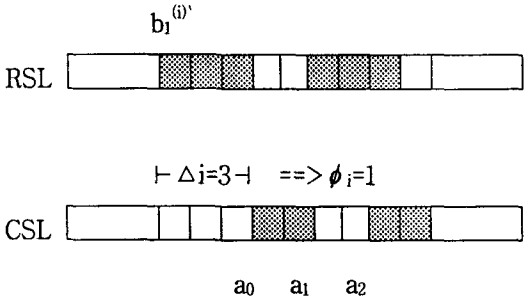


그림 2-1. DM 알고리즘의 각 화소의 정의
[Fig. 2-1] Definition of each pel in DM algorithm

여기서 각각의 경우에 대한 처리를 진리표로 보면 표 2-1과 같다.

표 2-1. 각 경우의 처리에 대한 진리표
[Table 2-1]. Truth table in each case

a) $RL(a_0,a_1) \neq 1$인 경우

ϕ_i	s	ϕ_j	비고	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

b) $RL(a_0,a_1) = 1$인 경우

ϕ_i	s	ϕ_j	비고	f
0	0	0	ϕ_i를 그대로	f_1
0	1	1	ϕ_i를 반전	f_3
1	0	0	ϕ_i를 반전	f_3
1	1	1	ϕ_i를 그대로	f_1

따라서 $RL(a_0,a_1) \neq 1$인 경우, $f_1 = \sim(\phi_i \oplus s)$이고 $f_2 = (\phi_i \oplus s)$이고,

$RL(a_0,a_1) = 1$인 경우, $f_1 = \sim(\phi_i \oplus s)$이고 $f_3 = (\phi_i \oplus s)$이다.

표 2-2를 고려해 DM알고리즘을 유도하기 위해 각 처리기능을 다음과 같이 정의한다.

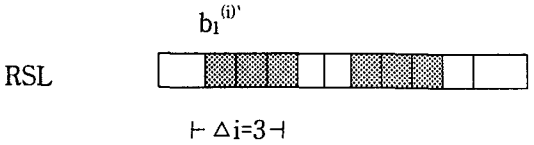
f_1: distance를 그대로 유지(No operation)

f_2: distance를 반전 → a_0 위치를 한 화소 우측으로 이동(a_0 ->)

f_3: distance를 반전 → a_1 위치를 한 화소 우로 이동 후 a_0를 한 화소
우로 이동 즉, Shift Right(a_1 ->, a_0 ->)

그림 2-1의 부호화 주사선의 변화화소 a_0 와 비밀키에 의한 의사 난수(Pseudorandom number)에 의해 선택되는 참조주사선의 변화화소 $b_1^{(i)}$사이의 거리의 우기성 ϕ_i에 따라 합성하고자 하는 데이타의 비트열을 합성 부호화한다. ϕ_i가 짝수일 경우 합성하고자 하는 문서로부터 1비트를 취해 그 값이 "1"이라면 화소 ϕ_i를 짝수로 만들고 "0"이라면 그대로 짝수로 둔다. ϕ_i가 홀수라면 합성할 데이타에서 1비트를 취해 그 값이 "0"이라면 짝수로 만들고 "1"이라면 그대로 홀수로 둔다. 위의 방법으로 합성된 비트를 수신측에서는 다음과 같이 복호한다. ϕ_i가 짝수라면 합성비트 "0"을 추출하고 ϕ_i가 홀수라면 합성 비트 "1"을 추출한다.

DM 알고리즘을 이용한 합성 예는 그림 2-2과 같다.



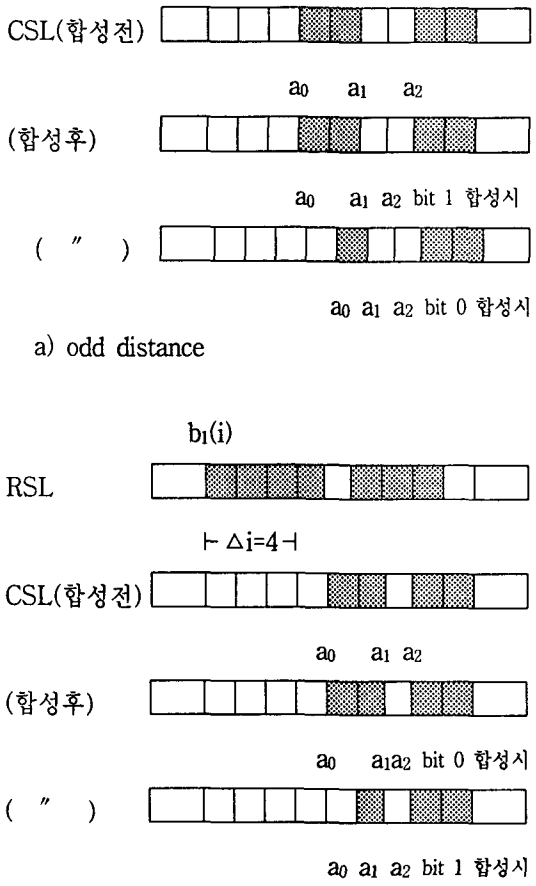


그림 2-2. 비트 합성 방법
(Fig 2-2). Mixing method of one Bit

이와 같이 n개의 주사선에 의존하도록 서명 데이타를 합성하면, 1개의 변화화소 a_0에 n개의 우기성 $\Psi(\phi_1, \phi_2, \cdots, \phi n)$이 존재하게 되어 만일 제 3자가 문서를 해독하거나 위조할 경우, 문서상의 변화 화소 a_0에 대해 n개의 우기성 Ψ에 대해 모두 조사해 봐야하므로 매우 어려운 일이다. DM 알고리즘은 합성시 전제조건이 없어 합성 가능량이 저하되지 않으며 문서의 일부

분에의 서명 합성이 문서상의 다른 영역으로 확산되어 문서의 일부분에만 합성하면 족하므로 서명 속도가 개선된다.

2.2 부호장과 거리의 우기성을 이용한 합성 알고리즘(Runlength & Distance Mixing Algorithm: 이하 RDM 알고리즘)[8,9,10]

DM 알고리즘은 디지털 서명에는 적합하나 다음과 같은 점에서의 보완이 요구되는 문제점이 있다.

첫째, 방대한 량의 보안 문서 자체를 합성하기 위해서는 다량의 비보안 일반 문서가 필요하게 되어 이 경우 송 수신 부호량이 과다해지고, 둘째, 방대한 량의 보안 문서 합성시 다소 시간이 지연되는 문제점이 있다.

RDM 알고리즘은 이를 개선한 것으로 디지털 서명 뿐아니라 보안 문서(Secure Document:이하 SD)를 비보안 문서(Non-Secure Document: 이하 NSD)에 합성하기에 적합하다. 이는 앞서 제시한 DM 알고리즘에 비해 동일한 문서 공간에 약 2배의 합성이 가능하므로 송 수신 부호량을 반감시킬 수 있으며 합성 속도를 개선할 수 있다.

우선 그림 2-3에 대해 다음을 정의한다.

a_0: CSL상에서 부호화될 흑 부호장 최초의 변화화소로 CSL상의 최초의 화소가 백화소인 경우 부호장 1의 가상의 흑부호장을 최초의 화소 직전에 설정

$b_0^{(i)}$: 기 주사된 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)

ϕ_i: ∇_i 의 우기성, 즉 ∇_i 가 우수이면 0이고 기수이면 1로 한다.

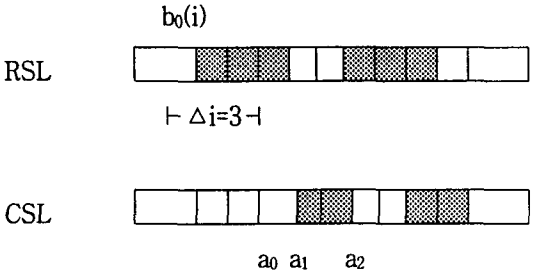


그림 2-3. RDM알고리즘의 각 화소의 정의
(Fig. 2-3) Definition of each pel in RDM algorithm

RDM 알고리즘은 RL과 ϕ_i를 고려한 수신 측에서의 복호를 고려하여 송신 측에서 합성 BIT s_0, s_1에 따라 CSL의 RL과 CSL과 RSL간 ϕ_i를 신축 조작함으로써 합성을 실현한다.

여기서 각각의 경우에 대한 처리를 진리표로 보면 표 2-2와 같다.

표 2-2. 각 경우의 처리에 대한 진리표
[Table 2-2]. Truth Table in each case

RL	ϕ_i	S_1	S_0	RL'	ϕ_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

표 2-2를 고려하여 합성을 실현하기 위한 각 처리기능(Processing Function)을 다음과 같이 정의한다.

f_1: 현 상태 유지
RL' <- RL , ϕ_i' <- ϕ_i

f_2: RL과 ϕ_i를 반전

f_2': RL(a_0,a_1)=1인 경우의 처리로 a_1의 위치를 두 화소 우로 이동후 a_0의 위치를 한 화소 우로 이동
(a_1 ->->,a_0 ->)

f_2'': RL(a_0,a_1)≥2인 경우의 처리로 a_0의 위치를 한 화소 우로 이동
RL' <- (RL+1)MOD2, ϕ_i' <- (ϕ_i+1)MOD2
(a_0 ->)

f_3: RL만 반전시키기 위해 a_1의 위치를 한 화소 우로 이동
RL' <- (RL+1)MOD2, ϕ_i' <- ϕ_i
(a_1 ->)

f_4: ϕ_i만 반전시키기 위해 a_1의 위치를 한 화소 우로 이동 후 a_0의 위치를 한 화소 우로 이동
RL' <- RL, ϕ_i' <- (ϕ_i+1)MOD2
(a_1 ->,a_0 ->)

예를 들어 그림 2-4와 같은 경우의 다음과 같이 처리된다.

이 경우 합성 BIT s_1=1, s_0=0이고 RL=0, ϕ_i=1이므로 f_2=(RL ⊕ s_1) (ϕ_i ⊕ s_0)=1인 경우에 해당되므로 f_2 처리를 시행하여 RL'=1, ϕ_i'=0으로 만들어 합성시켜야 한다. 그런데 RL(a_0,a_1)≥2이므로 f_2''처리한다. 즉 a_0의 위치를 한 화소 우로 이동한다.

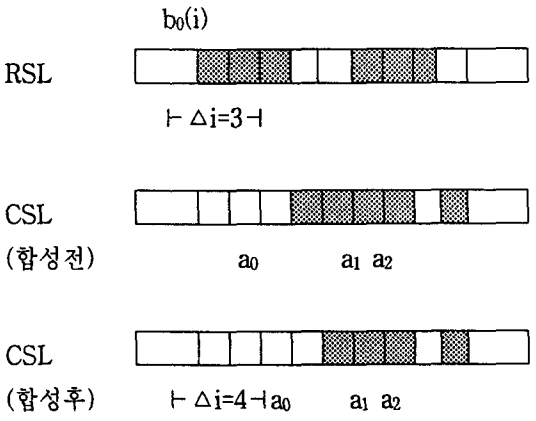


그림 2-4. 합성처리 예(s_1=1,s_0=0,RL=0,φi=1인 경우)
[Fig 2-4]. Example of Mixing

수신측에서는 CSL상에서 a_0, a_1을 설정한 후 RL(a_0,a_1)와 ∇_i를 구하고 RL = RL(a_0,a_1) MOD2, ϕ_i = ∇_i MOD2에 의해 거리의 우기성 RL 및 부호장의 우기성 ϕ_i를 구해 s_1 = RL, s_0 = ϕ_i로 두 개의 합성 비트를 추출한다.

Ⅲ. 문서 화상에 대한 보안 체계

3.1 문서 화상의 보안 체계 및 처리 절차

그림 3-1은 합성 기법을 이용한 문서 화상에 대한 보안 체계이다. 우선 송신 측에서는 서명(Signatures)을 보안 문서(Secure Document)에 합성하여 디지털 서명(Digital Signature)을 시행한 후 이를 압축한 후 비보안문서(Non-Secure Document)에 합성하여 디지털 서명된 보안 문서를 수신 측에 보안 송신하면 수신 측에서는 역 수순에 의해 보안 문서 및 디지털 서명을 분리함으로써 보안 송수신 및 문서의 무결성과 인증을 구현한다. 보안 전송 및 디지털 서명의 3가지 조건을 동시에 만족하도록 하기 위해 기존의 대표적인 공개키 암호 방식인 RSA(Rivest Shamir & Adleman)[15] 알고리즘을 이용해 서명 데이터를 암호화한 후 앞서 제시한 바 있는 서명 속도에서 우수한 DM 알고리즘을 이용해 이를 합성한다. 보안 문서의 합성시에는 RDM 알고리즘을 적용하여 합성 속도 및 합성량을 높였다. 구체적인 송수신 처리 절차는 그림 3-2와 같다.

3.2. 분쟁시 처리 절차

3.2.1. 분쟁시 처리 절차(I)〔R 조건〕

우선 송신자 A는 수신자 B가 문서를 위조하는 등의 문제 발생시 그림 3-3(a)의 절차를 실행해 분쟁을 해결한다.

또한 수신자는 수신 문서에 대해 송신자가 송신 사실을 부인할 경우 그림3-3(b)과 같은 절차를 통해 분쟁을 해결할 수 있다.

3.3. 안전성 평가

전수탐색의 경우 키(Key)의 크기가 n 비트로 구성된 경우의 비도는 일반적으로 2^n으로 평가할 수 있으므로 키를 크게 하면 비도를 높일 수 있다. 그러나 이와 같은 방식으로는 동일 크기의 키를 사용하면 모든 암호 알고리즘의 비도를 같게 볼 수 밖에 없다. 또한 사용하는 난수 발생 방식에 따라 비도가 상당히 달라질 수 있다. 따라서 여기서는 문서 화상이라는 특성을 고려해 NSD에 합성된 SD가 해독될 확률을 비도(Crypto-degree)로 평가한다. 우선 합성 알고리즘 자체는 공개되었고 공격자는 NSD내에 SD가 합성된 사실을 사전에 알고 있으며 RDM 및 DM 알고리즘의 특징을 이용해 공격을 시도한다고 가정한다. 즉, 본 합성 알고리즘에서 합성의 위치는 문장이 위치하고 있는 주사선 중에서도 변화화소가 있는 부분이므로 이 부분을 공격하여 합성 비트에 대한 무제한 추출 공격을 시도하는 경우를 고려한다. 또한 SD에 대해 암호화나 압축 등 여타 방법을 이용해 내용을 변경하지 않은 것으로 가정한다. RSL부인 NSD_{RSL}의 주사선(Scan line) 수를 s, NSD의 하나의 주사선내의 변호화소수를 p, 한줄의 문장(Sentence)의 수직 방향의 주사선수를 q, 한 장의 NSD의 총 문장수를 r이라 할 때 각 경우의 비도는 표 3-2와 같다.

표 3-2. 해독 확률에 따른 비도
〔Table 3-2〕. Crypto-degree according to probability of cryptanalysis

	보안 문서의 비도		서명의 비도	
	합성위치 공개시	합성위치 비공개시		
$(P_{SD})_{1L}$	s^{-p}	$s^{-p}*p^{-1}*r^{-1}$	P_{SN}	$(i/m)^{-p}$
$(P_{SD})_{1S}$	s^{-p-q}	$s^{-p-q}*p^{-1}*r^{-1}$		
$(P_{SD})_{1T}$	s^{-p-q-r}	$s^{-p-q-r}*p^{-1}*r^{-1}$		

단, $(P_{SD})_{1L}$: NSD내의 하나의 주사선이 해독될 확률

$(P_{SD})_{1S}$: NSD내의 한 줄의 문장이 해독될 확률

$(P_{SD})_{1T}$: 한장의 NSD내에 합성된 SD 전체가 해독될 확률

P_{SN} : 서명이 해독될 확률

p : 주사선내 변화화소수

q : 문장(sentence)내 수직주사선수

r : NSD내의 총문장의 수

s : 참조주사선수

공격자가 가용 자료에 따라 공격을 시도할 경우의 안전상을 고려하면 다음과 같다.

첫째로 단지 RDM 알고리즘이 적용된 문서 NSD만을 갖고 해독을 실행하는 암호문 단독 공격(Cipher-text only attack : 이하 COA)의 경우(단, 공격자는 알고리즘 전반에 대해 알고 있다고 가정)로 공격자가 도청한 문서 화상 NSD를 확대한 후 화소의 손실을 확인하고 손실되거나 추가된 화소를 복원하여 복원된 NSD'와 도청한 NSD를 비교하며 RDM 추출 알고리즘으로 해독을 시행하는 경우 RDM 알고리즘의 처리 기능상 화소의 증감만으로는 합성한 비트를 판독하여 추출해낼 수 없다. 단, RL을 구해 합성 비트 S_1을 판독해 낼 수 있다. 즉, $S_1S_0S_1S_0S_1S_0$---에서 S_1을 판독해내어 홀수번째 비트들이 해독될 수 있다. 그러나 해독된 데이터 자체도 압축된 데이터이므로 결국 원래의 합성 문서 화상을 복원하기 위해서는 합성 데이터 전체가 필요하므로 S_1을 해독한 후 다른 방법으로 해독을 실행하여야한다. 한편으로는 이와같은 형태의 공격에 대비해 보다 높은 안전성을 요구하는 분야에 적용하기 위해서는 합성할 보안 문서에 대해 압축 후 기존의 암호(DES등)를 적용하여 RL을 이용한 공격에 대한 안전성을 확보할 수도 있다.

둘째로 일부의 평문과 이에 대응되는 암호문을 갖고 해독을 시행하는 알려진 평문 공격(Known-plaintext attack :이하 KPA)에 대한 안전성을 고려하면, 이는 공격자가 사용한 알고리즘(RDM)에 대해 알고 있고 평문(SD)의 일부와 이에 대응되는 보안문(NSD)를 갖고서 해독을 시행하는 경우와 같은데 이 경우 NSD에는 평문이 압축된 형태로 합성되어 있으므로 전수 탐색으로 NSD에서 데이터를 추출한다 해도 기지의 평문(SD)과 일치하는 데이터를 추출할 수 없다. 따라서 공격자는 추출한 데이터의 압축을 해제한 후에 평문과 비교해 보아야 하는데 합성된 전체 압축문을 해제할 수는 있으나 전체 압축문 중에 중간의 일부분만을 갖고 압축을 해제할 수는 없다. 결국 공격자가 KPA에서 전수 탐색으로 해독을 시행하기 위해서는 압축된 평문의 일부를 입수해야하는데 이는 압축된 전체 평문(혹은 전체 평문)을 입수하는 것과 다를바 없으므로 이는 COA의 경우에 해당된다. 따라서 본 논문의 KPA에 따른 비도는 COA의 비도와 유사하다고 볼 수 있다.

세째로 전체 평문과 이에 대응되는 암호문 쌍을 갖고 해독을 시행하는 선택 평문 공격(Chosen-plaintext attack : 이하 CPA)의 경우로 공격자에게는 가장 좋은 공격 환경이다. 본 논문의 RDM 알고리즘이 적용된 NSD에 대해 CPA를 시도할 경우 역시 추출한 데이터 전체에 대해 압축을 해제하여 입수한 평문과 비교하여야하므로 COA와 유사한 과정을 요한다. 따라서 본 논문의 KPA에 따른 비도는 COA의 비도와 유사하다고 볼 수 있다. 결국 가용 자료에 따른 공격에 관계없이 비도가 COA 공격에 대한 비도를 유지한다.

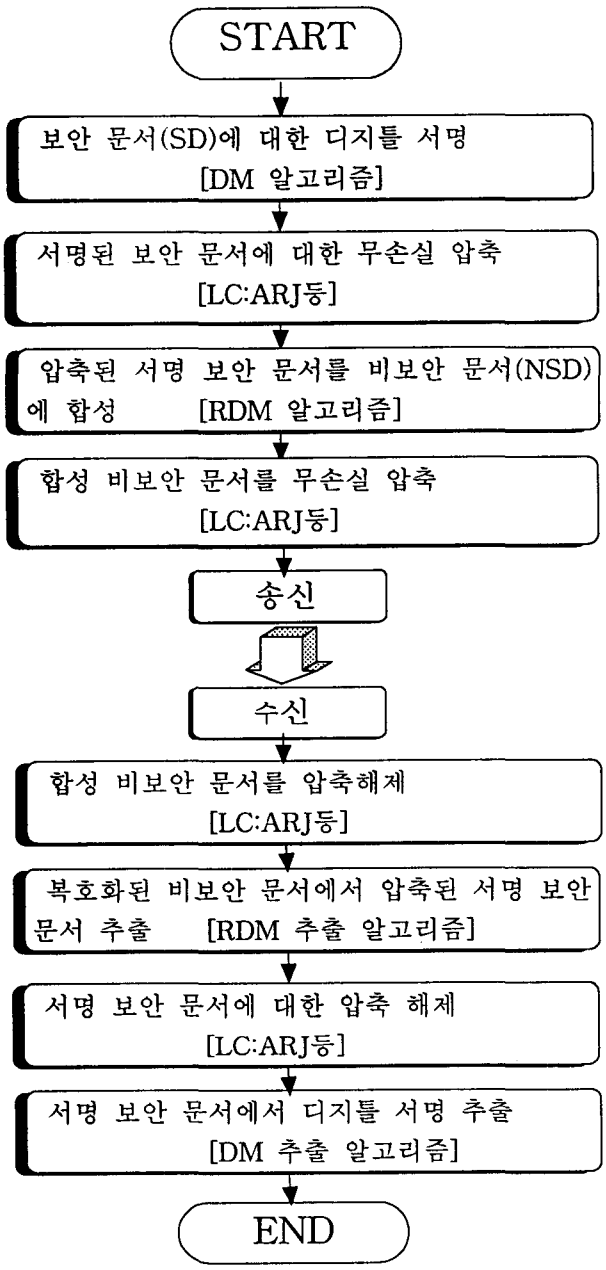
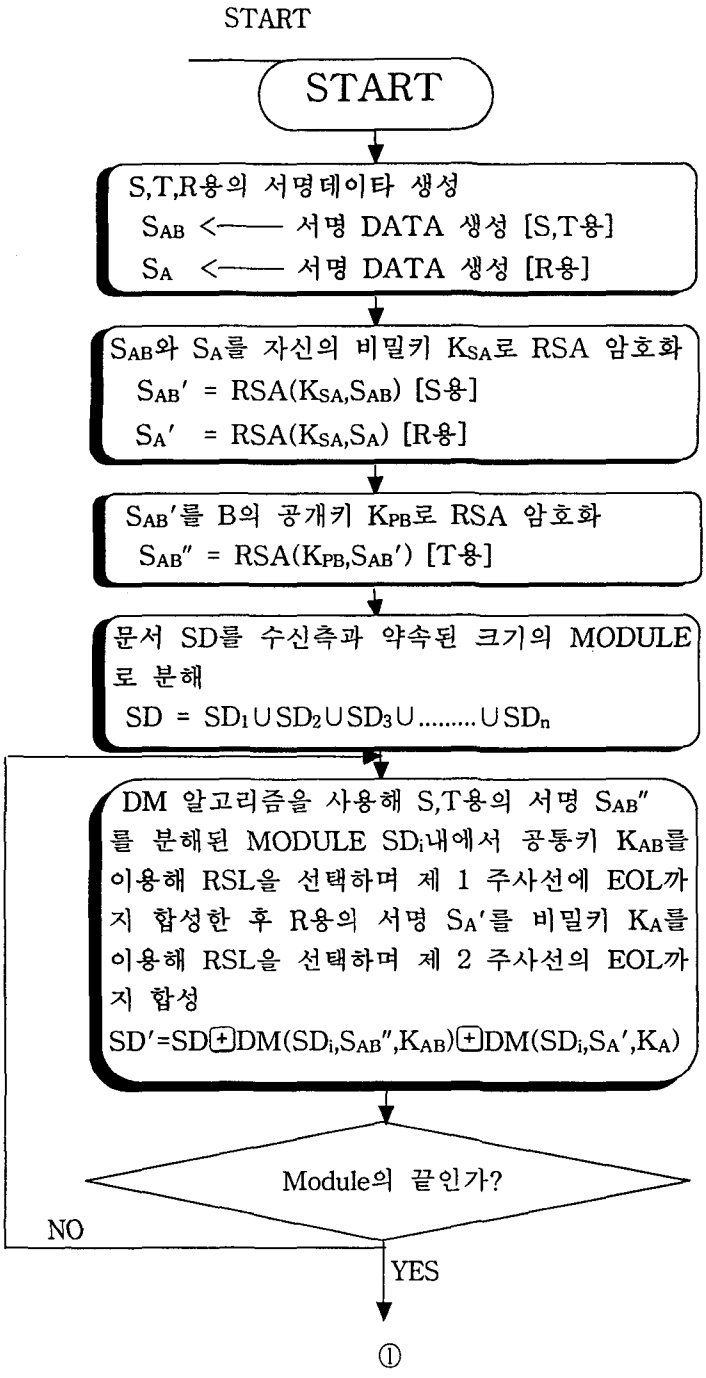
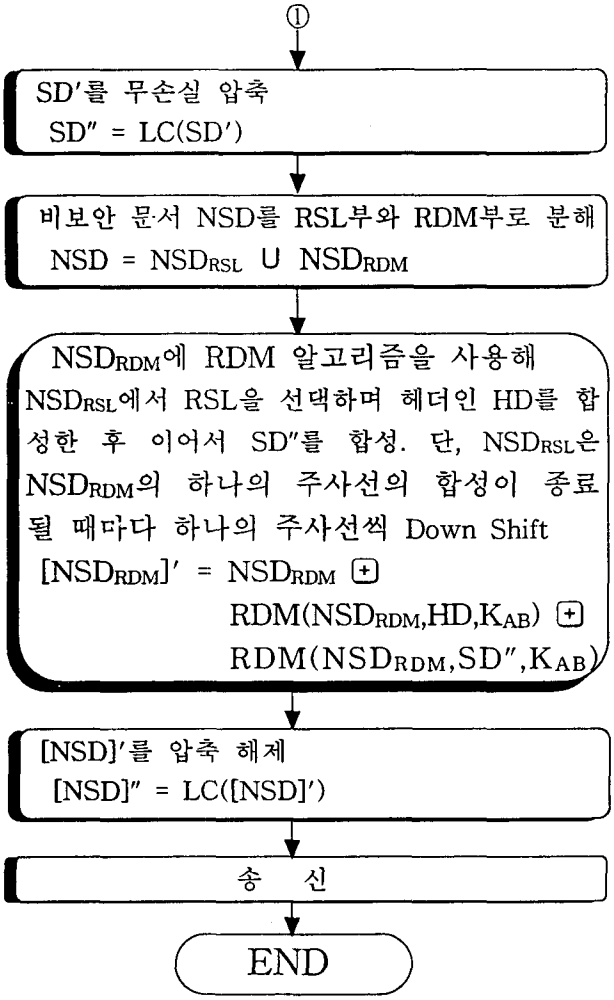


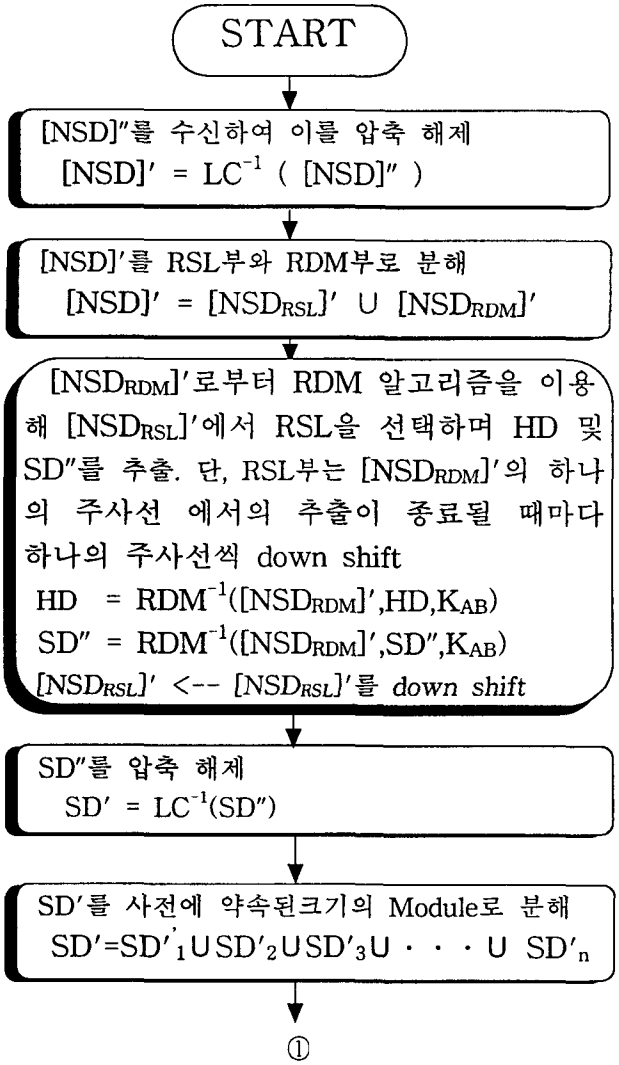
그림 3-1. 문서 화상에 대한 보안 체계

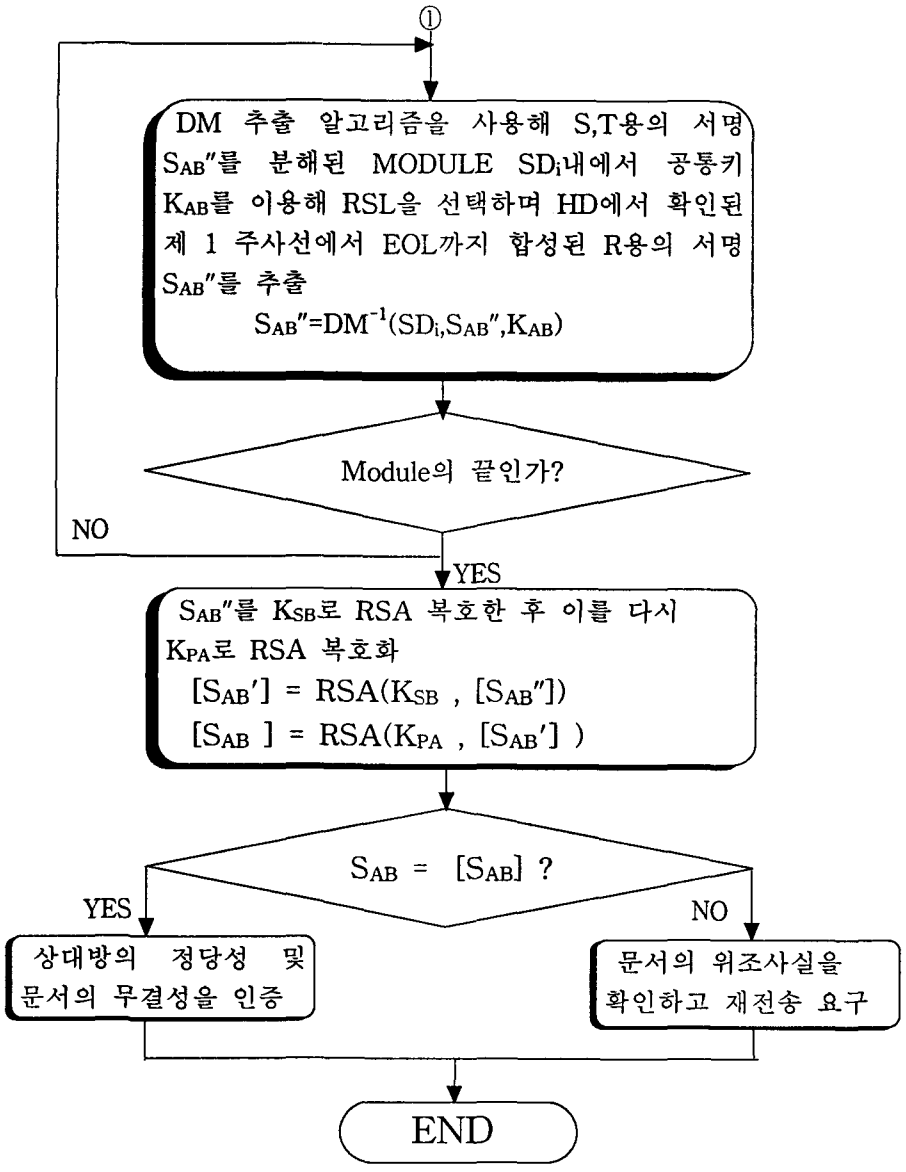
[Fig 3-1]. Security System for document image


START
START
S,T,R용의 서명데이타 생성
SAB <—— 서명 DATA 생성 [S,T용]
SA <—— 서명 DATA 생성 [R용]
SAB와 SA를 자신의 비밀키 KSA로 RSA 암호화
SAB′ = RSA(KSA,SAB) [S용]
SA′ = RSA(KSA,SA) [R용]
SAB′를 B의 공개키 KPB로 RSA 암호화
SAB″ = RSA(KPB,SAB′) [T용]
문서 SD를 수신측과 약속된 크기의 MODULE로 분해
SD = SD1∪SD2∪SD3∪.....∪SDn
DM 알고리즘을 사용해 S,T용의 서명 SAB″를 분해된 MODULE SDi내에서 공통키 KAB를 이용해 RSL을 선택하며 제 1 주사선에 EOL까지 합성한 후 R용의 서명 SA′를 비밀키 KA를 이용해 RSL을 선택하며 제 2 주사선의 EOL까지 합성
SD′=SD⊕DM(SDi,SAB″,KAB)⊕DM(SDi,SA′,KA)
Module의 끝인가?
NO
YES
①


①
SD′를 무손실 압축
SD″ = LC(SD′)
비보안 문서 NSD를 RSL부와 RDM부로 분해
NSD = NSDRSL ∪ NSDRDM
NSDRDM에 RDM 알고리즘을 사용해 NSDRSL에서 RSL을 선택하며 헤더인 HD를 합성한 후 이어서 SD″를 합성. 단, NSDRSL은 NSDRDM의 하나의 주사선의 합성이 종료될 때마다 하나의 주사선씩 Down Shift
[NSDRDM]′ = NSDRDM ⊞
RDM(NSDRDM,HD,KAB) ⊞
RDM(NSDRDM,SD″,KAB)
[NSD]′를 압축 해제
[NSD]″ = LC([NSD]′)
송 신
END

a)송신측 처리 절차

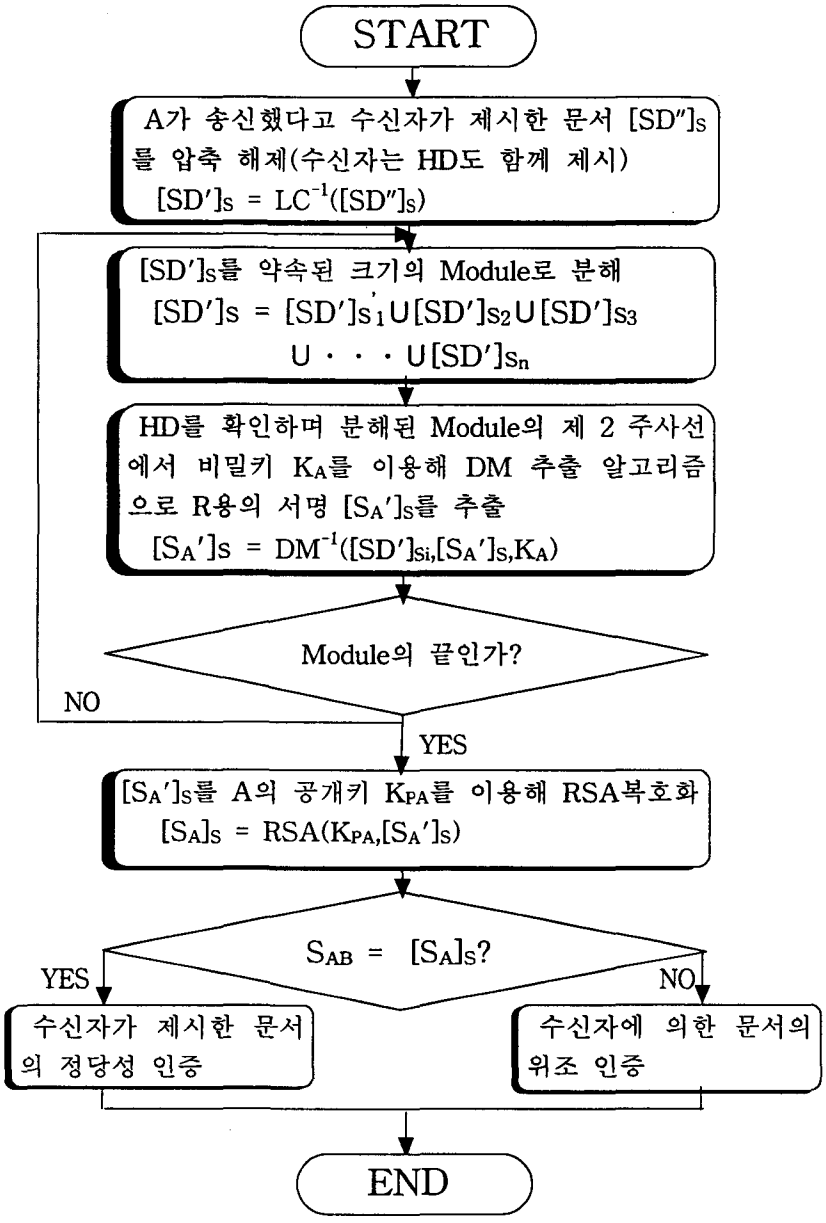

START
[NSD]″를 수신하여 이를 압축 해제
[NSD]′ = LC^{-1} ([NSD]″)
[NSD]′를 RSL부와 RDM부로 분해
[NSD]′ = [NSD$_{RSL}$]′ ∪ [NSD$_{RDM}$]′
[NSD$_{RDM}$]′로부터 RDM 알고리즘을 이용해 [NSD$_{RSL}$]′에서 RSL을 선택하며 HD 및 SD″를 추출. 단, RSL부는 [NSD$_{RDM}$]′의 하나의 주사선 에서의 추출이 종료될 때마다 하나의 주사선씩 down shift
HD = RDM^{-1}([NSD$_{RDM}$]′,HD,K$_{AB}$)
SD″ = RDM^{-1}([NSD$_{RDM}$]′,SD″,K$_{AB}$)
[NSD$_{RSL}$]′ <-- [NSD$_{RSL}$]′를 down shift
SD″를 압축 해제
SD′ = LC^{-1}(SD″)
SD′를 사전에 약속된크기의 Module로 분해
SD′=SD′$_1$∪SD′$_2$∪SD′$_3$∪ · · · ∪ SD′$_n$
①



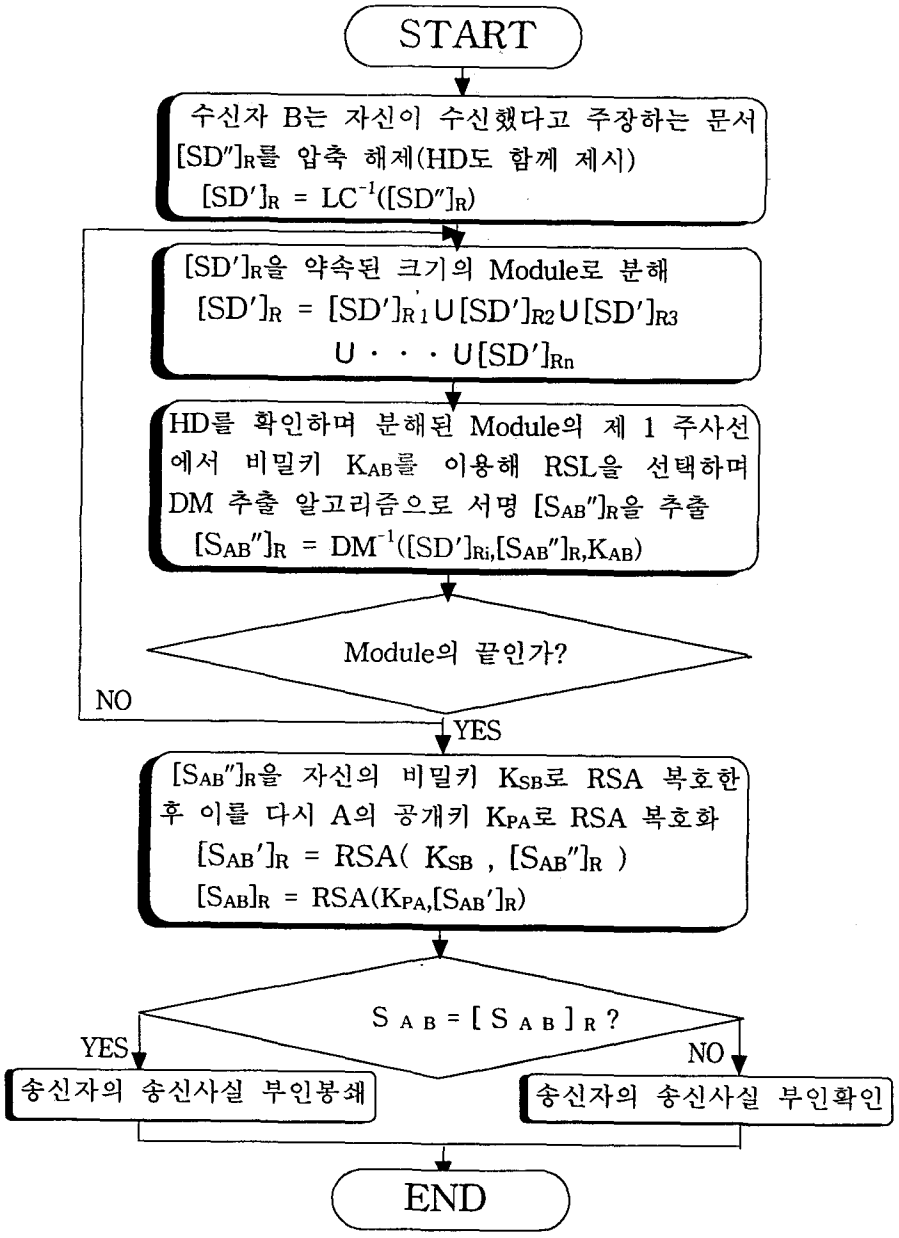
b)수신측 처리 절차

그림 3-2. 송수신 처리 절차

(Fig 3-2). Processing procedure of proposed system



a)수신자 B의 문서 위조 인증 절차(송신측 처리)



b)송신자 A의 송신 부인 봉쇄 절차(수신측 처리)

그림 3-3. 분쟁시 처리 절차

(FIG 3-3). Processing Procedure in a trouble

Ⅳ. 결론

본고에서는 합성 알고리즘을 이용한 문서 화상에 대한 보안 방식에 대해 알아보았다. 이를 위해 참조 주사선과 부호화 주사선의 변화 화소의 거리의 우기성을 이용한 DM 합성 알고리즘 및 부호화 주사선의 흑부호장의 우기성과 참조 주사선과 부호화 주사선의 변화화소간 거리의 우기성을 합성 비트에 따라 신축 조작함으로써 2 비트의 동시 합성을 구현하는 RDM 알고리즘에 대해 알아보았고 이를 이용한 문서 보안 체계에 대해 살펴보았다. 한글 문서를 대상으로 제시한 예를 통해 합성 전후의 문서상에서의 뚜fut한 시각적 차이를 느낄 수 없어 비밀 서명 및 보안 문서의 비밀 전송이 가능하므로 제 3자에게는 통상의 문서 교환으로 인식될 것임을 알 수 있었다. 안전성을 분석한 결과, 비보안 문서에서 보안 문서 화상이 해독될 경우의 시간 복잡도가 $O(n^k)$로 기존의 주사선 전치를 이용한 화상 스크램블 방식의 O(n!)에 비해 안전함을 확인하였다. 가용 자료에 따른 공격에 대해 암호문 단독 공격에 준하는 정도의 비도를 유지하므로 공격에 대해 안전성이 확보됨을 확인하였다. 본고에서 논한 보안체계를 적용할 경우 우선 문서의 보안 전송 여부를 제 3자가 판독할 수 없게 되어 1차적으로는 공격의 가능성을 줄고 2차적으로는 공격이 가해진다 해도 비밀 합성에 의해 해독이 용이하지 않게 되며 송 수신자간에 수신 문서의 위조나 송신 사실 부인시 본 논문의 디지털 서명 방식에 의해 이를 해결할 수 있을 것이다. 본고에서 제시한 방식은 문서 화상의 보안 전송 뿐 아니라 문자열 형태의 텍스트 화일을 보안 전송하는 데에도 적용될 수 있으며 파일의 보안 저장에도 적용 가능할 것이다.

참고문헌

1] Charles P.Pfleeger," Security in Computing", Prentice Hall, 1989

2] 한국전자통신연구소, "현대암호학", 1991. 8

3] Feistel. H., "Cryptography and Computer Privacy", Scientific American, May,(1973), pp.15-23

4] Maywr, C. H. amd Matyas, S. M., Cryptography : A New Dimension in Computer Data Security, John-Wiley and Sons, 1982.

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

6] 박일남외, "FAX 문서에 대한 DM 합성 알고리즘을 이용한 디지털 서명의 제안", 한국통신정보보호학회 논문집, 1997. 6

7] 박일남 외, "변화화소간의 차분치를 이용한 FAX문서에서의 디지털서명법", 한국통신학회 추계 종합 학술 발표회 논문집, 1995

8] 박일남 외, "문서 화상에 대한 RDM 합성 알고리즘", 충남전문대학논문집, 제14집, 1996

9] 박일남 · 이대영, "문서화상에 대한 RDM 합성 알고리즘 및 디지털 서명에의 응용", 한국통신 학회 논문집, 1996. 12

10] 박일남외, "합성 알고리즘을 이용한 안전한 문서화상 전송체계에 관한 연구", 한국통신학회 논문집, 1997

11] CCITT Study Group Ⅷ Contribution D134, "Explanation of the Use of the DTAM

and ODA Recommandations for Facsimile Group4," PTT Nerherlands, Study Group Ⅷ meeting, 5-14, October 1990, Geneva, Switzerland.

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

13] ITU-T Recommendation T.4, 1993

14] ITU-T Recommendation T.6, 1993

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

A Study on Security System of Document Image using Mixing Algorithm

Yoon-Seok, Heo*/Il-Kyung, Kim**/Il-Nam, Park***

Abstract

In this paper, we present a countermeasure for a various trouble occurred in secure communication of document image.

We propose a security system for transmission of document image using mixing algorithm that the third party cannot conceive secure transmission of information instead of existing scheme which depend on crypto-degree of security algorithm, itself. For this, RM, DM and RDM algorithm for mixing of secure bits are proposed and applied to digital signature for mixing for secure document and mixing for non-secure document by secure document. Security system for document image involves not only security scheme for document image transmission itself, but also digital signature scheme. The transmitter embeds secretly the signatures onto secure document, embeds it to non-secure document and transfers it to the receiver. The receiver makes a check of any forgery on the signature and the document. Because the total amount of transmitted data and the image quality are about the same to those of the original document image, respectively, the third party cannot notice the fact that signatures and secure document are embedded on the document image. Thus, the probability of attack will be reduced.

* Dept. of Electronics Eng., Chungcheong College.
** Dept. of Information Communication, Taedok College.
*** Dept. of Office Automation, Taedok College