정보학연구 제4권 제4호 2001년 12월(pp.25-35)
The Journal of Information Technology, Vol.4, No.4

차분 혼합 알고리즘을 이용한 디지틀 서명에 관한 연구

박일남*

요 약

본 논문은 문서상에 서명을 직접 합성하는 문서화상에 대한 디지털 서명 구조 를 제안한다. 서명에 소요되는 시간은 서명의 확산에 의해 감축된다. 본 구조에 의해 디지털 서명의 제 3 조건인 발신 부인 봉쇄가 실현된다. 발신자가 비밀리에 서명을 합성하여 전송하면 수신자는 서명과 문서상의 오류를 확인 할 수 있다. 본 구조는 ITU-T.4 규격과 호환한다.

Ⅰ. 서론

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 디지틀 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 시행한다 해도 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

* 대덕대학 컴퓨터정보통신계열 교수

제안되어 있으나[2,3,4], FAX 문서에 대한 서명은 데이터 통신의 인증법을 그대로 적용할 수도 없고 그 특수성으로 인해 연구가 미비한 상태이다. 차분혼합 알고리즘은 부호화 주사선(Coding Scan Line:이하 CSL)과 키에 의해 선택된 참조 주사선(Reference Scan Line:이하 RSL)의 변화 화소사이의 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 차분 혼합 알고리즘과 함께 DES 알고리즘 및 RSA 알고리즘을 적용한 디지틀 서명 구조를 제안한다.

II. 차분 혼합 알고리즘을 이용한 디지틀 서명

2.1 디지틀 서명 알고리즘

차분혼합 알고리즘을 이용한 서명 알고리즘을 그림 1에 제안한다. 이는 차분혼합 알고리즘의 특성을 이용하여 문서의 일부분에만 서명을 시행하여 서명 속도를 높였고 RSA 알고리즘을 적용하여 논문[7,8]의 문제점인 디지틀 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.

$$S'_{AB} = RSA(K_S , S_{AB})$$
$$S''_{AB} = DES(K_{AB} , S'_{AB})$$
$$S'_A = RSA(K_P , S_A) \quad \text{----------} \quad (2\text{-}1)$$

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.

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

분해된 모듈 단위로 각 모듈의 최후주사선 직전의 주사선을 찾아 차분혼합 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.

$$\begin{aligned} M' = {} & [M_1 + \Delta(M_1, S''_{AB}, K_{AB}) + \Delta(M_1, S'_A, K_A)] \\ & \cup [M_2 + \Delta(M_2, S''_{AB}, K_{AB}) + \Delta(M_2, S'_A, K_A)] \\ & \cup \cdots\cdots + \cdots\cdots \\ & \cup [M_n + \Delta(M_n, S''_{AB}, K_{AB}) + \Delta(M_n, S'_A, K_A)] \end{aligned}$$
$$\text{----------} \quad (2\text{-}3)$$

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

$$M'' = LCC\ (\ M'\ ) \text{ ---------- (2-4)}$$

수신자 B는 M″를 수신하여 복호화하여 디지틀 서명된 문서 M′를 구한다.

$$M' = LCC^{-1}\ (\ M''\ ) \text{ ---------- (2-5)}$$

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

$$M' = M'_1 \cup M'_2 \cup M'_3 \cup \cdots \cup M'_n \quad \text{---------- (2-6)}$$

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.

$$[S''_{AB}]_1 = \Delta^{-1}\ (M_1,[S''_{AB}]_1,K_{AB})$$
$$[S''_{AB}]_2 = \Delta^{-1}\ (M_2,[S''_{AB}]_2,K_{AB})$$
$$\vdots$$
$$[S''_{AB}]_n = \Delta^{-1}\ (M_n,[S''_{AB}]_n,K_{AB}) \text{ ------ (2-7)}$$

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

$$[S_{AB}']_1 = DES^{-1}(\ K_{AB}\ ,\ [S''_{AB}]_1\ )$$
$$[S_{AB}']_2 = DES^{-1}(\ K_{AB}\ ,\ [S''_{AB}]_2\ )$$
$$\vdots$$
$$[S_{AB}']_n = DES^{-1}(\ K_{AB},\ [S''_{AB}]_n\ ) \text{ ----- (2-8)}$$

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

$$[S_{AB}]_1 = RSA^{-1}(\ K_p\ ,\ [S_{AB}']_1)$$
$$[S_{AB}]_2 = RSA^{-1}(\ K_p\ ,\ [S_{AB}']_2\ )$$
$$\vdots$$
$$[S_{AB}]_n = RSA^{-1}(\ K_p\ ,\ [S_{AB}']_n\ ) \text{ ------ (2-9)}$$

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

$$(S_{AB}=[S_{AB}]_1)\ AND\ (S_{AB}=[S_{AB}]_2)\ AND$$
$$\cdots\ AND\ (S_{AB}=[S_{AB}]_n) \text{ -------- (2-10)}$$

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

$$(S_{AB}\neq[S_{AB}]_1)\ OR\ (S_{AB}\neq[S_{AB}]_2)\ OR$$
$$\cdots\ OR\ (S_{AB}\neq[S_{AB}]_n) \text{ ---------- (2-11)}$$

2.2 분쟁시 처리

한편 송신자 A는 수신자 B가 문서를 위조 하는등의 문제 발생시 다음의 절차를 실행한다.(그림 2) B가 제시한 문서($[M'']_S$)에 대해 식(2-5), 식(2-6)을 시행한후 모듈의 최후 주사선에서 비밀키 K_A로 복호를 실행하여 R용의 서명 데이타

$[S'_A]_S$를 추출한다.

$$[S'_A]_{S1} = \Delta^{-1}\ ([M']_{S1},[S'_A]_{S1},K_A)$$
$$[S'_A]_{S2} = \Delta^{-1}\ ([M']_{S2},[S'_A]_{S2},K_A)$$
$$\vdots$$
$$[S'_A]_{Sn} = \Delta^{-1}\ ([M']_{Sn},[S'_A]_{Sn},K_A) \text{ --- (2-12)}$$

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

$$[S_A]_{S1} = RSA(K_S , [S'_A]_{S1})$$
$$[S_A]_{S2} = RSA(K_S , [S'_A]_{S2})$$
$$\vdots$$
$$[S_A]_{Sn} = RSA(K_S , [S'_A]_{Sn}) \text{ ------ (2-13)}$$

송신자 A는 다음과 같은 경우 수신자 B의 위조를 인증한다.

$$(S_A \neq [[S_A]_{S1}) \text{ OR } (S_A \neq [S_A]_{S2}) \text{ OR}$$
$$\cdots \text{ OR } (S_A \neq [S_A]_{Sn}) \text{ ---------- (2-14)}$$

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 디지틀 서명된 문서 $[M']_R$을 복호한다.

$$[M']_R = LCC^{-1} ([M'']_R) \text{ ---------- (2-15)}$$

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

$$[M']_R=[M']_{R1} \cup [M']_{R2} \cup [M']_{R3} \cup \cdots$$
$$\cup [M']_{Rn} \text{ ---------- (2-16)}$$

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

$$[S''_{AB}]_{R1} = \Delta^{-1} ([M']_{R1},[S''_{AB}]_{R1},K_{AB})$$
$$[S''_{AB}]_{R2} = \Delta^{-1} ([M']_{R2},[S''_{AB}]_{R2},K_{AB})$$
$$\vdots$$
$$[S''_{AB}]_{Rn} = \Delta^{-1} ([M']_{Rn},[S''_{AB}]_{Rn},K_{AB}) \text{ ------- (2-17)}$$

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

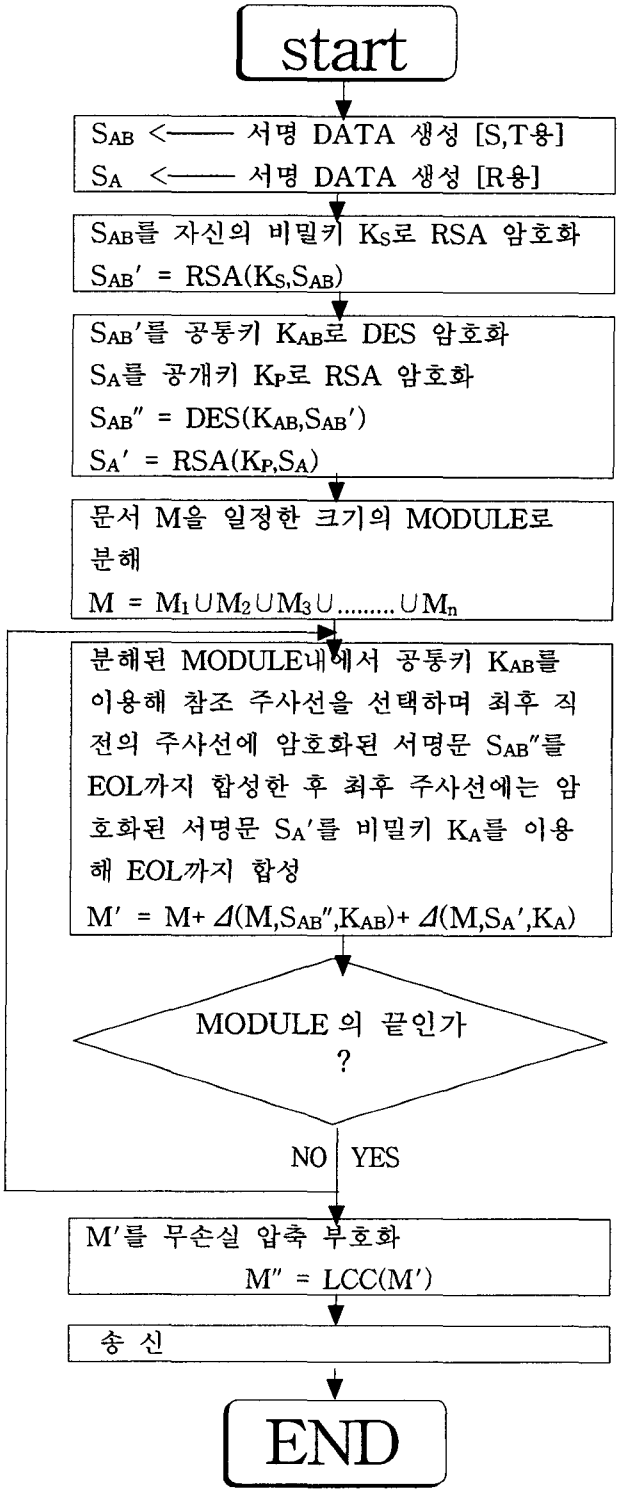
$$[S_{AB}']_{R1} = DES(K_{AB} ,[S''_{AB}]_{R1})$$
$$[S_{AB}']_{R2} = DES(K_{AB} ,[S''_{AB}]_{R2})$$
$$\vdots$$
$$[S_{AB}']_{Rn} = DES(K_{AB} ,[S''_{AB}]_{Rn}) \text{ ---- (2-18)}$$

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

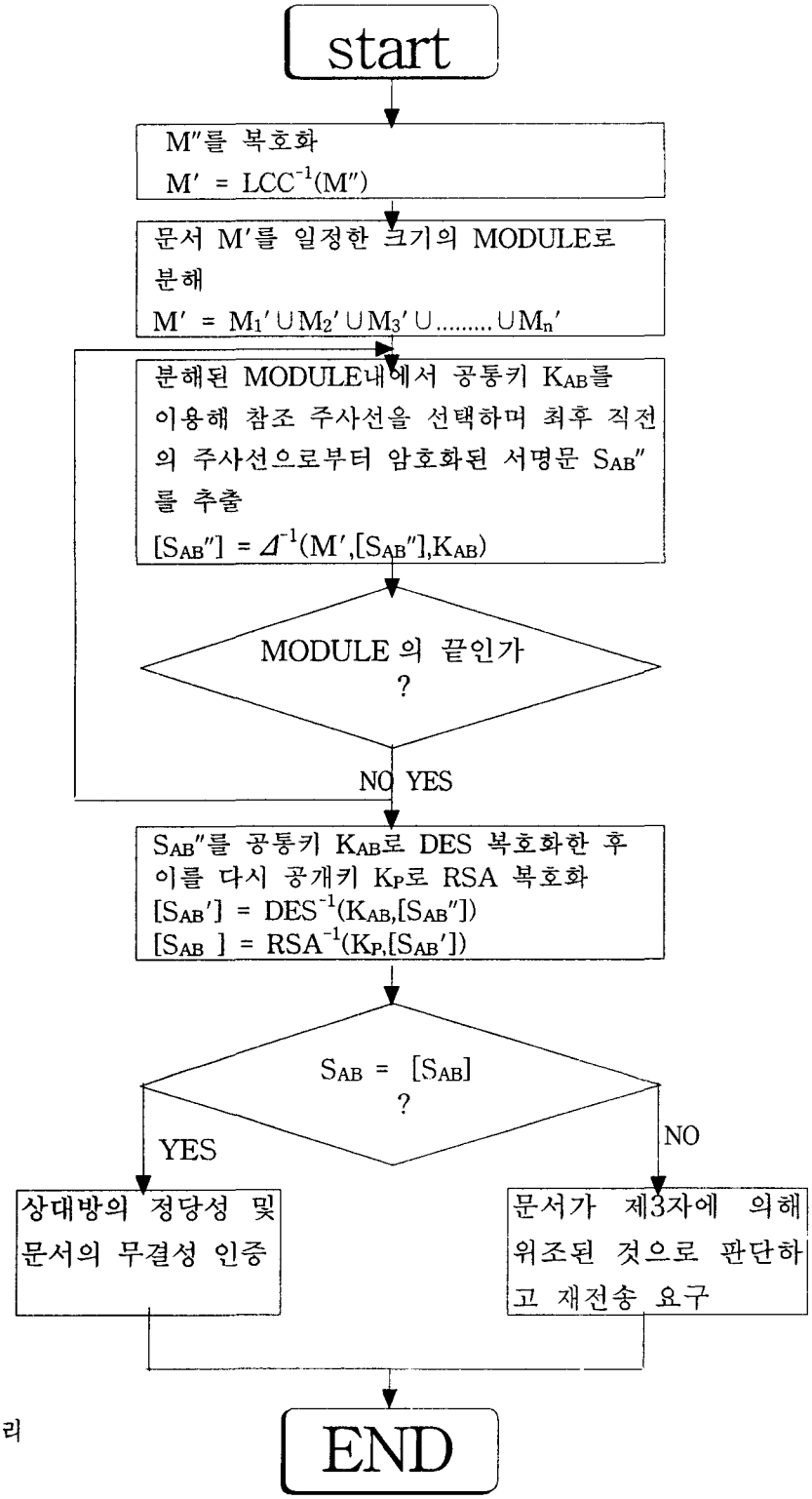
$$[S_{AB}]_{R1} = RSA(K_p ,[S_{AB}']_{R1})$$
$$[S_{AB}]_{R2} = RSA(K_p ,[S_{AB}']_{R2})$$
$$\vdots$$
$$[S_{AB}]_{Rn} = RSA(K_p ,[S_{AB}']_{Rn}) \text{ ---- (2-19)}$$

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.

$$(S_{AB})_1=[S_{AB}]_{R1} \text{ AND } (S_{AB})_2=[S_{AB}]_{R2} \text{ AND}$$
$$\cdots \text{AND } (S_{AB})_n=[S_{AB}]_{Rn} \text{ -------- (2-20)}$$

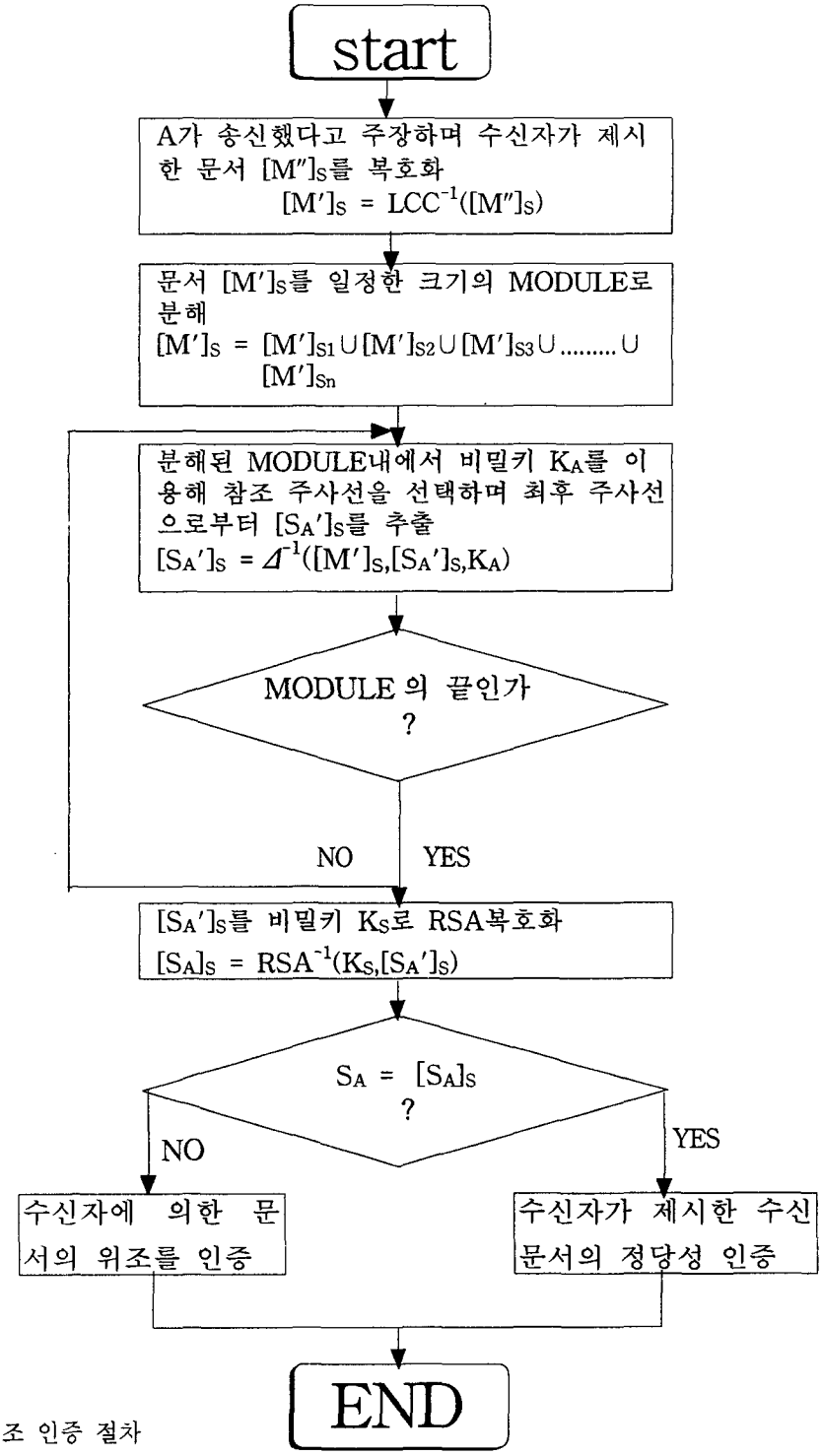

start
S_{AB} <—— 서명 DATA 생성 [S,T용]
S_A <—— 서명 DATA 생성 [R용]
S_{AB}를 자신의 비밀키 K_S로 RSA 암호화
$S_{AB}' = RSA(K_S, S_{AB})$
S_{AB}'를 공통키 K_{AB}로 DES 암호화
S_A를 공개키 K_P로 RSA 암호화
$S_{AB}'' = DES(K_{AB}, S_{AB}')$
$S_A' = RSA(K_P, S_A)$
문서 M을 일정한 크기의 MODULE로 분해
$M = M_1 \cup M_2 \cup M_3 \cup \ldots\ldots \cup M_n$
분해된 MODULE내에서 공통키 K_{AB}를 이용해 참조 주사선을 선택하며 최후 직전의 주사선에 암호화된 서명문 S_{AB}''를 EOL까지 합성한 후 최후 주사선에는 암호화된 서명문 S_A'를 비밀키 K_A를 이용해 EOL까지 합성
$M' = M + \Delta(M, S_{AB}'', K_{AB}) + \Delta(M, S_A', K_A)$
MODULE 의 끝인가 ?
NO
YES
M'를 무손실 압축 부호화
$M'' = LCC(M')$
송 신
END

a)송신측 처리

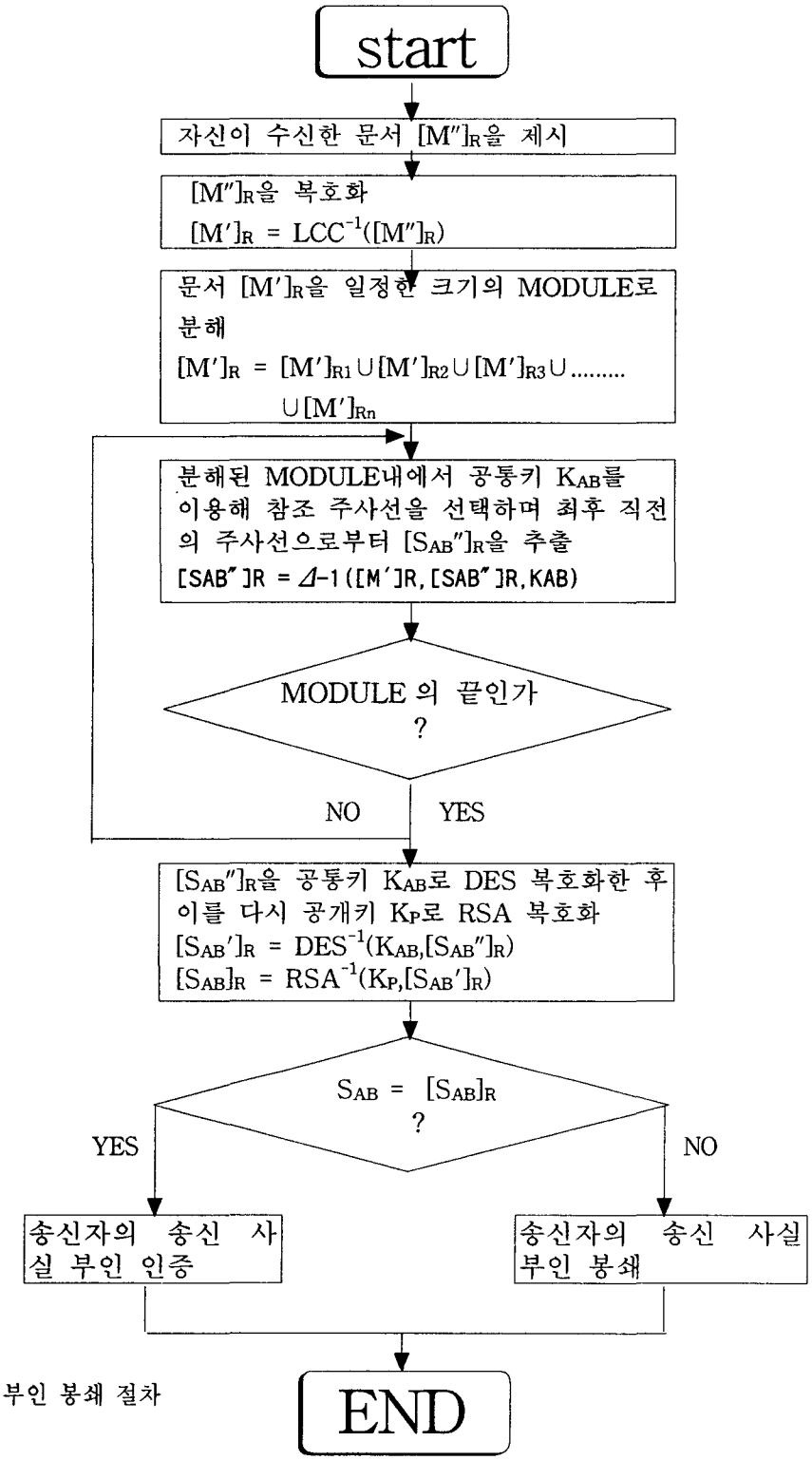


b) 수신측 처리

(그림 1) 차분혼합 알고리즘을 이용한 디지틀 서명 알고리즘


start
A가 송신했다고 주장하며 수신자가 제시한 문서 $[M'']_S$를 복호화
$[M']_S = LCC^{-1}([M'']_S)$
문서 $[M']_S$를 일정한 크기의 MODULE로 분해
$[M']_S = [M']_{S1} \cup [M']_{S2} \cup [M']_{S3} \cup ..... \cup [M']_{Sn}$
분해된 MODULE내에서 비밀키 K_A를 이용해 참조 주사선을 선택하며 최후 주사선으로부터 $[S_A']_S$를 추출
$[S_A']_S = \Delta^{-1}([M']_S, [S_A']_S, K_A)$
MODULE 의 끝인가 ?
NO
YES
$[S_A']_S$를 비밀키 K_S로 RSA복호화
$[S_A]_S = RSA^{-1}(K_S, [S_A']_S)$
$S_A = [S_A]_S$?
NO
YES
수신자에 의한 문서의 위조를 인증
수신자가 제시한 수신문서의 정당성 인증
END

a) 수신자 위조 인증 절차



b) 송신자 부인 봉쇄 절차

(그림 2) 분쟁시 처리 절차

Ⅲ. 비도 분석

문서상의 서명이 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_{DM}은 다음과 같다.

$$(P_{DM})_m = i^{-(j+1)} * m^j \text{ ---------- (3-1)}$$

따라서 문서 전체가 해독될 확률 P_{DM}은 다음과 같다.

$$P_{DM} = (i^{-(j+1)} * m^j)^m \text{ ---------- (3-2)}$$

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

Ⅳ. 결론

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 변화화소의 거리의 우기성을 이용한 차분혼합 합성 알고리즘을 이용하여 FAX 문서에 디지틀 서명의 3 조건인 [T],[R],[S]조건을 만족하는 디지틀 서명을 시행하는 알고리즘을 제안하였다. ITU의 TEST CHART를 대상으로 실험한 결과, 차분혼합 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 디지틀 서명 뿐아니라 비밀문서를 일반문서에 합성할 경우에 대한 연구가 필요할 것이며 이를 위해서는 보다 다량의 데이터를 합성할 수 있는 알고리즘을 개발해야할 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] 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", 신호처리학회 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] 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 디지틀 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.

A Study On Digital Signature Using Distance Mixing Algorithm

Il-Nam, Park*

Abstract

This paper presents a digital signature scheme for document image which directly embeds a signature onto the document. 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(CCITT G3 or G4 facsimile standards).

* Dept. of Computer & Information Communication, Taeduk college