論文 97-22-11-20

합성 알고리즘을 이용한 안전한 문서화상 전송체계에 관한 연구

正會員 朴 一 男*, 李 大 寧**

A Study On Secure Transmission System For Document Image Using Mixing Algorithm

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

요 약

본 논문에서는 문서 화상에 대한 합성에 의한 안전한 전송 체계을 제 안한다. 이를 위해 앞서 제안한 바 있는 DM 및 RDM 알고리즘을 적용한다. 문서 화상의 보안 체계는 문서 자체의 보안 뿐아니라 문서의 무결성과 사용자의 정당성을 인증하기 위한 디지털 서명 체계가 포함된다. 디지털 서명된 보안 문서는 비보안 문서에 합성되고, 이는 합성 여부의 시각적 구분이 어려워 제 3자에게는 통상의 문서 교환으로 인식될 것이다.

ABSTRACT

This paper presents a secure transmission system for document image using mixing algorithm. For this, we apply DM and RDM algorithm propoposed before. The transmitter embeds secretly the signature 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. The total amount of data transmitted and the image quallity are about the same to that of the original document. Thus, a third party can not notice the fact that signatures and secure document is embedded on the document.

Ⅰ. 서 론

문서 화상을 포함한 화상 정보에 대한 보안을 위한 몇몇 연구[1, 2, 3, 4, 5, 6]가 있었으나 이는 대개 화상을 스크램블(Scramble)하거나[1, 2, 3, 4, 5, 6] 화상에 가장 영향을 미치는 부분만을 기존에 연구된 암호 알고리즘으로 암호화하는것[5, 6]이 대부분이었다. 이와 같은 방식은 문서의 암호화 사실을 제 3자에게 노출시키는 방식으로 이의 보안은 암호 알고리즘이 갖는 비도(Crypto-degree)에 의존하게되므로 매우 강한 암호 알

*경희대학교 전자공학과
論文番號:97216-0627
接受日字:1997年 6月 27日

고리즘을 적용하지 않는 한 문서의 보안(Security)을 보장할 수 없으며 이러한 강한 암호의 적용은 문서 화상의 데이터량을 고려할 때 과대한 시간이 소요된다. 또한 기존의 연구는 거의 화상을 목적지까지 비밀리에 보내는데 초점을 맞추고 있어 민감한 문서의 교환시 상호간 이익에 관계된 민감한 분쟁을 해결하기 어렵다. 다시 말해 기존의 문서 화상의 보안 서비스는 데이터 비밀 보장 서비스를 제공하는데에 국한되어 있었기 때문에 화상 통신에서 요구되는 상대방의 신분 확인 서비스(Identification),데이터 무결성 서비스(Data integrity), 송수신자의 송수신 부인 봉쇄 서비스(Non-repudiation)등을 제공하지 못하고 있어 분쟁의 소지가 많은 상태이다. 본 논문은 문서 화상의 보안을 위해서 기존에 연구되어온 각종 암호화 방식 및 스크램블 방식과 같이 정보의 보안 여부를 노출시키고 비도에 의지하는 방식과 달리 정보의 보안 여부를 제 3자가 판독하기 어렵도록하여 일상의 문서 교환으로 인식하게함으로써 1차적으로 이의 해독에 따른 위험을 감소시키고 2차적으로는 해독이 가해진다해도 알고리즘 자체의 비도에 의해 해독을 용이하지 않도록 하는 방식의 보안 구조를 제안한다. 이러한 보안 체계의 구성을 위해 Bit 합성에 의한 문서의 보안 기법으로 부호장(Runlength)의 우기성(Even-Odd Feature)을 이용해 합성 하고자 하는 BIT열에 따라 부호장을 신축 조절하여 합성을 시행하는 RM (Runlengh Mixing) 알고리즘[7, 8, 9]과 참조 주사선의 변화화소와 부호화 주사선의 변화화소의 거리의 우기성을 이용해 역시 합성 하고자 하는 BIT열에 따라 변화 화소간 거리를 신축 조절하여 합성을 시행하는 DM (Distance Mixing)알고리즘[10] 그리고 앞의 두가지 방식의 합성 알고리즘의 개념을 결합하여 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 신축 조작함으로써 2비트의 동시 합성을 구현한 RDM(Runlength & Distance Mixing) 알고리즘[11] 및 이를 이용한 디지털 서명 방식(Digital Signature Scheme)을 제안한 바 있다. 본 논문에서는 앞서 제안한 합성 알고리즘중 DM 및 RDM 알고리즘을 적용해 보안 체계를 구성한다. 이를 위해 문서 화상에 대한 보안 서비스 구현을 위한 디지털(Digital) 서명에는 합성량보다 서명 실행 속도가 우선이므로 DM 알고리즘을 적용하고 비밀 문서의 보안을 위한 합성에는 합성량을 고려해 RDM 알고리즘을 적용한다. 보안 서비스를 위한 디지털 서명의 [T], [S], [R] 조건중 [S], [R] 조건[12, 13, 14, 15]을 만족시키기 위해 서명 데이터의 암호화에 기존의 공개키 암호화 방식인 RSA 알고리즘[16, 17]을 적용한다. 본 논문의 보안 체계를 적용할 경우 우선 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 않게되며, 송 수신자간의 분쟁시 디지털 서명에 의해 이를 해결할 수 있다. 본 논문은 우선 DM, RDM 및 RSA 알고리즘[16, 17]을 적용한 보안 체계를 제시하고 분쟁시의 처리 절차를 제시한다. 실험을 통해 제안한 보안 체계를 적용한 예를 분석한 후 본 보안 체계의 안전성을 비도 측면에서 분석한다.

Ⅱ. FAX문서에 대한 보안 체계

2.1 FAX문서의 보안 체계 및 처리 절차

그림 1에 FAX문서의 보안 체계를 제시한다.

우선 송신 측에서는 서명(Signatures)을 보안 문서(Secure Document:이하 SD)에 합성하여 디지털 서명을 시행한 후, 이를 다시 비보안 문서(Non-Secure Document:이하 NSD)에 합성하여 디지털 서명된 보안 문서를 수신 측에 보안 송신하면 수신 측에서는 역 수순에 의해 SD 및 디지털 서명을 분리함으로써 보안 송 수신 및 문서의 무결성과 인증을 구현한다.

디지털 서명의 3가지 조건 즉, [T], [R], [S] 조건을 동시에 만족하도록 하기 위해 기존의 대표적인 공개키 암호 방식인 RSA 알고리즘을 앞서 제안한 바 있는 서명 실행 속도에서 우수한 DM 합성 알고리즘과 함께 적용하였다. 보안 문서의 합성시에는 RDM 알고리즘을 적용하여 합성량을 높였다. 구체적인 송 수신 처리 절차는 그림 2와 같다.

우선 송신자 A는 S, T용의 서명 데이터 S_{AB}와 R용의 서명 데이터 S_A를 생성하여 이의 보안을 위해 각

각 자신의 비밀키 K_{SA}와 B의 공개키 K_{PB}를 이용해 RSA 암호화한다.

$$S_{AB}' = E(K_{SA}, S_{AB})$$
$$S_{AB}'' = E(K_{PB}, S_{AB}')$$
$$S_{AB}' = E(K_{SA}, S_A) \quad (2\text{-}1)$$

그후 A는 보안 문서 SD를 일정 크기의 모듈(Module)로 분해(이하 수식에서는 합집합의 의미로 기호 ∪를 사용)한다.

$$SD = SD_1 \cup SD_2 \cup SD_3 \cup \cdots \cup SD_n \quad (2\text{-}2)$$

분해된 모듈 단위로 각 모듈의 최후주사선 직전의 주사선을 찾아 DM 알고리즘을 이용해 그 주사선의 처음부터 끝까지(EOL) 암호화된 [S], [T]용의 서명 데이터 S_{AB}''를 A, B간 공통키 K_{AB}를 이용해 합성한 후 최후 주사선에는 EOL까지 암호화된 [R]용의 서명 데이터 S_A'를 자신의 비밀키 K_A를 이용해 합성한다.

$$\begin{aligned} SD' = &[SD_1 \cup DM(SD_1, S_{AB}'', K_{AB}) \cup DM(SD_1, S_A', K_A)] \\ &\cup [SD_2 \cup DM(SD_2, S_{AB}'', K_{AB}) \cup (SD_2, S_A', K_A)] \\ &\cup \cdots \qquad\qquad \cup \quad \cdots \\ &\cup [SD_n \cup DM(SD_n, S_{AB}'', K_{AB}) \cup DM(SD_n, S_A', K_A)] \end{aligned} \quad (2\text{-}3)$$

송신자 A는 속도 향상 및 전송 부호량 감소를 위해 디지털 서명된 문서 SD'를 무손실 압축부호화(Lossless Compression Coding: 이하 LCC)한다.

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

비보안 문서 NSD를 RSL부와 RDM 합성부로 나눈다.

$$NSD = NSD_{RSL} \cup NSD_{RDM} \quad (2\text{-}5)$$

RDM 합성부에는 RDM 알고리즘을 이용해 RSL부에서 RSL을 공통의 암호화키 K_{AB}를 이용해 선택한 후 SD''를 합성한다. 이때 RSL부는 하나의 주사선에 대한 합성이 끝날때마다 하나의 주사선 씩 아래로 이동(Down shift)한다.

$$[NSD_{RDM}]' = NSD_{RDM} \cup RDM(NSD_{RDM}, SD'', K_{AB}) \quad (2\text{-}6)$$

마지막으로 보안 문서가 합성된 비 보안 문서 [NSD]'를 무손실 압축 부호화한 후 송신한다.

$$[NSD]'' = LCC([NSD]') \quad (2\text{-}7)$$

여기서는 MH, MR, MMR[18, 19, 20]등을 적용할 수 있다.

수신 측 처리 절차는 다음과 같다.

우선 수신자 B는 [NSD]''를 수신하고 이를 복호화하여 [NSD]'를 구한다.

$$[NSD]' = LCC^{-1}([NSD]'') \quad (2\text{-}8)$$

복호된 비보안 문서 [NSD]'를 RSL부와 RDM 합성부로 나눈다.

$$[NSD]' = [NSD_{RSL}]' \cup [NSD_{RDM}]' \quad (2\text{-}9)$$

RDM 합성부에서 RDM 추출 알고리즘[이하 수식에서는 RDM^{-1}로 표기]을 이용해 공통키 K_{AB}로 RSL부에서 RSL을 선택하면서 SD''를 추출한다. 이때 RSL부는 하나의 CSL에서의 추출이 끝날때마다 하나의 주사선씩 아래로 이동(Down shift)한다.

$$SD'' = RDM^{-1}([NSD_{RDM}]', SD'', K_{AB}) \quad (2\text{-}10)$$

단 RDM^{-1}은 RDM 추출 알고리즘을 의미한다.

SD''를 복호해서 디지털 서명된 보안 문서 SD'를 구한다.

$$SD' = LCC^{-1}(SD'') \quad (2\text{-}11)$$

다음은 디지털 서명된 보안 문서 SD'를 송신자 A와 사전에 약속된 크기의 모듈로 분해한다.

$$SD' = SD'_1 \cup SD'_2 \cup SD'_3 \cup \cdots \cup SD'_n \quad (2\text{-}12)$$

DM 추출 알고리즘[이하 수식에서는 DM-1로 표기]을 이용해 분해된 모듈단위로 부터 각 모듈의 최후 주사선 직전의 주사선을 찾아 그 주사선의 처음부터 EOL까지 합성되어 있는 **암호화된 [S], [T]**용의 서명 데이터 S_{AB}''를 추출한다.

$$[S_{AB}'']_1 = DM^{-1}(SD'_1, [S_{AB}'']_1, K_{AB})$$
$$[S_{AB}'']_2 = DM^{-1}(SD'_2, [S_{AB}'']_2, K_{AB})$$
$$\vdots$$
$$[S_{AB}'']_n = DM^{-1}(SD'_n, [S_{AB}'']_n, K_{AB}) \quad (2\text{-}13)$$

단,DM^{-1}은 DM 추출 알고리즘을 의미한다.

추출된 $[S_{AB}'']_1$, $[S_{AB}'']_2$,…,$[S_{AB}'']_n$을 B의 비밀키 KSB를 이용해 RSA 복호한다.

$$[S_{AB}']_1 = D(K_{SB}, [S_{AB}'']_1)$$
$$[S_{AB}']_2 = D(K_{SB}, [S_{AB}'']_2)$$
$$\vdots$$
$$[S_{AB}']_n = D(K_{SB}, [S_{AB}'']_n) \quad (2\text{-}14)$$

이를 다시 A의 공개키 K_{PA}로 RSA복호하여 S_{AB}를 구한다.

$$[S_{AB}]_1 = D(K_{PA}, [S_{AB}']_1)$$
$$[S_{AB}]_2 = D(K_{PA}, [S_{AB}']_2)$$
$$\vdots$$
$$[S_{AB}]_n = D(K_{PA}, [S_{AB}']_n) \quad (2\text{-}15)$$

수신자 B는 다음의 경우 상대방을 인증함과 동시에 문서의 무결성을 인증한다.

$$(S_{AB} = [S_{AB}]_1) \text{ AND } (S_{AB} = [S_{AB}]_2) \text{ AND } \cdots \text{ AND } (S_{AB} = [S_{AB}]_n) \quad (2\text{-}16)$$

단, AND 기호는 동시에 만족한다는 의미로 나타낸다.

그러나 다음과 같은 경우 위조 부분을 검출함과 동시에 송신 측에 재전송을 요구한다.

$$(S_{AB} \neq [S_{AB}]_1) \text{ OR } (S_{AB} \neq [S_{AB}]_2) \text{ OR } \cdots \text{ OR } (S_{AB} \neq [S_{AB}]_n) \quad (2\text{-}17)$$

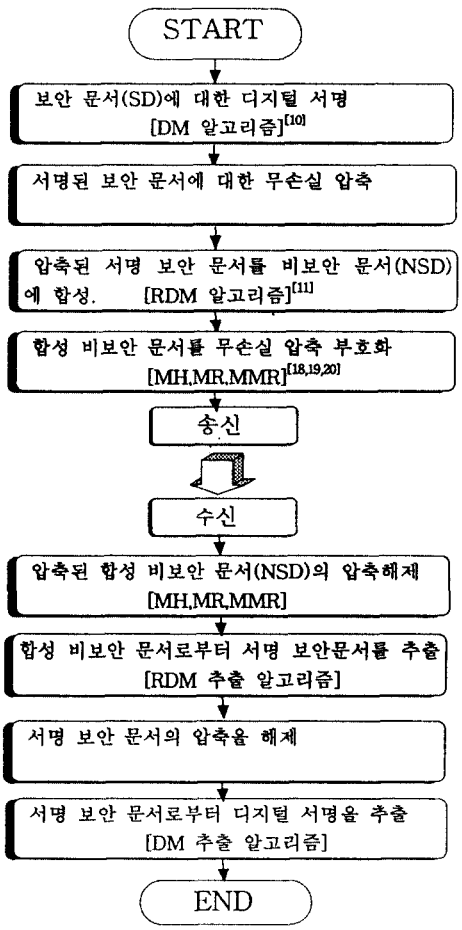
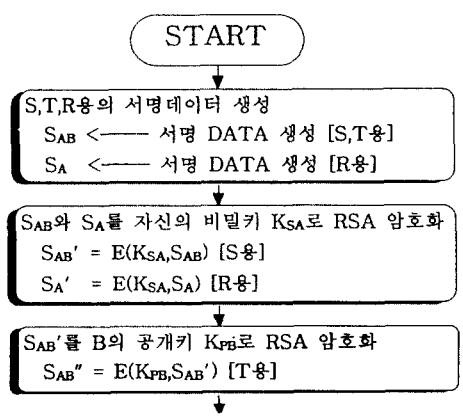
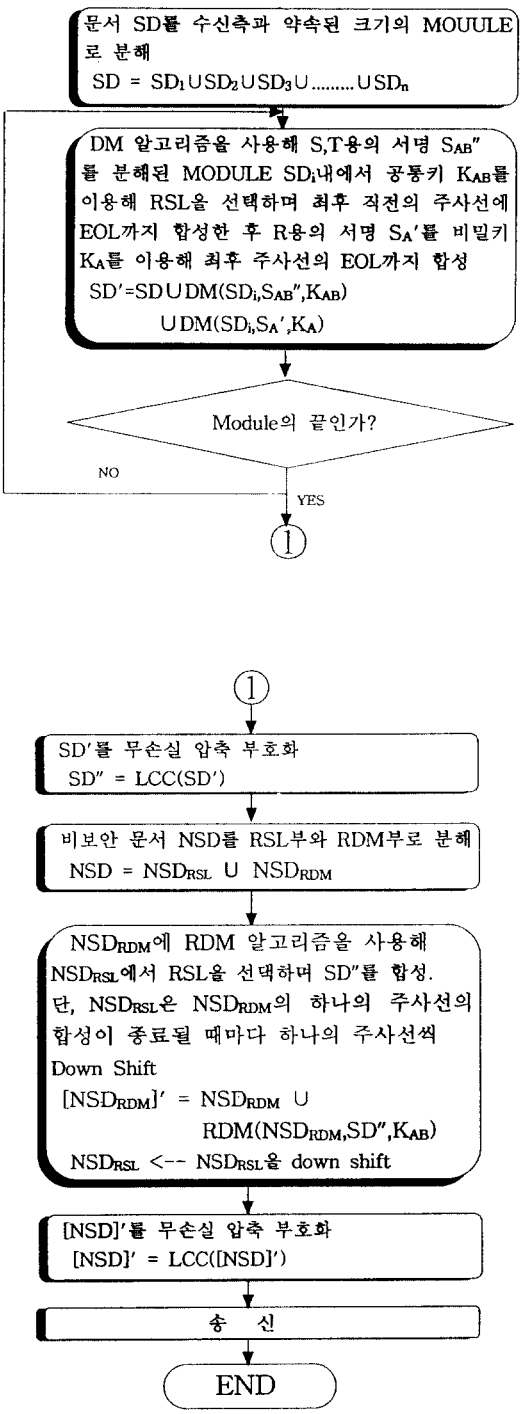
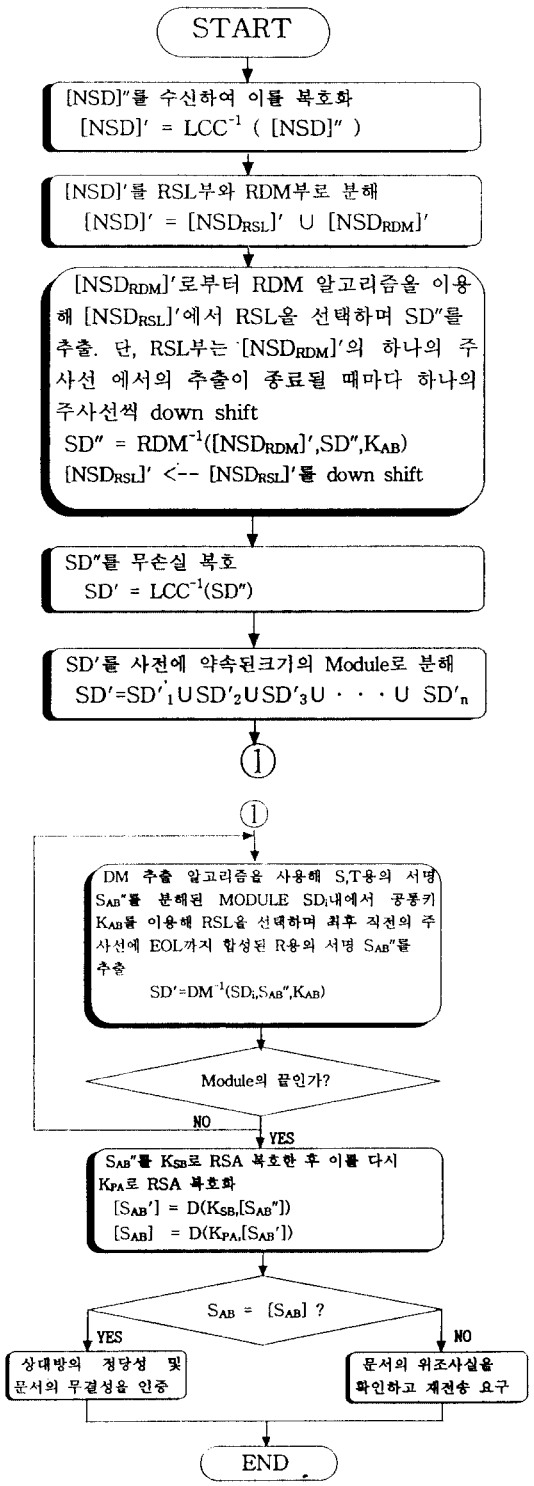


그림 1. FAX문서에 대한 보안 체계
Fig 1. Security System for FAX document





a) 송신측 처리 절차



b) 수신측 처리 절차

그림 2. 송수신 측 처리 절차
Fig. 2. Implementation procedure of proposed system

단, OR 기호는 여러개중에 하나만을 만족해도 된다는 의미를 나타낸다.

2.2 분쟁시 처리 절차

분쟁시 처리 절차는 그림 3과 같다. 우선 송신자 A는 수신자 B가 문서를 위조 하는등의 문제 발생시 다음의 절차를 실행한다. 우선 송신자 A는 수신자가 A가 송신했다고 제시하는 문서 $[SD'']_S$에 대해 식(2-9)부터 식(2-12)의 절차를 시행한 후 각 모듈의 최후 주사선에서 자신의 비밀키 KA를 이용해 [R]용의 서명 데이터 $[S_A']_S$를 추출한다.

$$[S_A']_{S1} = DM^{-1}([SD']_{S1}, [S_A']_{S1}, K_A)$$
$$[S_A']_{S2} = DM^{-1}([SD']_{S2}, [S_A']_{S2}, K_A)$$
$$\vdots$$
$$[S_A']_{Sn} = DM^{-1}([SD']_{Sn}, [S_A']_{Sn}, K_A) \quad (2\text{-}18)$$

추출된 $[S_A']_{S1}$, $[S_A']_{S2}$,…,$[S_A']_{Sn}$을 A의 공개키 K_{PA}를 이용해 RSA 복호한다.

$$[S_A]_{S1} = D(K_{PA}, [S_A']_{S1})$$
$$[S_A]_{S2} = D(K_{PA}, [S_A']_{S2})$$
$$\vdots$$
$$[S_A]_{Sn} = D(K_{PA}, [S_A']5_{Sn}) \quad (2\text{-}19)$$

송신자 A는 다음과 같은 경우 수신자 B의 위조를 인증한다. ([R]조건)

$$(S_A \neq [S_A]_{S1}) \text{ OR } (S_A \neq [S_A]_{S2} \text{ OR}$$
$$\cdots \text{ OR } (S_A \neq [S_A]_{Sn}) \quad (2\text{-}20)$$

수신자는 수신 문서에 대해 송신자가 송신 사실을 부인할 경우 다음과 같은 절차를 밟는다. 우선 수신자는 자신이 송신자 A로 부터 수신했다고 주장하는 문서 $[S_D']_R$로 부터 식(2-9)부터 식(2-12)의 절차를 시행한 후 분해된 모듈단위로 각 모듈의 최후 주사선 직전의 주사선을 찾아 그 주사선의 처음부터 EOL까지 DM 추출 알고리즘을 이용해 합성되어 있는 암호화된 [S], [T]용의 서명 데이터 $[S_{AB}'']_R$을 추출한다.

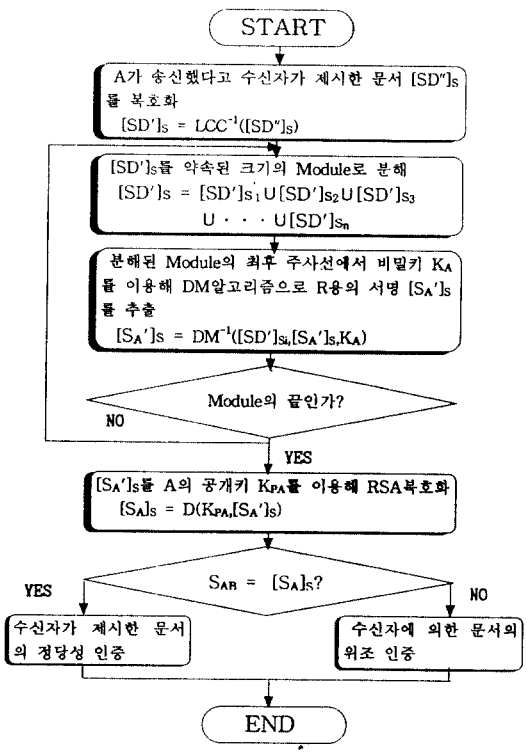
$$[S_{AB}'']_{R1} = DM^{-1}([SD']_R, [S_{AB}'']_{R1}, K_{AB})$$
$$[S_{AB}'']_{R2} = DM^{-1}([SD']_R, [S_{AB}'']_{R2}, K_{AB})$$
$$\vdots$$
$$[S_{AB}'']_{Rn} = DM^{-1}([SD']_R, [S_{AB}'']_{Rn}, K_{AB}) \quad (2\text{-}21)$$

그 후 추출된 $[S_{AB}'']_{R1}$, $[S_{AB}'']_{R2}$,…,$[S_{AB}'']_{Rn}$을 B의 비밀키 KSB를 이용해 RSA 복호한다.

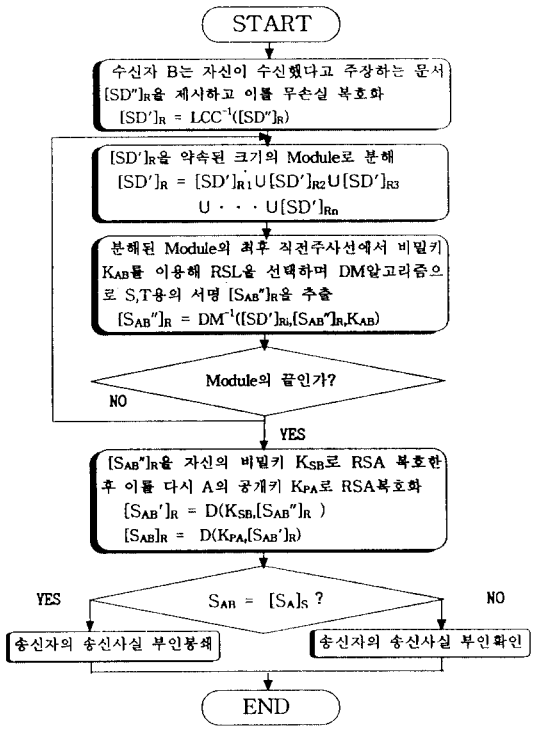
$$[S_{AB}']_{R1} = D(K_{SB}, [S_{AB}'']_{R1})$$
$$[S_{AB}']_{R2} = D(K_{SB}, [S_{AB}'']_{R2})$$
$$\vdots$$
$$[S_{AB}']_{Rn} = D(K_{SB}, [S_{AB}'']_{Rn}) \quad (2\text{-}22)$$

이를 다시 A의 공개키 K_{PA}로 RSA복호하여 $[S_{AB}]_R$을 구한다

$$[S_{AB}]_{R1} = D(K_{PA}, [S_{AB}']_{R1})$$
$$[S_{AB}']_{R2} = D(K_{PA}, [S_{AB}']_{R2})$$
$$\vdots$$
$$[S_{AB}]_{Rn} = D(K_{PA}, [S_{AB}']_{Rn}) \quad (2\text{-}23)$$



a) 수신자 B의 문서 위조 인증 절차(송신측 처리)



b) 송신자 A의 송신 부인 봉쇄 절차(수신측 처리)

그림 3. 분쟁시 처리 절차
Fig 3. Processing Procedure in a trouble

이때 $[S_{AB}']_R$은 송신자 A 자신의 비밀키 K_{SA}에 의해 공개키 암호화된 것으로 A의 공개키 K_{PA}에 의해서만 해독되므로 복호된 서명이 정상적인 경우 수신자가 제시한 문서 $[SD"]_R$의 송신 사실을 부인할 수 없게 된다. 즉, 다음과 같은 경우 송신자는 송신 사실을 부인할 수 없다.

([S]조건)

$$(S_{AB})_1 = [S_{AB}]_{R1} \text{ AND } (S_{AB})_2 = [S_{AB}]_{R2} \text{ AND } \cdots \text{ AND } (S_{AB})_n = [S_{AB}]_{Rn} \quad (2\text{-}24)$$

Ⅲ. 실험 및 고찰

본 논문에서 제안된 알고리즘에 대해 ITU의 FAX용 TEST화상(1024 × 723)[18, 19] 두개를 선택하여 PC상에서 실험을 행하였다. 실험 결과는 다음과 같다.

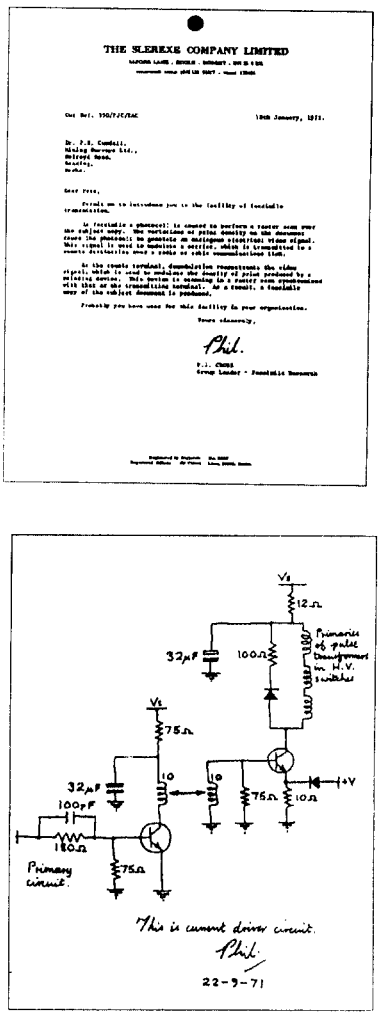


그림 4. ITU.T4 문서화상
Fig 4. ITU.T4 TEST CHART

서명 데이터 : DIGITAL SYSTEM LAB
01000100 01001001 01000111 01001001 01100011 01000001
01010011 00100000 01100010 01101000 01100010 01100011
01000101 01010100 00100000 01010011 01000001 01000010

RSA 암호화된 데이터
01001111 01000010 01001100 01000010 01011111 01001010
01000111 00101011 01011000 01010010 01011000 01011111
01001110 01000110 00101011 01000111 01001010 01001001

나.RSA 알고리즘에서 공개키와 비밀키 선택은 다음과 같다.
[P=11,Q=13,N=P*Q=143,ϕ=(P-1)(Q-1)=120,E*D=1modϕ(N)
E=11,D=11]

a) S, T용의 서명 데이터 및 암호화

서명 데이터 : PARK IL NAM 036					
01010000	01000001	01010010	01001011	00100000	01001001
01001100	00100000	01001110	01000001	01001101	00100000
00110000	00110011	00110110	00100000		

RSA 암호화된 데이터					
01011011	01001010	01011001	01000000	00101011	01000010
01000111	00101011	01000101	01001010	01000110	00101011
00111011	00111000	00111101	00111011		

b) R용의 서명 데이터 및 암호화

그림 5. 서명 데이터의 암호화

Fig 5. Encryption of signature data

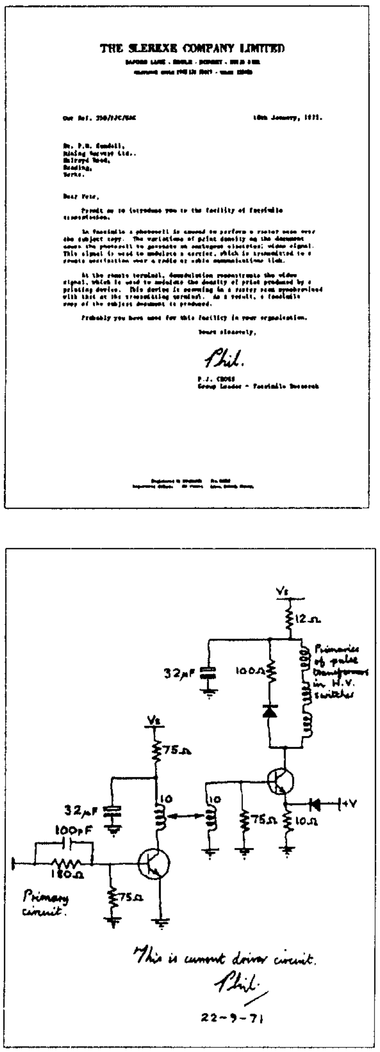
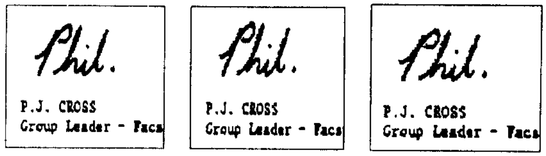


그림 6. 서명데이터가 합성된 T.4 문서화상

Fig 6. T.4 test chart mixed by signature data



(a) 원 문서 화상　(b) DM 서명 문서　(c) RDM 합성 문서

그림 7. 합성된 문서와의 비교

Fig 7. Comparison between mixing test chart and original test chart

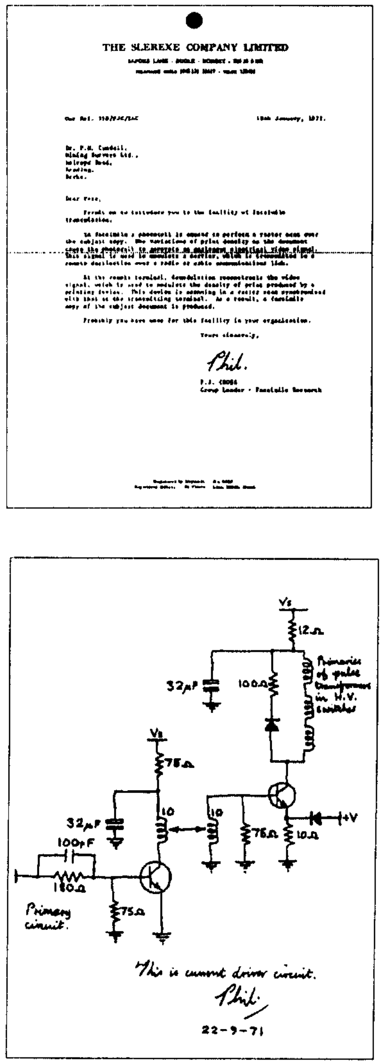


그림 8. 보안 문서가 합성된 문서 화상

Fig 8. Document image mixed by secure document

표 1. 합성 가능량 및 부호량의 변화 비교
Table 1. Comparison of mixing capability and change in quantity of code

실험결과 실험차트	합성 가능량 (단위:BIT)				부호량의 변화 (단위:BIT)			
ITU-TES0T CHART (N0 1)	RM [7]	DM [10]	RDM	증가율 [DM 비교]	합성부 호화 전	RM	DM	RDM
	6188	9243	18080	95.6 %	740352	178812	181374	168899
						24.15%	24.45%	22.81%
ITU-TEST CHART (NO 2)	RM	DM	RDM	평균 증가율	합성부 호화 전	RM	DM	RDM
	5102	5359	10740	100.4 %	740352	107625	107886	107498
						14.54%	14.57%	14.52%

단, 문서화상의 크기:(1024*723 = 740352)

단,RSA 알고리즘에서 공개키와 비밀키 선택은 다음과 같다.

[P = 11, Q = 13, N = P*Q = 143,
ϕ = (P-1)(Q-1) = 120, E*D = 1modϕ(N)
E = 11, D = 11]

여기서 합성하는 데이터는 DM, RDM 합성 모두 p21 그림 5의 RSA 암호화된 데이터이고 합성되는 문서 화상은 그림 4의 ITU.T4 TEST CHART NO1, N02 이다.

그림 4, 6, 8에서 보는 바와 같이 원 문서 화상과 서명이 합성된 문서 화상간의 시각적인 차이를 느낄 수 없어 비밀 서명이 확보되며 보안 문서가 합성된 문서 화상의 합성 여부의 구분이 어렵고 합성 여부를 안다 하더라도 스크램블 처리에 의해 문서의 보안이 가능한 것을 확인할 수 있었다. 표 1에서와 같이 앞서 발표한 RM 합성 방법[7] 및 DM 합성 방법[10]에 비교했을 때 합성 가능량이 상당히 증가함을 확인하였다. 또한 합성 전후의 전송 부호량의 변화가 거의 없어 부호량의 증대에 따른 부하가 거의 없음을 확인하였다.

본 알고리즘은 기본적으로 세 3자로 하여금 보안 여부를 위장하여 통상의 문서 교환으로 인식하게 하여 공격의 가능성을 줄였지만 만일 공격이 가해지는 경우의 안전성을 검토한다. NSD에 합성된 SD가 해독될 확률을 비도(Crypto-degree)로 평가하면 다음과 같다. 우선 합성 알고리즘 자체가 공개되었고 DM 알고리즘의 모듈의 크기와 RSL부의 크기도 공개(즉,합성 위치가 공개)되었다고 가정한다. 문서 화상의 해상도를 (i*j), RSL부인 NSD_{RSL}의 주사선 수를 s라 할 때 보안 문서중 하나의 주사선이 해독될 확률 $(P_{SD})_{1L}$은 다음과 같다.

$$(P_{SD})_{1L} = s^{-j} \tag{3-1}$$

그리고 한 줄의 문장의 주사선 수를 1라 할 때 한 줄의 문장이 해독될 확률 $(P_{SD})_{1S}$는 다음과 같다.

$$(P_{SD})_{1S} = s^{-j*i} \tag{3-2}$$

또한 한장의 NSD내에 합성된 SD 전체가 해독될 확률 $(P_{SD})_{1T}$는 다음과 같다.

$$(P_{SD})_{1T} = s^{-(i*j+j*s} \tag{3-3}$$

SD의 합성 위치가 공개되지 않은 경우는 각각 다음과 같다.

$$\begin{aligned}(P_{SD})_{1L} &= s^{-(i*j} \\ (P_{SD})_{1S} &= s^{-(i*j)*1} \\ (P_{SD})_{1T} &= s^{-(i*s)+(i*j*s}\end{aligned} \tag{3-4}$$

합성 위치를 공개하지 않는 경우 비도가 상당히 증가함을 알 수 있다. 여기서 i^2*j는 $i*j*s$에 비해 매우 크므로 본 방식의 해독을 위한 시간 복잡도(Time complexity)는 $O(n^k)$(단, $n \ll k$)로 볼 수 있고,따라서 시간 복잡도가 O(n!)인 기존의 스크램블 방식[1]에 비해 매우 안전함을 알 수 있다.

보안 문서 SD상의 서명이 해독될 확률은 다음과 같다. SD의 모듈 수를 m이라 하면 1개의 모듈내에는 i/m개의 주사선이 존재하게되므로 1개의 모듈내의 서명이 노출될 확률 $(P_{SN})_{1m}$은 다음과 같다.

$$(P_{SN})_{1m} = i^{-(j+1)} * m^j \quad (3\text{-}5)$$

따라서 문서 전체의 서명이 노출될 확률 $(P_{SN})_{1T}$은 다음과 같다.

$$(P_{SN})_{1T} = (i^{-(j+1)} * m^j)^m \quad (3\text{-}6)$$

[1]이때 보통 $i \gg m$이므로 서명이 노출될 시간 복잡도는 $O(n^k)$ 로 볼 수 있고 여기에 RSA 알고리즘 자체의 안전성을 고려할 때 서명이 해독되어 보안 문서가 위조될 가능성은 거의 없으므로 매우 안전함을 알 수 있다.

Ⅳ. 결 론

본 논문에서는 문서 화상에 대한 합성에 의한 보안 체계을 제안하였다. 이를 위해 앞서 제안한 바 있는 DM 및 RDM 알고리즘을 각각 디지털 서명 및 보안 문서 합성에 적용하였다. 또한 디지털 서명의 [T], [S], [R] 조건을 만족시키기 위해 서명 데이터의 암호화에 기존의 대표적 공개키 암호화 방식인 RSA 알고리즘을 적용하였다. ITU의 TEST CHART를 대상으로 실험한 결과 보안 문서의 합성시 합성 전후 부호량의 변화가 거의 없어 합성에 따른 부하가 거의 없었고 합성 후의 문서상에서의 합성 여부를 뚜렷히 느낄 수 없어 제 3자에게는 통상의 문서 교환으로 인식될 것이며 합성 여부를 예측한다 해도 알고리즘 자체가 갖는 비도에 의해 충분히 안전함을 확인하였다. 본 논문의 보안 체계를 적용할 경우 우선 문서의 보안 전송 여부를 제 3자가 판독할 수 없게되어 1차적으로는 공격(Attack)의 가능성을 줄이고 2차적으로는 공격이 가해진다 해도 비밀 합성에 의해 해독이 용이하지 않게되며 송 수신자간에 수신 문서의 위조나 송신 사실 부인시 본 논문의 디지털 서명 방식에 의해 이를 해결할 수 있을 것이다.

참 고 문 헌

1. Noriaki Minami외 2인 "畫像情報のセキュリティ確保に關する考察", 信學技報, vol. ISEC91-8, 1991.
2. Takeshi Komiyama외 1인 "A study on document / image scrambleing algorithm using space filling curve", SCIS92-17D, 1992.
3. 庶中외 1인, "ファクシミリ信號スクランフリンクの一方式", 信學技報 , vol.SAT89-26, 1989.
4. Masaki Kameya외 1인, "Coded scramble of digital images using convolution of enciphering and encoding", SCIS92-17B, 1992.
5. Masayuki Kanda외 3인, "A study on image scrambling method using DCT coding", SCIS93-13B, 1993.
6. 박일남 외, "JPEG에서의 암호화 방식에 대한 비익성 및 안전성 분석", 충남전문대학 산업기술 연구소 논문집, 제7호, 1995.
7. 김한상, "MH부호화를 사용하는 FAX 문서에 대한 계층적 디지털 서명법 연구", 경희대학교 석사 학위 논문, 1995.
8. 박일남외, "MH부호화를 사용하는 FAX 문서에 대한 다중화 서명법 연구", 신호처리 학회 발표 논문집. 1995.
9. 박일남외, "합성에 의한 FAX문서에의 디지틀 서명법 연구", 충남전문대학 논문집, 제13집, 1995.
10. 박일남외, "변화화소간의 차분치를 이용한 FAX 문서에서의 디지틀서명법", 한국통신학회 추계 종합 학술 발표회 논문집, 1995.
11. 박일남외, "문서화상에 대한 RDM 합성 알고리즘 및 디지틀 서명에의 응용", 한국통신 학회 논문집, 1996. 12.
12. 한국전자통신연구소, "현대암호학", 1991, 8
13. Selim G. Akl, "Digital Signatures: A Tutorial Survey", IEEE Computer, p15-24, Feb, 1983.

14. R. R. Jueneman, C. H. Meyer, and S. M. Matyas, "Message Authentication", IEEE Communications Magazine, vol. 23, no. 9, pp. 29-40, Sept. 1985.
15. Robert R. Jueneman, "Eletronic Document Authentication", IEEE Network Magazine, vol. 1, no. 2, pp. 17-23, April. 1987.
16. 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.
17. R. L. Rivest,A. Shamir and L. Adleman, "A method for optaining digital signature and public key cryptosystem", COMM.ACM, VOL21, pp 120-126, Feb. 1978 89-26, 1989.
18. ITU-T Recommendation T.4, 1993.
19. ITU-T Recommendation T.6, 1993.
20. R. Hunter and A. H. Robinson, "International digital facsimile coding standards", Proc. IEEE, 68, 7, pp. 854-867, 1980.

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 : 디지털 시스템, 영상처리, 암호학

李 大 寧(Dai Young Lee) 정회원
한국통신학회 논문지 제20권 3호 참조
현재 : 경희대학교 전자공학과 교수
한국통신학회 수석부회장