(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)
H04L 12/22 (2006.01)
H04L 9/08 (2006.01)

(45) 공고일자 2007년07월02일
(11) 등록번호 10-0734577
(24) 등록일자 2007년06월26일

(21) 출원번호 10-2005-0084052
(22) 출원일자 2005년09월09일
심사청구일자 2005년09월09일

(65) 공개번호 10-2006-0051144
(43) 공개일자 2006년05월19일

(30) 우선권주장 JP-P-2004-00264611 2004년09월10일 일본(JP)

(73) 특허권자
가부시키가이샤 히다치 고쿠사이 덴키
일본국 도쿄도 지요다구 소토 간다 4죠메 14반 1고

(72) 발명자
나카바야시 스미에
일본국 도쿄도 고다이라시 미유키쵸 32, 가부시키가이샤 히다치고쿠사이 덴키, 지적재산권 앤드 라이센싱부 내

야에가시 가즈히토
일본국 도쿄도 고다이라시 미유키쵸 32, 가부시키가이샤 히다치고쿠사이 덴키, 지적재산권 앤드 라이센싱부 내

구와바라 무네미츠
일본국 도쿄도 고다이라시 미유키쵸 32, 가부시키가이샤 히다치고쿠사이 덴키, 지적재산권 앤드 라이센싱부 내

우사미 히로타케
일본국 도쿄도 고다이라시 미유키쵸 32, 가부시키가이샤 히다치고쿠사이 덴키, 지적재산권 앤드 라이센싱부 내

(74) 대리인
특허법인화우

(56) 선행기술조사문헌
US 2004/0165724 A1

심사관 : 나용수

전체 청구항 수 : 총 15 항

(54) 암호화방법, 암호화장치, 데이터축적 전송장치 및 데이터 전송시스템

(57) 요약

본 발명은 암호화 대상이 되는 데이터를 송신장치에 의하여 암호화하고, 수신장치에 의하여 암호 복호화하는 데이터 전송 시스템으로, 암호화 대상이 되는 데이터를 효과적으로 암호화하는 것이다.

이를 위하여 본 발명에서는 입력 파라미터로부터 유니크하게 정해지는 난수열을 생성하는 난수 생성부에 의하여 생성된 난수열을 사용하여 암호화 대상이 되는 데이터의 암호화 및 복호화를 행하는 구성에 있어서, 송신장치는 암호화 대상이 되는 데이터의 메타데이터에 의거하여 입력 파라미터를 생성하여 암호화를 행하고, 수신장치는, 암호화 대상이 되는 데이터에 매립된 메타데이터에 의거하여 입력 파라미터를 생성하여 암호 복호화를 행한다.

대표도

도 1

특허청구의 범위

청구항 1.

초기 벡터와 암호키로 이루어지는 입력 파라미터로부터 유니크하게 정해지는 난수열을 생성하는 난수 생성수단에 의하여 생성된 난수열을 사용하여 암호화 대상이 되는 데이터의 암호화를 행하는 암호화방법에 있어서,

상기 암호화 대상이 되는 데이터의 메타데이터에 의거하여 상기 초기 벡터를 생성하는 방식으로 상기 입력 파라미터를 생성하는 것을 특징으로 하는 암호화방법.

청구항 2.

제 1항에 있어서,

상기 암호화 대상이 되는 데이터 또는 암호화된 상기 암호화 대상이 되는 데이터에 상기 메타데이터를 매립하고,

상기 암호화된 상기 암호화 대상이 되는 데이터를 복호하는 경우는, 상기 매립된 메타데이터에 의거하기 상기 입력 파라미터를 생성하는 것을 특징으로 하는 암호화방법.

청구항 3.

제 2항에 있어서,

상기 암호화 대상이 되는 데이터 중, 헤더나 상기 메타데이터 등을 제외하는 데이터 본체의 암호화를 행하는 것을 특징으로 하는 암호화방법.

청구항 4.

제 1항에 있어서,

상기 암호화 대상이 되는 데이터의 1 또는 복수단위마다 상기 입력 파라미터를 갱신함과 동시에 상기 난수 생성수단을 초기화하는 것을 특징으로 하는 암호화방법.

청구항 5.

제 2항에 있어서,

상기 암호화 대상이 되는 데이터의 1 또는 복수단위마다 상기 입력 파라미터를 갱신함과 동시에, 상기 난수 생성수단을 초기화하는 것을 특징으로 하는 암호화방법.

청구항 6.

제 3항에 있어서,

상기 암호화 대상이 되는 데이터의 1 또는 복수단위마다 상기 입력 파라미터를 갱신함과 동시에, 상기 난수 생성수단을 초기화하는 것을 특징으로 하는 암호화방법.

청구항 7.

제 4항에 있어서,

상기 암호키는, 미리 설정한 것으로부터 갱신하지 않는 것을 특징으로 하는 암호화방법.

청구항 8.

제 5항에 있어서,

상기 암호키는, 미리 설정한 것으로부터 갱신하지 않는 것을 특징으로 하는 암호화방법.

청구항 9.

제 6항에 있어서,

상기 암호키는 미리 설정한 것으로부터 갱신하지 않는 것을 특징으로 하는 암호화방법.

청구항 10.

제 3항 기재의 암호화방법에 의하여 암호화된 데이터의 검색방법에 있어서,

상기 매립된 메타데이터에 의거하여 상기 암호화된 데이터를 검색하는 것을 특징으로 하는 검색방법.

청구항 11.

암호화 대상이 되는 데이터를 송신장치에 의하여 암호화하고, 수신장치에 의하여 복호화하는 데이터 전송시스템에 있어서,

상기 송신장치는, 초기 벡터와 암호키로 이루어지는 입력 파라미터로부터 유니크하게 정해지는 난수열을 생성하는 난수생성수단과,

상기 암호화 대상이 되는 데이터의 메타데이터에 의거하여 상기 초기 벡터를 생성하는 방식으로 상기 입력 파라미터를 생성하는 입력 파라미터생성수단과,

상기 암호화 대상이 되는 데이터에 상기 메타데이터를 매립하는 메타데이터 매립수단과,

상기 난수 생성수단에 의하여 생성된 난수열을 사용하여 상기 암호화 대상이 되는 데이터중, 헤더나 상기 메타데이터등을 제외하는 데이터 본체를 암호화하는 암호화수단을 구비하고,

상기 수신장치는, 상기 난수 생성수단과,

상기 암호화된 상기 암호화 대상이 되는 데이터로부터 상기 메타데이터를 추출하는 메타데이터 추출수단과,

상기 메타데이터 추출수단에 의하여 추출된 메타데이터에 의거하여 상기 입력 마파미터 생성수단과,

상기 난수 생성수단에 의하여 생성된 난수열을 사용하여 상기 암호화된 상기 암호화 대상이 되는 데이터 중, 헤더나 상기 메타데이터 등을 제외하는 데이터 본체를 복호화하는 복호화수단을 구비한 것을 특징으로 하는 데이터 전송시스템.

청구항 12.

제 11항에 있어서,

상기 암호화 대상이 되는 데이터의 1 또는 복수단위마다 상기 입력 파라미터를 갱신함과 동시에, 상기 난수 생성수단을 초기화하는 것을 특징으로 하는 데이터 전송시스템.

청구항 13.

암호화 대상이 되는 데이터를 암호화하는 암호화장치에 있어서,

초기 벡터와 암호키로 이루어지는 입력 파라미터로부터 유니크하게 정해지는 난수열을 생성하는 난수 생성수단과,

상기 암호화 대상이 되는 데이터의 메타데이터에 의거하여 상기 초기 벡터를 생성하는 방식으로 상기 입력 파라미터를 생성하는 입력 파라미터 생성수단과,

상기 암호화 대상이 되는 데이터 또는 암호화된 상기 암호화 대상이 되는 데이터에 상기 메타데이터를 매립하는 메타데이터 매립수단과,

상기 난수 생성수단에 의하여 생성된 난수열을 사용하여 상기 암호화 대상이 되는 데이터 중, 헤더나 상기 메타데이터 등을 제외하는 데이터 본체를 암호화하는 암호화수단을 구비한 것을 특징으로 하는 암호화장치.

청구항 14.

제 13항에 있어서,

상기 암호화 대상이 되는 데이터의 1 또는 복수단위마다 상기 파라미터를 갱신함과 동시에, 상기 난수 생성수단을 초기화하는 것을 특징으로 하는 암호화장치.

청구항 15.

초기 벡터와 암호키로 이루어지는 입력 파라미터의 상기 초기 벡터를 암호화 대상이 되는 데이터의 메타데이터에 의거하여 생성하는 방식으로 입력 파라미터를 생성하고, 상기 입력 파라미터로부터 유니크하게 정해지는 난수열을 사용하여 상기 암호화 대상이 되는 데이터 중, 헤더나 상기 메타데이터 등을 제외하는 데이터 본체를 암호화한 암호화 데이터로서 상기 메타데이터가 매립되어 있는 상기 암호화 데이터를 기억하는 기억부를 가진 데이터축적 전송장치에 있어서,

클라이언트로부터의 원하는 조건을 가지는 상기 암호화 데이터의 검색요구에 따라 상기 메타데이터에 의거한 검색을 행하여, 상기 검색요구에 적합한 상기 암호화 데이터를 상기 클라이언트에게 송신하는 것을 특징으로 하는 데이터축적 전송장치.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 출원은, 2004년 9월 10일에 출원된 일본국 특허출원 제2004-264611호의 우선권을 주장하고, 그 내용을 참조함으로써 본 출원에 도입된다.

본 발명은, 암호화 대상이 되는 데이터를 암호화하는 암호화방법 및 데이터 전송시스템에 관한 것으로, 특히 암호화 대상이 되는 데이터를 효과적으로 암호화할 수 있는 암호화방법 및 데이터 전송시스템에 관한 것이다.

방범 등을 목적으로 하는 감시시스템에 있어서는, 예를 들면 인터넷(Internet) 등의 네트워크(network)를 사용한 시스템을 구축하는 것이, 비용 경쟁력(cost-competitiveness)이나 종래 시스템과의 차별화의 면에서 필수가 되고 있다. 한편, 인터넷 등, 오픈된 네트워크에 있어서는, 도청(eavesdropping/packet sniffering)이나 개찬(data tampering) 등이라는 위험성이 증대하고 있다.

여기서, 네트워크에서의 도청이나 개찬의 대책기술로서는 암호(criptography/ cryptography)나 메시지인증(message authentication)이 알려져 있다.

예를 들면, 인터넷에 관한 기술의 표준규격인 RFC(Request for Comments) 3711에는 RTP(Real-time Transport Protoco1) 패킷의 암호화 및 메시지인증기술이 소개되어 있다.

그러나, 예를 들면 감시 카메라가 촬상한 화상을 인터넷을 거쳐 서버에 축적하여, 필요에 따라 클라이언트에게 전송하고, 클라이언트에 있어서 모니터링 등을 행하는 시스템에 있어서 암호화기술을 적용하는 경우, 이하와 같은 과제가 있다.

제 1 과제는, 패킷 로스(packet loss)시의 암호동기(cryptographic synchronization)이다. 화상 등의 콘텐츠를 암호화하는 경우, 처리가 고속인 스트림암호(stream cipher)방식을 사용하는 경우가 많다.

예를 들면, 외부 동기식 암호의 스트림암호방식에서는, 송신측은 난수 생성기(random number generator)에 의하여 생성되는 키스트림과 평문(plaintext)의 배타적논리합으로부터 암호문을 생성하여, 네트워크를 거쳐 수신측으로 암호문을 전송한다. 한편, 수신측은 난수 생성기에 의하여 생성되는 키스트림과 수신한 암호문과의 배타적 논리합(exclusive or)으로부터 암호문을 평문으로 되돌린다.

따라서, 패킷 로스에 의하여 암호문의 데이터가 일부 결핍되면, 송신측과 수신측의 난수 생성기의 동기가 벗어나게 되어, 수신측에서는 이후 전혀 암호문을 복호할 수 없게 된다는 문제가 있었다. 이것에 대한 대책으로서는, 패킷단위로 난수 생성기를 초기화하는 방법이 일반적으로 행하여지고 있다.

여기서, 암호키와 초기 벡터를 입력하여 난수 생성기에 의해 키스트림을 생성하고, 상기 키스트림을 사용하여 암호화를 행하는 암호화방식에 있어서는, 생성되는 키스트림은 암호키와 초기 벡터의 조합에 의하여 유니크하게 결정된다.

이와 같은 암호화방식의 경우, 패킷단위로 난수 생성기를 초기화하여도 암호키 또는 초기 벡터를 변경하지 않으면, 이전 패킷에 적용한 키스트림과 동일한 키스트림이 생성되기 때문에 암호의 안전성이 저하된다.

종래기술인 RFC 3711에서는, RTP 패킷 헤더의 시퀀스번호로부터 초기 벡터를 도출하여, 패킷마다 초기 벡터를 갱신함으로써 동일 키스트림의 재사용을 회피하고 있다. 또 RTP의 시퀀스번호는 16 비트이기 때문에, 32 비트 롤오버 카운터를 설치하여, 2의 48승개의 패킷까지는 다른 초기 벡터를 도출하고, 2의 48승개의 패킷을 송신하기 전에 암호키를 갱신하는 것이 권장되고 있다.

제 2 과제는 시스템의 키 관리에 관한 것이다. 암호화를 행하는 시스템에 있어서는 예를 들면 화상부호화장치와, 화상축적 전송장치와, 화상 복호화장치와의 사이에서의 암호키의 설정이나 암호키의 갱신에 따르는 암호키의 배송 등의 키 관리가 복잡해진다는 문제나, 사용자의 키 관리의 부하가 커진다는 문제가 있었다.

발명이 이루고자 하는 기술적 과제

본 발명은, 이와 같은 종래의 사정을 감안하여 이루어진 것으로, 암호화 대상이 되는 데이터를 효과적으로 암호화할 수 있는 암호화방법 및 데이터 전송시스템을 제공하는 것을 목적으로 한다.

발명의 구성

상기 목적을 달성하기 위하여 본 발명에 관한 암호화방법은, 입력 파라미터로부터 유니크하게 정해지는 난수열을 생성하는 난수 생성부에 의하여 생성된 난수열을 사용하여 암호화 대상이 되는 데이터의 암호화를 행하는 암호화방법으로서, 상기 암호화 대상이 되는 데이터의 메타데이터에 의거하여 생성하는 것을 제공한다.

여기서, 데이터로서는 여러가지의 데이터가 사용되어도 좋다. 또 메타데이터로서는, 여러가지 데이터가 사용되어도 좋다.

또 본 발명에 관한 암호화방법에 있어서 상기 암호화 대상이 되는 데이터에 상기 메타데이터를 매립하고, 상기 암호화된 상기 암호화 대상이 되는 데이터를 복호하는 경우는, 상기 매립된 메타데이터에 의거하여 상기 입력 파라미터를 생성하는 것을 제공한다.

또, 본 발명에 관한 암호화방법은, 상기 암호화 대상이 되는 데이터중, 예를 들면, 헤더나 상기 메타데이터 등을 제외한 부분의 데이터의 암호화를 행한다.

또, 본 발명에 관한 암호화방법에 있어서, 상기 암호화 대상이 되는 데이터의 1 또는 복수단위마다 상기 입력 파라미터를 갱신함과 동시에, 상기 난수 생성부를 초기화한다.

또, 본 발명에 관한 암호화방법에 있어서, 상기 입력 파라미터는, 초기 벡터와 암호키로 이루어지고, 상기 초기 벡터는, 상기 메타데이터에 의거하여 생성된다. 상기 암호키는, 미리 설정한 것으로부터 갱신하지 않아도 된다.

또, 본 발명에 관한 암호화방법에 의하여 암호화된 데이터의 검색방법으로서, 상기 매립된 메타데이터에 의거하여 상기 암호화된 데이터를 검색한다.

또, 상기 목적을 달성하기 위하여 본 발명에 관한 데이터 전송시스템은, 암호화 대상이 되는 데이터를 송신장치에 의하여 암호화하고, 수신장치에 의하여 복호화하는 데이터 전송시스템으로서,

상기 송신장치는, 입력 파라미터로부터 유니크하게 정해지는 난수열을 생성하는 난수 생성부와, 상기 암호화 대상이 되는 데이터의 메타데이터에 의거하여 상기 입력 파라미터를 생성하는 입력 파라미터생성부와, 상기 암호화 대상이 되는 데이터 또는 암호화된 상기 암호화 대상이 되는 데이터에 상기 메타데이터를 매립하는 메타데이터 매립부와, 상기 난수 생성부에 의하여 생성되는 난수열을 사용하여 상기 암호화 대상이 되는 데이터중, 헤더나 상기 메타데이터 등을 제외하는 데이터 본체를 암호화하는 암호화부를 구비하고,

상기 수신장치는, 상기 난수 생성부와, 상기 암호화된 상기 암호화 대상이 되는 데이터로부터 상기 메타데이터를 추출하는 메타데이터 추출부와, 상기 메타데이터추출부에 의하여 추출된 메타데이터에 의거하여 상기 입력 파라미터를 생성하는 입력 파라미터 생성부와, 상기 난수 생성부에 의하여 생성된 난수열을 사용하여 상기 암호화된 상기 암호화 대상이 되는 데이터중, 헤더나 상기 메타데이터 등을 제외하는 데이터 본체를 복호화하는 암호 복호화부를 구비하도록 구성된다.

또, 본 발명에 관한 데이터 전송시스템에 있어서, 상기 암호화 대상이 되는 데이터의 1 또는 복수단위마다 상기 입력 파라미터를 갱신함과 동시에, 상기 난수 생성부를 초기화한다.

이하, 본 발명의 실시형태에 대하여 도면을 참조하면서 설명한다. 본 발명의다른 목적, 특징 및 이점은 첨부도면에 관한 이하의 본 발명의 실시예의 기재로부터 분명해질 것이다.

도 1에는 본 발명의 일 실시예에 관한 화상 전송시스템의 구성예를 나타내고 있다.

도 1에 나타내는 화상 전송시스템은, 카메라(101)와, 화상부호화장치(102)와, 화상축적 전송장치(104)와, 화상 복호화장치(105)와, 모니터(106)로 구성된다. 화상부호화장치(102), 화상축적 전송장치(104), 화상 복호화장치(105)의 사이는, 예를 들면 인터넷 등의 네트워크(103)에 의해 접속된다.

여기서, 카메라(101)는 예를 들면 NTSC 방식의 TV 카메라이고, 소정의 장소를 촬상하여 영상신호를 입력화상으로서 화상부호화장치(102)에 출력한다. 화상부호화장치(102)는, 접속된 카메라(101)로부터의 입력화상을, 예를 들면 MPEG (Motion Picture Experts Group)방식이나 JPEG(Joint Photographic Experts Group)방식 등에 의하여 압축 부호화하고, 다시 부호화된 화상 데이터(이하, 부호화 화상 데이터라 한다.)를 암호화하고, 암호화된 부호화 화상 데이터를 네트워크(103)에 출력한다.

화상축적 전송장치(104)는, 네트워크(103)로부터 수신한 암호화된 부호화 화상 데이터를 장치내의 디스크장치(데이터를 축적하기 위한 랜덤 엑세스 가능한 기록 장치)에 축적하고, 또한 예를 들면 클라이언트[화상 복호화장치(105)]로부터의 요구 에 의거하여 암호화된 부호화 화상 데이터의 네트워크(103)에 대한 전송을 행한다.

화상 복호화장치(105)는, 네트워크(103)로부터 암호화된 부호화 화상 데이터를 수신하면, 암호의 복호화(decrypt) 및 화상의 복호화(decode)를 행하여, 복호한 (decrypted and decoded) 화상 데이터를 화상 복호화장치(105)에 접속된 모니터(106)에 출력한다. 모니터(106)에서는 암호의 복호 및 화상의 복호된 화상이 표시 또는 재생(reproduce)된다.

여기서, 상기한 화상 전송시스템에 있어서는, 간단화를 위하여 카메라(101)나 화상부호화장치(102)나 화상축적 전송장치(104)나 화상 복호화장치(105)는 각각 1대씩 설치하는 것으로 가정하나, 이들의 대수는 임의로 선택할 수 있다.

또, 상기한 화상 전송시스템에 있어서는, 화상 복호화장치(105)는 화상축적 전송장치(104)로부터 암호화된 화상 데이터를 수신하는 구성을 나타내었으나, 다른 구성예로서는 화상 복호화장치(105)는, 화상부호화장치(102)로부터 직접 암호화된 화상 데이터를 수신하는 구성을 사용하여도 좋다.

또, 카메라(101)와 화상부호화장치(102)의 기능이 일체화된 장치나, 화상부호화장치(102)와 화상축적 전송장치(104)의 기능이 일체화된 장치 등을 사용하여도 좋고, 화상 전송시스템은 이상의 실시예에 한정되는 것이 아니다.

도 2에는 본 발명의 일 실시예에 관한 화상부호화장치의 구성예를 나타내고 있다.

도 2에 나타내는 화상부호화장치(102)는 카메라 인터페이스부(21), 화상부호화부(22), 메타데이터생성부(23), 암호화부(24), 네트워크 인터페이스부(25)로 구성된다.

카메라 인터페이스부(21)는, 카메라(101)로부터의 입력화상을 도입하여 입력화상을 화상부호화부(22)에 출력한다.

화상부호화부(22)는 입력화상을 압축 부호화하여, 부호화 화상 데이터를 암호화부(24)에 출력한다.

메타데이터생성부(23)는 부호화 화상 데이터의 생성원인 카메라(101)의 ID 번호나, 부호화 화상 데이터의 타임스탬프정보나, 부호화 화상 데이터의 화상 프레임번호 등, 상기 화상 데이터에 관한 부속정보(이하, 메타데이터라 한다.)를 생성하여, 암호화부(24)에 출력한다.

여기서 메타데이터생성부(23)는 1개 또는 복수의 데이터를 기초로 메타데이터를 작성한다. 예를 들면 카메라 인터페이스부(21)로부터의 정보에 의거하여 카메라(101)의 ID 번호를 생성하고, 화상부호화부(22)에 의해 부호화 화상 데이터가 생성되는 시각에 의거하여 타임스탬프를 생성하고, 화상부호화부(22)가 구비하는 프레임번호를 카운트하기 위한 카운터의 정보에 의거하여 화상 프레임번호를 생성하는 등, 메타데이터의 생성방법에 대해서는 여러가지 방법을 사용하는 것이 가능하다.

또, 메타데이터로서는 상기한 것 이외에도 예를 들면, 카메라(101)의 촬영영역에 설치되는 적외선센서, 초음파센서, 연기센서, 가스누출센서 등의 촬영영역의 이상을 검출하기 위하여 설치된 센서로부터 얻어진 알람정보 등에 의거하여 생성된 데이터가 사용되어도 좋다.

암호화부(24)는, 화상부호화부(22)로부터 입력된 부호화 화상 데이터에 대응하는 메타데이터를 메타데이터생성부(23)로부터 판독하고, 상기 메타데이터에 의거하여 암호화처리에 사용하는 키스트림을 생성하고(상세한 것은 뒤에서 설명한다), 생성한 키스트림을 사용하여 화상부호화부(22)로부터 입력된 부호화 화상 데이터의 암호화를 행하고, 암호화된 부호화 화상 데이터와, 대응하는 메타데이터를 네트워크 인터페이스부(25)에 출력한다.

네트워크 인터페이스부(25)는 암호화부(24)로부터 입력된 암호화된 부호화 화상 데이터와, 대응하는 메타데이터를 네트워크(103)에 출력한다.

다음에, 도 3a 내지 도 6을 참조하여, 본 발명의 특징적인 부분인 암호화부(24)에 의하여 행하여지는 암호화처리의 예를 설명한다.

도 3a, 도 3b는, 본 발명의 종래기술을 나타내는 도면이다.

도 3c는 본 발명에 관한 암호화처리의 일 실시예를 나타내는 도면이다. 도 3d는 본 발명에 관한 암호 복호화처리의 일 실시예를 나타내는 도면이다.

화상 데이터나 음성 데이터 등의 콘텐츠의 암호화에 사용하는 암호 알고리즘에는 DES(Data Encryption Standard)나, AES(Advanced Encryption Standard) 등이 알려져 있다. 본 실시예의 암호화부(24)에서는 전자정부 권장 암호 리스트(the e-Government Recommended Ciphers List)에 게재되어 있는 MUGI를 적용한 경우에 대하여 설명한다.

본 실시예에서는 도 3c에 나타내는 바와 같이, 난수 생성기는 128 비트의 암호키(K)(비밀키)와, 128 비트의 초기 벡터(I)(공개 파라미터)를 입력단자로서 가진다. 난수 생성기는 암호키(K)와, 초기 벡터(I)가 입력될 때마다 내부상태를 초기화하여 상태천이(state transition)를 반복하면서, 난수열(키스트림)을 생성한다. 그리고 난수 생성기로부터 출력되는 키스트림과 평문을 비트마다 배타적 논리합을 취함으로써 암호문을 작성하는 암호화처리가 행하여진다.

본 실시예의 암호화처리는, 뒤에서 설명하는 바와 같이 하나의 데이터 프레임 내의 특정한 데이터영역을 암호화할 수 있다. 즉, 본 실시예의 암호화처리는 하나의 데이터 프레임내에 암호화 데이터(암호문)와 비암호화 데이터(평문)의 양쪽이 존재하는 구성을 실현할 수 있다.

상기와 같은 데이터 프레임의 구성을 실현하기 위하여 도 3c에 나타내는 바와 같은 구성이 사용되어도 좋다.

또, 도 3c에는 도시되어 있지 않으나, 암호화되는 데이터영역과 암호화되지 않은 데이터영역을 특정하는 암호 판단부를 사용하여도 좋다. 암호 판단부에 의하여 암호화가 필요하다고 판단된 데이터영역은, 비트마다 키스트림과 배타적 논리합이 취해져 암호화된다. 상기 이외의 데이터영역은, 배타적 논리합이 취해지지 않기 때문에 암호화되지 않는다.

이것에 의하여 뒤에서 설명하는 도 5b 등에 나타내는 바와 같은 암호화된 영역을 포함하는 데이터 프레임의 구성이 실현된다.

다음에 암호가 포함되어 있는 데이터 프레임을 복호(decrypt)하기 위하여 도 3d에 나타내는 바와 같은 구성이 사용되어도 좋다.

상기와 마찬가지로 도 3d에는 도시되어 있지 않으나, 데이터 프레임이 암호화되어 있는지의 여부를 특정하는 복호 판단부를 사용하여도 좋다. 복호 판단부는 암호화되어 있는 데이터영역을 특정하고, 특정된 데이터영역은 비트마다 키스트림과 배타적 논리합이 취해져 복호된다. 암호화되어 있지 않은 데이터영역은, 배타적 논리합이 취해지지 않는다.

이것에 의하여 모든 평문의(복호된) 데이터 프레임의 구성이 실현된다.

또한 소정의 데이터영역을 암호화/복호화할 수 있는 구성이면 상기 실시예 이외의 구성이어도 좋다.

여기서, 암호화부(24)는 먼저 암호화하는 부호화 화상 데이터에 대응하는 메타데이터를 메타데이터생성부(23)로부터 판독하고, 메타데이터에 의거하여 상기한 초기 벡터(I)를 생성한다.

예를 들면 도 4(a)에 나타내는 바와 같이, 어느 부호화 화상 데이터의 메타데이터로서도 카메라번호 「02」, 촬영일「04. 06. 14」, 촬영시간「12 : 30 : 30」, 화상 프레임번호「03」라는 정보가 포함되어 있던 경우, 도 4(b)에 나타내는 바와 같이, 메타데이터의 카메라번호 필드로부터 16 비트(예를 들면, 카메라번호「02」의「0」과 「2」를 각각 8 비트으로 나타낸다. 촬영일, 촬영시간, 화상 프레임번호에 대해서도 마찬가지.), 촬영일을 나타내는 필드로부터 48 비트, 촬영시간을 나타내는 필드로부터 48 비트, 화상 프레임번호를 나타내는 필드로부터 16 비트를 인출함으로써 메타데이터생성부(23)는 128 비트의 초기 벡터(I)를 생성한다.

그리고, 암호화부(24)는 예를 들면 미리 설정되어 있는 암호키(K)와, 상기한 초기 벡터(I)로부터 키스트림을 생성한다. 여기서 생성되는 키스트림은 암호키(K)와 초기 벡터(I)의 조합에 의하여 유니크하게 정해지는 것이기 때문에, 초기 벡터(I)를 생성할 때에 사용하는 메타데이터가 유니크한 것이면 생성되는 키스트림도 유니크한 것이 되어, 암호의 보안상의 위험을 회피할 수 있다.

또한, 도 4에 나타낸 예에서는 메타데이터로서 카메라번호, 촬영일, 촬영시간, 화상 프레임번호라는 정보를 사용하고, 또 그 정보를 카메라번호, 촬영일, 촬영시간, 화상 프레임번호라는 순서로 나열함으로써 초기 벡터(I)를 생성하는 경우에 대하여 나타내었으나, 메타데이터에 의거하는 초기 벡터의 생성방법으로서는 이것에 한정되지 않고, 여러가지 방법이 사용되어도 좋다. 즉, 하나의 메타데이터에 대하여 초기 벡터(I)가 유니크함과 함께 유니크한 키스트림이 생성되면, 메타데이터생성부(23)가 메타데이터를 어떻게 사용하여 초기 벡터(I)를 생성하는지는 자유이다.

또한 메타데이터에 의거하는 초기 벡터의 생성방법에 대해서는 예를 들면 미리 송신측[예를 들면, 화상부호화장치(102)의 암호화부(24)], 수신측[예를 들면 뒤에서 설명하는 화상 복호화장치(105)의 암호 복호화부(64)]의 양쪽에 사전에 정하여 둔 것을 설정하여 두면 좋다.

다음에 암호화부(24)는 화상부호화부(22)로부터 입력된 부호화 화상 데이터와, 상기한 바와 같이 생성되는 키스트림과의 배타적 논리합으로부터 암호화된 부호화 화상 데이터를 생성한다. 여기서 화상부호화부(22)의 압축 부호화방식으로서는 MPEG나 JPEG 등, 많은 종류의 방식이 적용 가능하다. 메타데이터를 매립하는 것이 가능한 데이터 프레임구성을 가진 방식이면 본 발명이 적용 가능하다.

여기서는 도 5를 참조하여 MPEG-4의 경우를 예로 설명한다. MPEG-4에 있어서는, 일반적으로 VO를 구성하는 각 화상을 VOP(Video Object Plane)라 부르고, VOP의 그룹을 GOV(Group Of V0P)로서 처리한다.

도 5a에는 MPEG-4의 스트림구성의 개략을 모식적으로 나타내고 있다.

MPEG-4의 스트림구성의 실제에 대해서는, ISO/IEC 14496-2에 규정되어 있는 바와 같으나, 개략을 모식적으로 나타내면, 도 5a에 나타내는 바와 같이 MPEG-4의 부호화 화상 데이터는, video object start code부터 시작되는 VO(Video Object) 헤더정보영역, video object layer start code부터 시작되는 VOL(Video 0bject Layer) 헤더정보영역, group vop start codes부터 시작되는 GOV(Group of V0P) 헤더정보영역, 어플리케이션에 맞추어 사용자가 사용 가능한 영역으로 user data start code부터 시작되는 사용자 데이터영역, vop start code(여기서는, VOP 코드라 부른다)부터 시작되는 VOP로 구성되다.

또한 VOP는 VOP 코드나, 그 VOP 전체를 복호(decode)하기 위하여 필요하게 되는 정보(VOP 헤더)나, 프레임에 상당하는 화상 본체의 부호화정보인 MB(Macro Block)부호화정보 등으로 구성되고, 도 5a에 나타내는 바와 같이 사용자 데이터영역의 뒤에는 복수의 VOP가 계속되는 구성으로 되어 있다.

도 5b에는 MPEG-4의 부호화 화상 데이터중, 본 발명의 일 실시예에 관한 암호화처리에 있어서 암호화를 행하는 위치를 나타내고 있다. 도 5b에 나타내는 바와 같이, 암호화부(24)는 MPEG-4의 부호화 화상 데이터중, MB 부호화 정보에 대해서만 암호화를 행한다.

도 5c에는 MPEG-4의 부호화 화상 데이터중, 본 발명의 일 실시예에 관한 암호화처리에 있어서 사용한 메타데이터를 매립하는 위치를 나타내고 있다.

암호화부(24)는, 각 GOV에 대하여 상기 GOV에 대응한 메타데이터에 의거하여 초기 벡터(I)를 생성하여, MB 부호화 정보의 암호화를 행함과 동시에, 도 5c에 나타내는 바와 같이, MPEG-4의 스트림의 상기 GOV의 사용자 데이터영역에 초기 벡터(I)의 생성에 사용한 메타데이터를 매립한 후, 암호화된 부호화 화상 데이터를 네트워크 인터페이스부(25)에 출력한다.

도 6에는 본 발명의 일 실시예에 관한 MPEG-4의 부호화 화상 데이터를 암호화할 때의 처리의 순서의 일례를 나타내고 있다.

먼저, 암호화부(24)는 새로운 GOV를 검출하였으면, 상기 GOV에 대응하는 메타데이터를 메타데이터생성부(23)로부터 판독하고, 판독한 메타데이터를 상기 GOV의 사용자 데이터영역에 매립한다(단계 S601).

다음에 암호화부(24)는, 메타데이터생성부(23)로부터 판독한 메타데이터에 의거하여 초기 벡터(I-1)[1번째 초기 벡터(I)]를 생성한다(단계 S602).

또한 초기 벡터의 생성방법은 상기한 바와 같으나, MPEG-4의 부호화 화상 데이터의 경우, 메타데이터중, 프레임번호나 타임스탬프에 대해서는 예를 들면 상기 GOV의 선두의 VOP에 대응하는 것(상기 GOV를 구성하는 VOP 중에서 가장 최신의 프레임번호나 가장 오래된 타임스탬프)을 사용한다.

다음에, 암호화부(24)는 난수 생성기의 초기화를 행하여(단계 S603), 초기 벡터(I-1)와, 미리 설정하여 둔 암호키(K)로부터 키스트림을 생성한다(단계 S604). 그리고 생성한 키스트림과 MPEG-4 부호화 화상 데이터의 MB 부호화 정보와의 배타적 논리합에 의하여 암호화를 행한다(단계 S605). 이후, 암호화부(24)는 다음 GOV를 검출할 때까지(예를 들면, 다음 video object start code를 검출할 때까지), 생성한 키스트림으로 MB 부호화 정보에 대한 암호화를 반복하여 행한다(단계 S606에서 NO).

여기서, 예를 들면 V0P 코드 등을 검출한 경우에는, 다음의 MB 부호화 정보의 위치까지 암호화를 스킵함으로써, MB 부호화 정보에 대해서만 암호화를 행할 수 있다.

한편, 다음의 GOV를 검출한 경우에는(단계 S606에서 YES), 암호화부(24)는, 상기와 마찬가지로 상기 GOV에 대응하는 메타데이터를 메타데이터생성부(23)로부터 판독하고, 판독한 메타데이터에 의거하여 초기 벡터(I-2)를 생성하고, 초기 벡터(I-2)를 사용하여 생성한 새로운 키스트림을 사용하여, 이후 상기 GOV의 MB 부호화 정보에 대하여 암호화를 행한다(단계 S601～S605).

이하, 다시 다음의 GOV를 검출한 경우에는, 암호화부(24)는 초기 벡터(I-n)(n = 3, 4, 5 …)를 생성하고, 상기와 동일한 암호화처리를 행한다.

이와 같이, 도 6에 나타낸 처리순서에 의하면, 초기 벡터(I)는 GOV 마다 갱신되고, 난수 생성기의 초기화도 GOV마다, 즉, 화상의 복수 프레임마다 행하여진다.

또한 도 6에 나타낸 처리순서에 의하면, 단계 S605에 있어서의 암호화를 행하기 전에 단계 S601에 있어서 부호화 화상 데이터에 메타데이터를 매립하고 있으나, 메타데이터를 매립하는 타이밍으로서는 상기한 타이밍에 한정되지 않고, 예를 들면 암호화를 행한 후에 메타데이터를 매립하는 등, 여러가지 타이밍이 사용되어도 좋다.

다음에, 화상축적 전송장치(104)에 대하여 설명한다. 화상축적 전송장치(104)는 예를 들면 도 5c에 나타내는 포맷에 의하여 암호화된 부호화 화상 데이터(암호화 데이터)를 축적하여, 클라이언트의 요구 등에 의하여 필요에 따라 네트워크(103)를 거쳐 암호화 데이터의 전송을 행한다.

또한 상기한 바와 같이 예를 들면 MPEG-4의 부호화 화상 데이터의 경우, 암호화는 MB 부호화 정보에 대해서만 행하여지고, VO 헤더정보영역, VOL 헤더정보영역, GOV 헤더정보영역, VOP 코드, VOP 헤더 등, 화상의 검색이나 전송 등에 필요한 정보는 암호화되어 있지 않기 때문에, 화상축적 전송장치(104)에서는 암호화 데이터를 비암호화 데이터와 동등하게 처리할 수 있다.

이 때문에, 예를 들면 어느 카메라(101)의 화상 데이터에 대해서는 암호화를 행하고, 다른 카메라(101)의 화상 데이터에 대하여 암호화를 행하지 않는다 라는 바와 같이 동일 시스템내에서 비암호 카메라와 암호 카메라의 공존이 가능해진다.

또 상기한 바와 같이 본 실시예에서는 메타데이터가 매립되는 사용자 데이터영역에 대해서도 암호화는 행하여지지 않기 때문에, 비암호화 데이터에 대해서도 마찬가지로 사용자 데이터영역에 메타데이터를 매립하는 구성을 사용하면, 메타데이터에 대해서도 화상의 검색 등, 암호화 데이터와 비암호화 데이터의 양쪽에서 공통으로 이용 가능하게 된다.

이것에 의하여 예를 들면, 클라이언트(복합화장치나 데이터단말 등)는, 암호화 데이터와 비암호화 데이터를 한번에 검색할 수 있다. 검색된 암호화 데이터는, 필요에 따라 복호화장치를 사용하여 복호하면 좋다. 환언하면, 복호화하는 키를 가지고 있지 않은 장치(또는 사용자)는, 암호화 데이터를 검색할 수는 있어도, 복호화된 데이터를 볼 수 없다.

또한 이상에서는 MB 부호화 정보만을 암호화하는 구성예를 나타내었으나, V0P 헤더 등이어도 화상의 검색이나 전송 등에 필요한 정보 이외에 대해서는 적절하게 암호화하도록 하여도 좋다.

다음에 화상 복호화장치(105)에 대하여 설명한다. 도 7에는 본 발명의 일 실시예에 관한 화상 복호화장치의 구성예를 나타내고 있다.

도 7에 나타내는 화상 복호화장치(105)는, 네트워크 인터페이스부(71), 암호 복호화부(72), 화상 복호화부(73), 모니터 인터페이스부(74)로 구성된다.

네트워크 인터페이스부(71)는 네트워크(103)로부터 암호화된 부호화 화상 데이터를 수신하고, 수신한 암호화된 부호화 화상 데이터를 암호 복호부(72)에 출력한다.

암호 복호부(72)는, 암호화된 부호화 화상 데이터의 암호의 복호화를 행하여, 부호화 화상 데이터를 화상 복호화부(73)에 출력한다.

화상 복호화부(73)는, 부호화 화상 데이터의 복호화를 행하여, 복호된 화상 데이터를 모니터 인터페이스부(74)에 출력한다.

모니터 인터페이스부(74)는, 복호된 화상 데이터를 모니터(106)에 출력한다. 화상 복호화장치(105)가 이상과 같이 동작함으로써, 암호화된 부호화 화상 데이터가 복호되어, 모니터(106)에 암호의 복호 및 화상의 복호된 화상이 표시 또는 재생된다.

여기서, MPEG-4의 부호화 화상 데이터의 경우를 예로, 암호 복호화부(72)의 동작의 일례를 나타낸다.

암호 복호화부(72)는, 네트워크 인터페이스부(71)로부터 도 5c에 나타내는 포맷에 의하여 암호화된 부호화 화상 데이터를 수취하면, 암호의 복호화처리를 행한다. 즉, 암호 복호화부(72)는 암호화된 부호화 화상 데이터의 GOV를 검출하면, 사용자 데이터영역중에 매립된 메타데이터를 추출한다.

그리고, 암호 복호화부(72)는 상기한 화상 부호화장치(27)의 암호화부(24)의 처리와 마찬가지로 추출한 메타데이터에 의거하여 초기 벡터(I)를 생성하여, 난수 생성기의 초기화를 행한 후, 도 3d에 나타내는 바와 같이, 초기 벡터(I)와, 미리 설정하고 있는 암호키(K)로부터 키스트림을 생성한다.

그리고 상기한 암호화처리와는 반대로, 생성한 키스트림과 암호화된 MB 부호화정보와의 배타적 논리합에 의하여 MB 부호화 정보의 암호의 복호화를 행한다.

이후, 암호 복호화부(72)는 다음 GOV를 검출할 때까지, 생성한 키스트림으로 암호화된 MB 부호화정보의 암호의 복호화를 행한다. 다음 GOV를 검출한 경우에는 암호 복호화부(72)는 새롭게 상기 GOV의 사용자 데이터영역 중의 메타데이터를 추출하여, 상기와 마찬가지로 메타데이터로부터 초기 벡터를 생성하고, 키스트림을 생성하여 이후의 암호화된 MB 부호화정보에 대한 복호화처리를 행한다.

또한 본 실시예에 관한 화상 전송시스템에서는 암호키(K)를 화상 부호화장치(102)와 화상 복호화장치(105) 사이에서 공유하여 둘 필요가 있다. 이 경우, 예를 들면 시스템 출하시에 미리 암호키(K)를 설정하여 두는 방법이나, 시스템의 운용시에 시스템관리자가 암호키(K)를 설정하는 방법 등, 암호키(K)는 종래 주지의 방법에 의하여 공유하는 것이 가능하다.

또 암호키(K)의 갱신에 대해서는 예를 들면 상기한 바와 같이 초기 벡터가 128 비트이면, 통상 제품수명중에 동일한 키스트림이 생성되는 일은 없고, 최초로 설정한 암호키(K)를 변경할 필요는 특별히 생기지 않으나, 필요에 따라 시스템관리자 등이 새로운 암호키(K)를 설정하게 하여도 좋다.

또, 복수의 화상 부호화장치(102), 복수의 화상 복호화장치(105)로 구성되는 시스템에 있어서도 동일 키스트림의 생성을 피하도록 유니크한 초기 벡터를 생성하 게 하면 암호의 보안은 취약화되지 않기 때문에 하나의 암호키(K)를 시스템내에서 공유하여도 지장이 없다.

이상과 같이 본 실시예에 관한 화상 전송시스템에서는 화상 부호화장치(102)는, 카메라(101)로부터의 입력화상을 부호화하는 수단과, 상기 부호화한 화상 데이터에 대응하는 메타데이터를 생성하는 수단과, 부호화한 화상 데이터를 암호화하는 수단을 가지고, 부호화한 화상 데이터를 암호화하는 수단은, 암호화 대상인 부호화한 화상 데이터에 대응하는 메타데이터에 의거하여 초기 벡터를 생성하고, 암호키와 초기 벡터로부터 키스트림을 생성하여, 그 키스트림에 의하여 부호화한 화상 데이터의 암호화를 행한다.

또, 부호화한 화상 데이터를 암호화하는 수단은, 키스트림의 생성에 사용하는 초기 벡터의 갱신 및 난수 생성기의 초기화를 화상단위(예를 들면, 화상의 복수 프레임 등)로 행한다.

따라서 본 실시예에 관한 화상 전송시스템에서는 화상단위(예를 들면, 1 VOP 단위)로 난수 생성기를 초기화함으로써 전송로상에서 패킷 로스가 발생하여도 화상단위로 암호 동기의 복귀가 가능해진다.

또, 예를 들면 메타데이터 중의 카메라번호, 촬영일시, 화상 프레임번호를 초기 벡터에 포함시킴으로써 시스템내에서 유니크한 키스트림을 생성하는 것이 가능해져, 암호키의 갱신을 행하지 않더라도 키스트림의 재사용을 회피할 수 있다.

따라서 키스트림의 재사용에 의한 암호의 보안의 취약화를 회피할 수 있다. 또 일반적으로 패킷의 데이터길이(data length)보다도 화상단위의 데이터길이의 쪽이 길기 때문에 종래예와 비교하여 초기 벡터의 갱신빈도가 내려가 초기 벡터의 갱신에 따르는 암호화나 복호화의 오버헤드(overhead)를 작게 할 수 있다.

또, 본 실시예에 관한 화상 전송시스템에서는 화상단위로 갱신되는 초기 벡터에 의하여 시스템내에서 유니크한 키스트림을 생성할 수 있기 때문에, 시스템내에서 하나의 암호키를 공유하는 것이 허용되어, 갱신이 불필요한 하나의 암호키로 시스템을 구축하는 것이 가능하게 되어, 시스템의 개발비용의 저감을 기대할 수 있다.

또, 시스템에 있어서 암호키의 설정이나 암호키의 갱신에 따르는 키 배송 등의 키 관리가 간략화되어, 사용자에 대해서는 키 관리의 부하가 경감되기 때문에, 사용하기 쉬운 시스템을 제공할 수 있다.

또, 본 실시예에 관한 암호화방법은, MPEG압축, JPEG압축, 음성압축 등의 복수종류의 코덱(codec)에 대응한 멀티 인코더(multi-encoder)에도 적용하는 것이 가능하다. 이 경우에 있어서도 메타데이터에 의거하여 각 코덱의 초기 벡터를 유니크한 값이라 하면, 암호키는 동일한 것을 공용하여도 코덱마다 유니크한 키스트림을 생성하는 것이 가능하다.

또, 본 실시예에 관한 화상 전송시스템의 화상축적 전송장치(104)에서는 화상부호화장치(102)로부터 출력되는 암호화 화상 데이터와 메타데이터를 축적하고, 암호화 화상 데이터의 검색에 있어서는 메타데이터 중의 정보 등을 검색 키로 함으로써 암호화된 상태에서의 암호화 화상 데이터의 검색, 암호화 화상 데이터의 전송을 행할 수 있다.

또, 화상축적 전송장치(104)에서는 암호화 데이터는 비암호화 데이터와 동등하게 처리할 수 있기 때문에, 동일 시스템내에서 비암호 카메라와 암호 카메라의 공존이 가능하다.

또, 본 실시예에 관한 화상 전송시스템에서는 초기 벡터는 스트림 데이터로부터 도출할 수 있기 때문에, 암호화에 의한 초기 벡터용 부가 비트가 불필요하게 되고, 시스템의 대역의 유효 이용이 가능하다.

또, 암호화는 어플리케이션층에서 행하기 때문에, 암호화에 따르는 하위레이어(lower layer)의 변경은 불필요하고, 패킷의 헤더압축을 적용하는 것도 가능하다.

또, 기존의 시스템에 영향을 주지 않기 때문에, 시스템 도입을 용이하게 행할 수 있는 효과가 있다.

또, 본 실시예에 관한 화상 전송시스템의 화상 복호화장치(105)에서는, 수신한 암호화된 부호화 화상 데이터 중에 매립된 메타데이터를 사용하여 키스트림을 생성하고 있기 때문에, 전송도중에서 메타데이터가 개찬된 경우, 암호의 복호화가 정확하게 행하여지지 않는다. 즉, 재생화상에 이상이 없으면, 메타데이터는 신뢰할 수 있게 되어, 개찬을 한눈에 확인할 수 있는 효과가 있다.

또한 본 실시예에서는 MPEG-4의 부호화 화상 데이터에 대하여 각 GOV의 MB 부호화 정보의 암호화를 행할 때, 상기 GOV의 메타데이터에 의거하여 초기 벡터를 생성하는 구성을 나타내었으나, 다른 구성예로서, 상기 GOV 이전의 GOV, 또는 이후의 GOV의 메타데이터에 의거하여 초기 벡터를 생성하는 구성으로 하여도 좋다.

단, 각 GOV 자체의 메타데이터에 의거하여 초기 벡터를 생성하는 구성의 경우, 즉 화상 프레임단위로 독립으로 암호화처리를 행하는 구성의 경우이면, 전송로에서 패킷 로스가 발생한 경우에 있어서도, 수신측에서 암호의 복호화를 행할 때의 패킷 로스의 영향을 최소한으로 억제할 수 있는 효과가 있다.

여기서, 본 실시예에서는 MPEG-4의 부호화 화상 데이터의 암호화를 행하는 경우에는, GOV 마다 초기 벡터를 갱신하여 암호화를 행하는 구성을 나타내었으나, 다른 구성예로서, VOP 마다 초기 벡터를 갱신하여 암호화를 행하는 구성이 사용되어도 좋다. 다음에 이것에 대하여 도 8 내지 도 10을 참조하여 설명한다.

도 8에는 본 발명의 일 실시예에 관한 MPEG-4의 부호화 화상 데이터를 VOP 마다 초기 벡터를 갱신하여 암호화할 때의 처리의 순서의 일례를 나타내고 있다.

즉, 암호화부(24)는 먼저 새로운 GOV를 검출하였으면, 상기 GOV에 대응하는 메타데이터를 메타데이터생성부(23)로부터 판독하고, 판독한 메타데이터를 상기 GOV의 사용자 데이터영역에 매립한다(단계 S701).

다음에 암호화부(24)는, 도 9에 나타내는 바와 같이 카메라번호나 촬영일이라는 메타데이터(도 9a)와 각 VOP에 대응하여 붙여지는 VOP번호(도 9b)로부터 도 9c에 나타내는 바와 같이 초기 벡터(I)를 생성한다(단계 S702).

또한 VOP 번호는, 메타데이터의 일종으로 메타데이터생성부(23)에 있어서 생성하게 하여도 좋고, 암호화부(24)에 있어서 VOP의 수를 카운트함으로써 생성하게 하여도 좋다.

다음에 암호화부(24)는, 난수 생성기의 초기화를 행하여(단계 S703), 초기 벡터(I)와 미리 설정하고 있는 암호키(K)로부터 키스트림을 생성한다(단계 S704).

그리고 생성한 키스트림과, 상기 VOP 번호에 대응하는 VOP의 MB 부호화 정보와의 배타적 논리합에 의하여 암호화를 행한다(단계 S705). 또 도 10에 나타내는 바와 같이 VOP 헤더의 바로 뒤에 부가 비트(오버헤드 비트)로서 상기 VOP 번호를 매립한다(단계 S706).

또한 VOP 번호를 매립하는 위치는, VOP 헤더의 바로 뒤에 한정되는 것이 아니다. 예를 들면, VOP 헤더 뒤의 1 바이트분의 영역 등, VOP 번호를 매립하는 위치는, 미리 송신측과 수신측의 양쪽에 사전에 정하여 둔 것을 설정하여 두면 좋다.

또, 뒤에서 설명하는 바와 같이 VOP 번호는 수신측에 있어서 각 VOP의 암호의 복호화를 행할 때에 사용할 필요가 있기 때문에, 스트림에 매립하는 VOP 번호에 대하여 암호화는 행하여지지 않는다.

이후, 다음 GOV를 검출하지 않는 경우에는(단계 S707에서 NO), 암호화부(24)는 VOP에 대응지어진 VOP 번호(예를 들면, 이전의 VOP의 VOP 번호로부터 1 증가한 번호)와 상기 메타데이터로부터 VOP 마다 초기 벡터(I)를 생성하고, 난수 생성기를 초기화하여 초기 벡터(I)와 미리 설정하고 있는 암호키(K)로부터 키스트림을 생성하고, 생성한 키스트림으로 VOP 번호에 대응하는 VOP의 MB 부호화 정보에 대한 암호화처리 및 VOP 번호의 매립을 반복하여 행한다(단계 S702~706).

한편, 다음의 GOV를 검출한 경우에는(단계 S707에서 YES), 상기와 마찬가지로 상기 GOV에 대응하는 메타데이터를 메타데이터생성부(23)로부터 판독하고, VOP에 대응지어진 VOP 번호와 메타데이터로부터 VOP 마다 초기 벡터(I)를 갱신하면서, 마찬가지로 암호화처리를 행한다.

또한 본 실시예에서는 VOP 마다 유니크한 초기 벡터(I)를 생성하여 이전의 VOP의 암호화에 사용한 키스트림의 재사용을 회피하기 위하여, 초기 벡터(I)의 생성에 VOP 번호를 사용하는 구성을 나타내었으나, VOP 번호 이외의 정보가 사용되어도 좋고, 또 초기 벡터(I)를 생성할 때의 메타데이터의 나열순서를 바꾸는 등, 다른 여러가지 방법에 의하여 VOP 마다 유니크한 초기 벡터(I)를 생성하는 구성으로 하여도 좋다.

또, 상기한 바와 같이 VOP 번호를 부가 비트로서 MPEG-4의 스트림에 매립하는 구성 이외에, 예를 들면 VOP에 포함되는 각 VOP의 고유정보에 의거하여 VOP 마다 유니크한 초기 벡터(I)를 생성하는 구성을 사용하여도 좋다.

다음에 상기한 바와 같이 VOP 단위로 초기 벡터를 갱신하여 암호화를 행한 MPEG-4의 부호화 화상 데이터를 수신한 화상 복호화장치(105)에 있어서의 동작의 일례에 대하여 설명한다.

화상 복호화장치(105)의 암호 복호화부(72)에서는 네트워크 인터페이스부(71)로부터 도 10에 나타내는 포맷에 의하여 암호화된 부호화 화상 데이터를 수취하면, 암호의 복호화처리를 행한다. 즉, 암호 복호화부(72)는 암호화된 부호화 화상 데이터의 GOV를 검출하면, 사용자 데이터영역 중에 매립된 메타데이터를 추출한다.

또, VOP 코드를 검출하면 암호 복호화부(72)는 부가 비트로서 VOP 헤더의 바로 뒤에 매립되어 있는 VOP 번호를 추출한다.

그리고 상기한 암호화부(24)의 처리와 마찬가지로 추출한 메타데이터와 VOP 번호에 의거하여 초기 벡터(I-1)를 생성하고, 난수 생성기의 초기화를 행한 후, 초기 벡터(I-1)와, 미리 설정하여 둔 암호키(K)로부터 키스트림을 생성한다.

그리고, 상기한 암호화처리와는 반대로, 생성한 키스트림과 암호화된 MB 부호화 정보와의 배타적 논리합에 의하여 MB 부호화 정보의 암호를 복호한다.

이후, 다음의 VOP 코드를 검출하면 암호 복호화부(72)는 부가 비트로서 VOP 헤더의 바로 뒤에 매립되어 있는 VOP 번호의 추출을 행하고, 메타데이터와 VOP 번호에 의거하여 초기 벡터(I-2)를 생성한다.

그리고 난수 생성기의 초기화를 행한 후, 초기 벡터(I-2)와 미리 설정하고 있는 암호화 키(K)로부터 키스트림을 생성하고, 생성한 키스트림으로 암호화된 MB 부호화정보의 암호의 복호화를 행한다.

또, 다음의 GOV를 검출한 경우에는 새롭게 상기 GOV의 사용자 데이터영역 중의 메타데이터를 추출하여, 상기와 마찬가지로 VOP 번호를 사용하여 VOP 마다 초기 벡터(I)를 갱신하면서 암호의 복호화를 행한다.

이와 같이, 도 8에 나타낸 처리순서에 의하면, 난수 생성기의 초기화는 VOP마다, 즉 화상의 1 프레임마다 행하여진다. 이에 의하여 네트워크(103)상에서 패킷 로스가 발생하여 송신측과 수신측의 난수 생성기의 동기가 벗어난 경우에 있어서도 다음의 VOP의 복호화로부터는 난수 생성기의 동기를 취할 수 있어, 화상 프레임단위로 암호동기의 복귀가 가능해진다.

또, 이 경우에 있어서 VOP 마다 초기 벡터(I)를 유니크한 값으로 갱신하고 있기 때문에, 항상 유니크한 키스트림을 사용할 수 있어, 동일한 키스트림의 재사용을 회피하는 것이 가능하다.

또한 다른 구성예로서 난수 생성기의 초기화는 VOP 단위로 행하고, 초기 벡터(I)의 갱신은 GOV 단위로 행하는 구성을 사용하여도 좋으나, 그 경우 초기 벡터(I)의 갱신없이 난수 생성기의 초기화를 행하기 때문에 동일한 키스트림이 생성되게 되어 암호의 보안이 저하되는 것은 물론이다.

또, 본 예에서는 VOP 번호를 부가 비트로서 스트림에 삽입하기 때문에 그것 만큼 데이터전송 효율은 저하된다. 그러나 수신측에서는 스트림에 매립된 VOP 번호를 추출하여 암호의 복호화에 사용할 수 있기 때문에, 네트워크(103)상에서 패킷 로스가 발생한 경우에 있어서도, 송신측과 수신측에 있어서, VOP 번호의 동기가 벗어날염려가 없어, 암호의 복호화가 항상 정확하게 행하여지는 것이 가능하다.

다음에 JPEG의 부호화 화상 데이터의 암호화를 행하는 구성의 일례에 대하여 도 11a 내지 도 11c를 참조하여 설명한다.

도 11a에 나타내는 바와 같이 JPEG의 부호화 화상 데이터는, SOI(Start Of Image), EOI(End Of Image) 등의 단독마커(marker)와, APP0(Application type 0), SOF0(Start 0f Frame type 0), SOS(Start 0f Scan) 등의 마커와 부가정보로 이루어지는 마커 세그먼트와, 화상 본체인 부호화 세그먼트로 구성된다.

여기서 암호화부(24)는 도 11b에 나타내는 바와 같이 JPEG의 부호화 화상 데이터중, 부호화 세그먼트에 대해서만 암호화를 행한다. 즉, SOI를 검출하였으면 암호화부(24)는 상기 화상 프레임에 대응하는 메타데이터를 메타데이터생성부(23)로부터 판독하고, 메타데이터에 의거하여 초기 벡터(I)를 생성하여 난수 생성기를 초기화한 후, 초기 벡터(I)와 미리 설정하고 있는 암호키(K)로부터 키스트림의 생성을 한다.

그리고 암호화부(24)는 생성한 키스트림과 상기 부호화 세그먼트와의 배타적 논리합에 의하여 암호화를 행한다. 다음의 SOI를 검출한 경우, 암호화부(24)는 마찬가지로 대응하는 메타데이터를 메타데이터생성부(23)로부터 판독하고, 메타데이터에 의거하여 초기 벡터(I)를 생성하여 새로운 키스트림으로 부호화 세그먼트의 암호화를 행한다.

또한 암호화부(24)는 어느 화상 프레임의 SOI와 다음의 화상 프레임의 SOI의 사이에서 다른 마커 등을 검출한 경우에는, 다음의 부호화 세그먼트의 위치까지 암호화를 스킵함으로써, 부호화 세그먼트에 대해서만 암호화를 행할 수 있다.

그리고, 암호화부(24)는 도 11c에 나타내는 바와 같이, JPEG 화상의 APP0 마커 세그먼트에 암호화에 사용한 메타데이터를 매립하여 네트워크 인터페이스부(25)에 출력한다.

한편, 화상 복호화장치(105)는, 도 11c에 나타내는 포맷에 의하여 암호화된 부호화 화상 데이터를 수취하면, APP0 마커 세그먼트에 매립된 메타데이터를 추출하고, 메타데이터에 의거하여 초기 벡터(I)를 생성한다.

그리고 화상 복호화장치(105)는 초기 벡터(I)와 미리 설정하고 있는 암호키(K)로부터 키스트림을 생성하고, 상기한 암호화처리와는 반대로 키스트림과 암호화된 부호화 세그먼트와의 배타적 논리합에 의하여 암호의 복호화를 행한다.

또한 상기한 구성에서는 JPEG 화상의 1 프레임마다 초기 벡터(I)의 갱신과, 난수 생성기의 초기화를 행하는 것을 상정하고 있으나, JPEG의 부호화 화상 데이터의 암호화시에도 예를 들면 5 프레임마다 등, 복수 프레임마다 초기 벡터(I)의 갱신이나 난수 생성기의 초기화를 행하게 하여도 좋다.

이 경우, 상기한 구성에서는 예를 들면 5 프레임 중의 선두의 프레임에 대응하는 메타데이터에 의거하여 초기 벡터(I)를 생성하여도 좋고, 예를 들면 5 프레임분의 메타데이터를 조합시켜 초기 벡터(I)를 생성하여도 좋다.

여기서, 본 실시예에서는 MPEG-4형식이나 JPEG형식의 부호화 화상 데이터의 암호화를 행하는 구성을 나타내었으나, 다른 구성예로서 상기와 동일한 구성이나 동작을 다른 부호화형식의 화상 데이터의 암호화에 대하여 적용하는 것이 가능하다.

또, 상기와 동일한 구성이나 동작을 화상 데이터 이외의 음성 데이터 등의 스트림 데이터의 암호화에 대하여 적용하는 것도 가능하다.

또한 본 예의 화상 부호화장치(102)에서는 암호화부(24)의 기능에 의해 난수 생성부가 구성되어 있고, 메타데이터생성부(23)나 암호화부(24)의 기능에 의하여 입력 파라미터생성부가 구성되어 있으며, 암호화부(24)의 기능에 의하여 메타데이터 매립부가 구성되어 있고, 암호화부(24)의 기능에 의하여 암호화부가 구성되어 있다.

또 본 예의 화상 복호화장치(105)에서는 암호 복호화부(72)의 기능에 의하여 난수 생성도가 구성되어 있고, 암호 복호화부(72)의 기능에 의하여 메타데이터 추출부가 구성되어 있으며, 암호 복호화부(72)의 기능에 의하여 입력 파라미터생성부가 구성되어 있고, 암호 복호화부(72)의 기능에 의하여 복호화부가 구성되어 있다.

여기서 본 발명에 관한 화상 전송시스템이나 화상 부호화장치나 화상 복호화장치 등의 구성으로서는 반드시 이상에 나타낸 것에 한정하지 않고 여러가지 구성이 사용되어도 좋다.

또, 본 발명은 예를 들면 본 발명에 관한 처리를 실행하는 방법 또는 방식이나, 이와 같은 방법이나 방식을 실현하기 위한 프로그램이나 상기 프로그램을 기록하는 기록매체 등으로서 제공하는 것도 가능하고, 또 여러가지 장치나 시스템으로서 제공하는 것도 가능하다.

또, 본 발명의 적용분야로서는 반드시 이상에 나타낸 것에 한정되지 않고, 본 발명은 여러가지 분야에 적용하는 것이 가능한 것이다. 응용예로서 감시목적 이외에도 예를 들면 유치원의 운동회나, 야구 등의 스포츠를 시청하는 목적 등의 시스템으로서 실현하는 것도 가능하다.

또, 본 발명에 관한 화상 전송시스템이나 화상 부호화장치나 화상 복호화장치등에 있어서 행하여지는 각종 처리로서는 예를 들면 프로세서나 메모리 등을 구비한 하드웨어자원에 있어서 프로세서가 ROM(Read Only Memory)에 저장된 제어프로그램을 실행함으로써 제어되는 구성이 사용되어도 좋고, 또 예를 들면 상기 처리를 실행하기 위한 각 기능부가 독립된 하드웨어회로로서 구성되어도 좋다.

또, 본 발명은 상기한 제어프로그램을 저장한 플로피디스크나 CD-ROM 등의 컴퓨터에 의하여 판독 가능한 기록매체나 상기 프로그램(자체)으로서 파악할 수도 있으며, 상기 제어프로그램을 상기 기록매체로부터 컴퓨터에 입력하여 프로세서에 실행시킴으로써, 본 발명에 관한 처리를 수행시킬 수 있다. 상기 기재는 실시예에 대하여 이루어졌으나, 본 발명은 이것에 한정되지 않고, 본 발명의 정신과 첨부하는 클레임의 범위내에서 여러가지의 변경 및 수정을 할 수 있는 것은 당업자에게는 분명하다.

발명의 효과

이상 설명한 바와 같이, 본 발명에 관한 암호화방법 및 데이터 전송시스템에 의하면, 입력 파라미터로부터 유니크하게 정해지는 난수열을 생성하는 난수 생성부에 의하여 생성된 난수열을 사용하여 암호화 대상이 되는 데이터의 암호화를 행할 때에, 암호화 대상이 되는 데이터의 메타데이터에 의거하여 입력 파라미터를 생성하게 하였기 때문에, 암호화 대상이 되는 데이터를 효과적으로 암호화할 수 있다.

도면의 간단한 설명

도 1은 본 발명의 일 실시예에 관한 화상전송시스템의 구성예를 나타내는 도,

도 2는 본 발명의 일 실시예에 관한 화상부호화장치의 구성예를 나타내는 도,

도 3a는 암호화처리의 종래기술을 나타내는 도,

도 3b는 암호 복호화처리의 종래기술을 나타내는 도,

도 3c는 본 발명의 일 실시예에 관한 암호화처리의 구성예를 나타내는 도,

도 3d는 본 발명의 일 실시예에 관한 암호 복호화처리의 구성예를 나타내는 도,

도 4는 본 발명의 일 실시예에 관한 초기 벡터의 생성방법의 일례를 설명하기 위한 도,

도 5a는 본 발명의 일 실시예에 관한 부호화 화상 데이터의 구성예에 있어서, 화상부호화부의 출력 포맷의 일례를 나타내는 도,

도 5b는 본 발명의 일 실시예에 관한 부호화 화상 데이터의 구성예에 있어서, 암호화를 행하는 위치의 일례를 나타내는 도,

도 5c는 본 발명의 일 실시예에 관한 부호화 화상 데이터의 구성예에 있어서, 메타데이터를 매립하는 위치의 일례를 나타내는 도,

도 6은 본 발명의 일 실시예에 관한 부호화 화상 데이터의 암호화처리의 순서의 일례를 설명하기 위한 도,

도 7은 본 발명의 일 실시예에 관한 화상복호화장치의 구성예를 나타내는 도,

도 8은 본 발명의 일 실시예에 관한 부호화 화상 데이터의 암호화처리의 순서의 일례를 설명하기 위한 도,

도 9는 본 발명의 일 실시예에 관한 초기 벡터의 생성방법의 일례를 설명하기 위한 도,

도 10은 본 발명의 일 실시예에 관한 부호화 화상 데이터의 구성예를 나타내는 도,

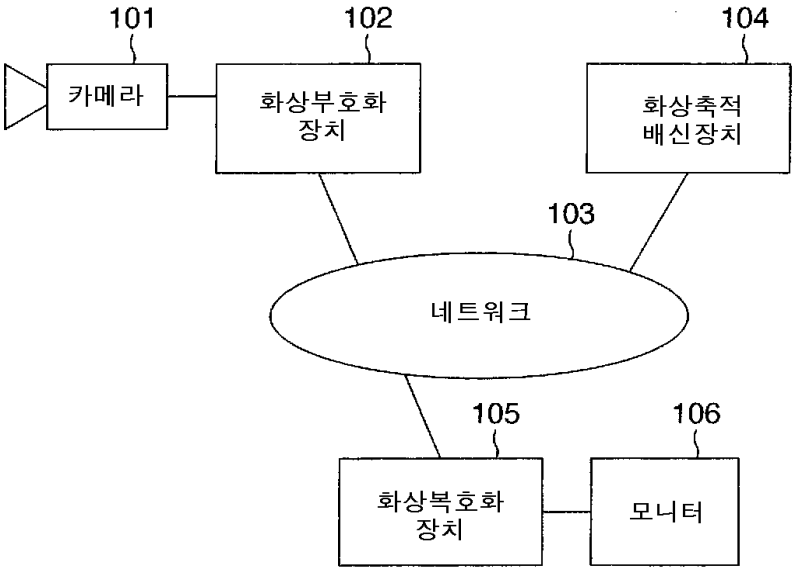
도 11a는 본 발명의 일 실시예에 관한 부호화 화상 데이터의 구성예에 있어서, 화상부호화부의 출력 포맷의 일례를 나타내는 도,

도 11b는 본 발명의 일 실시예에 관한 부호화 화상 데이터의 구성예에 있어서, 암호화를 행하는 위치의 일례를 나타내는 도,

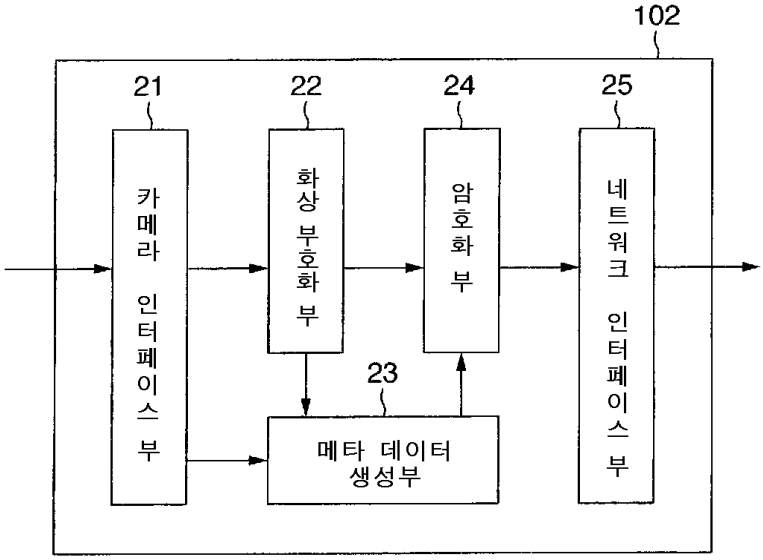
도 11c는 본 발명의 일 실시예에 관한 부호화 화상 데이터의 구성예에 있어서, 메타데이터를 매립하는 위치의 일례를 나타내는 도면이다.

도면

도면1

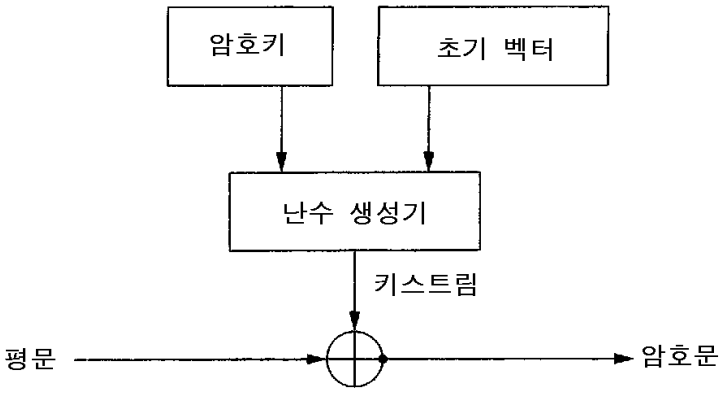


도면2



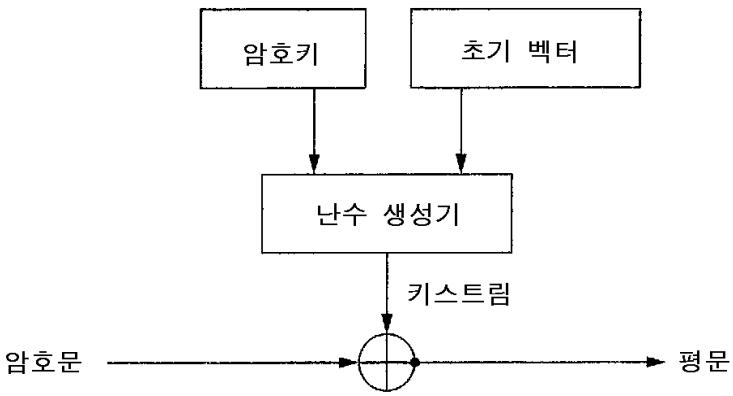
도면3a

종래 기술

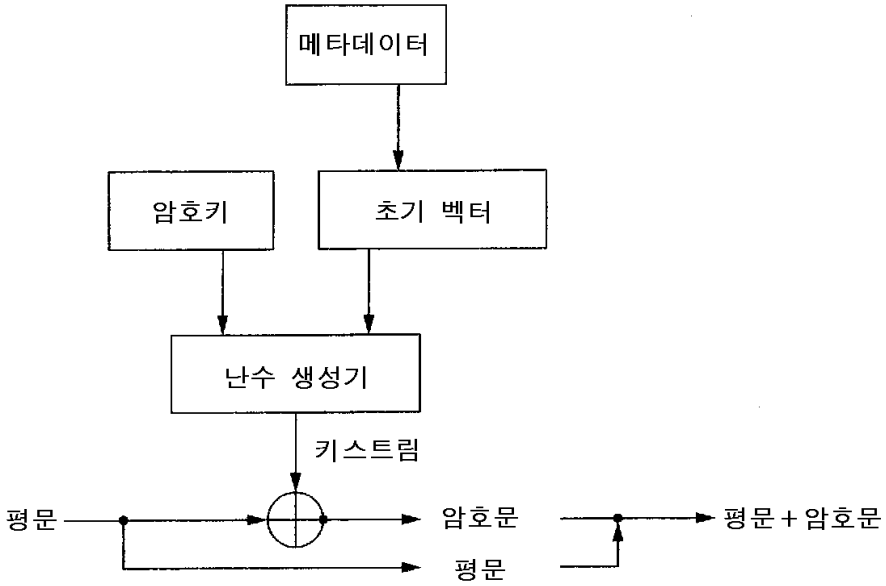


도면3b

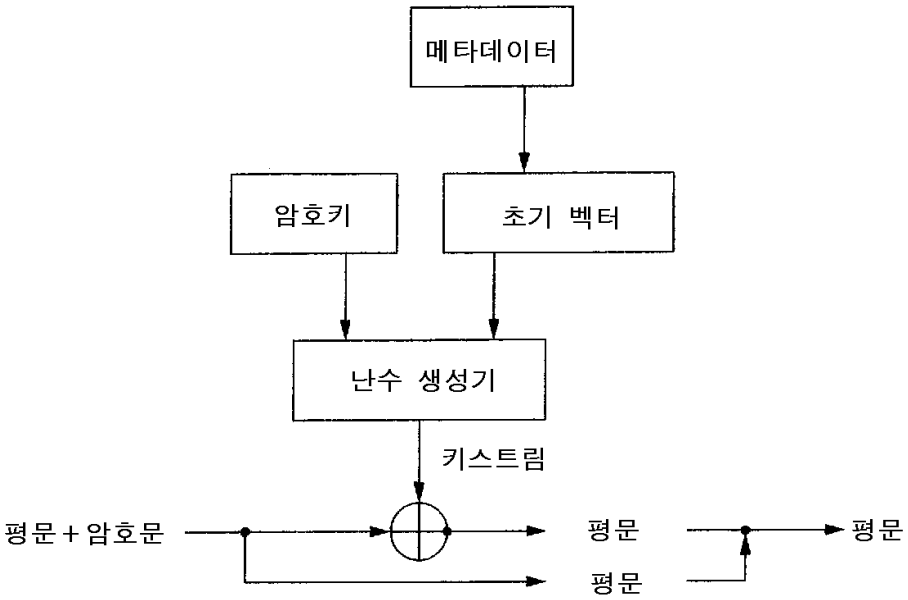
종래 기술



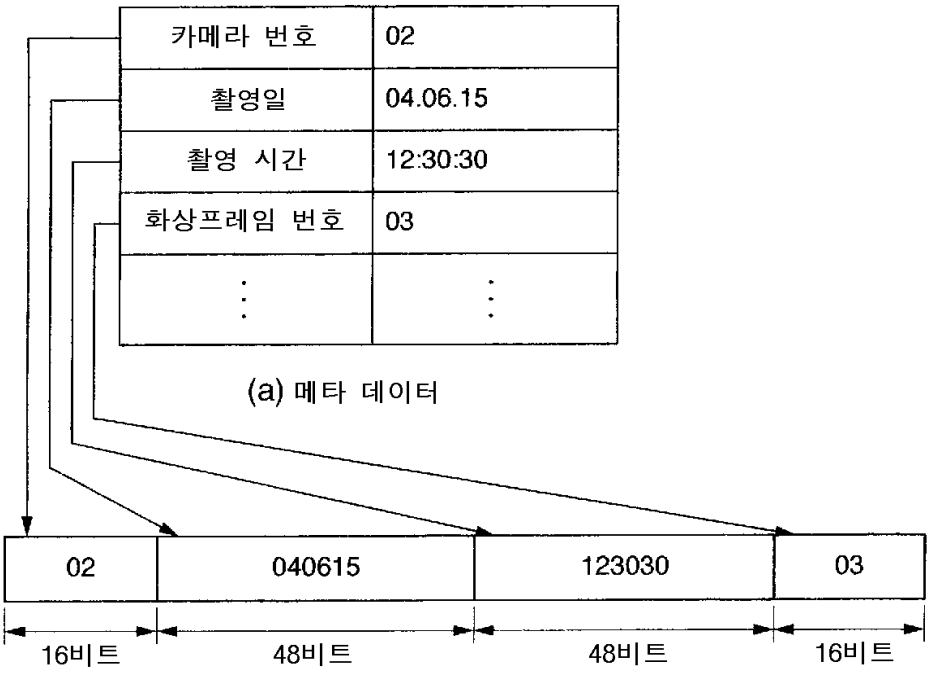
도면3c


메타데이터
암호키
초기 벡터
난수 생성기
키스트림
평문
암호문
평문
평문+암호문

도면3d

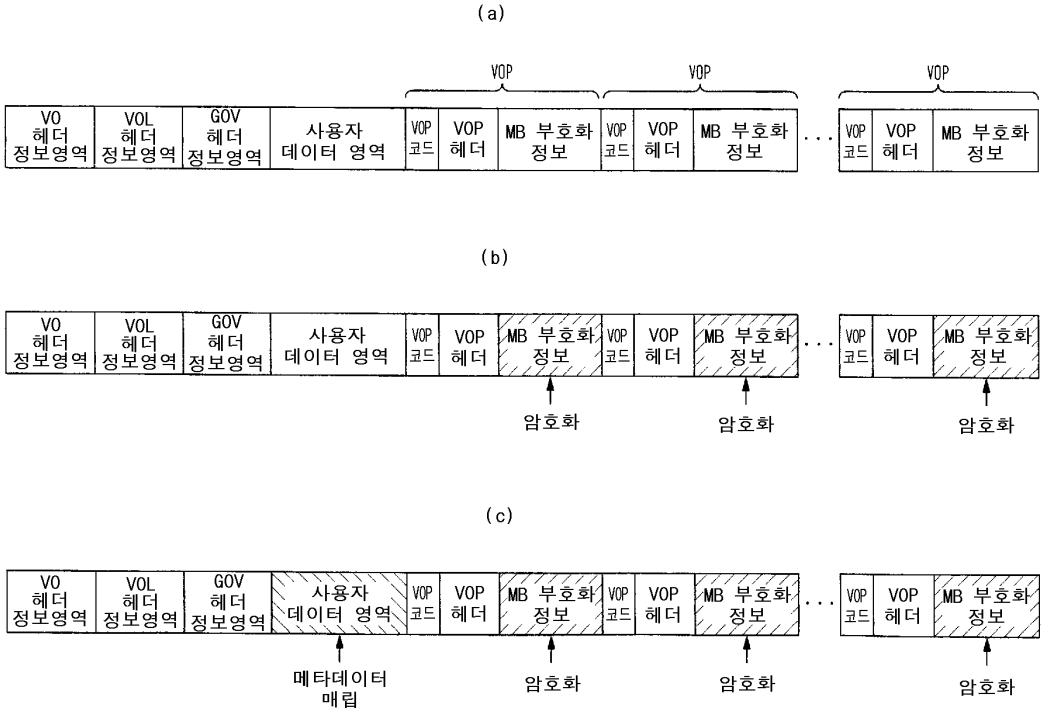

메타데이터
암호키
초기 벡터
난수 생성기
키스트림
평문+암호문
평문
평문
평문

도면4

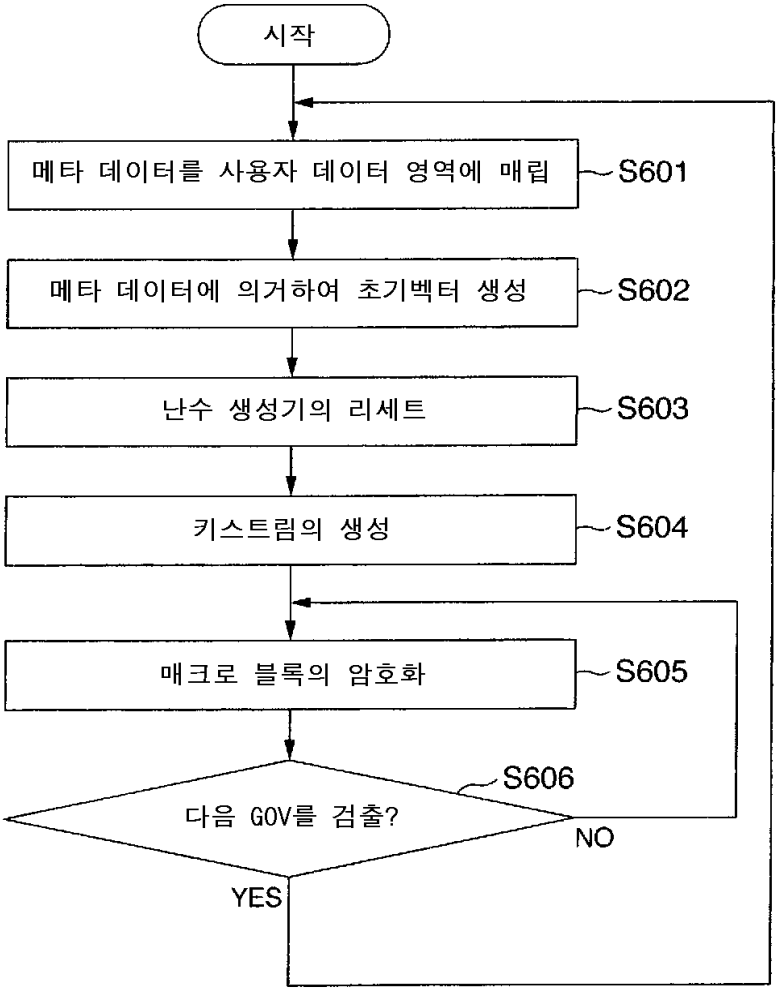


(b) 초기 벡터(128비트)

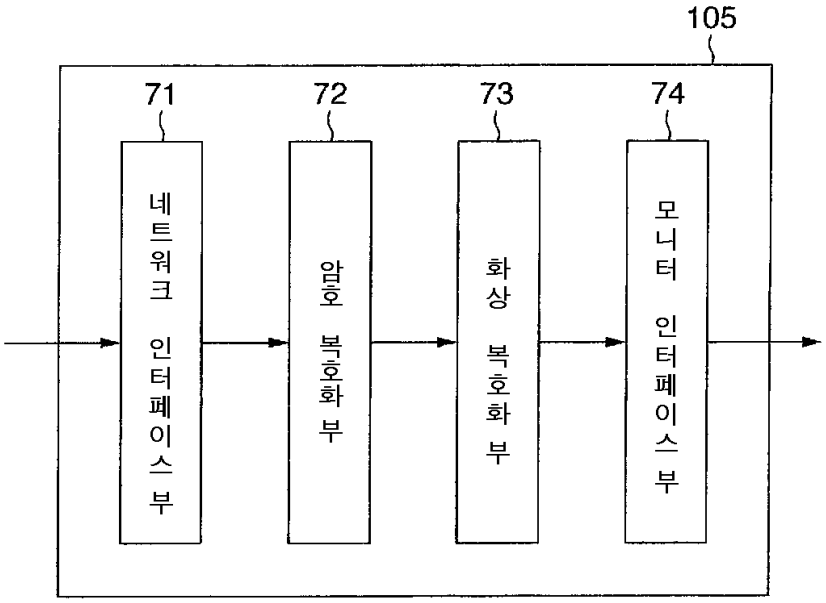
도면5



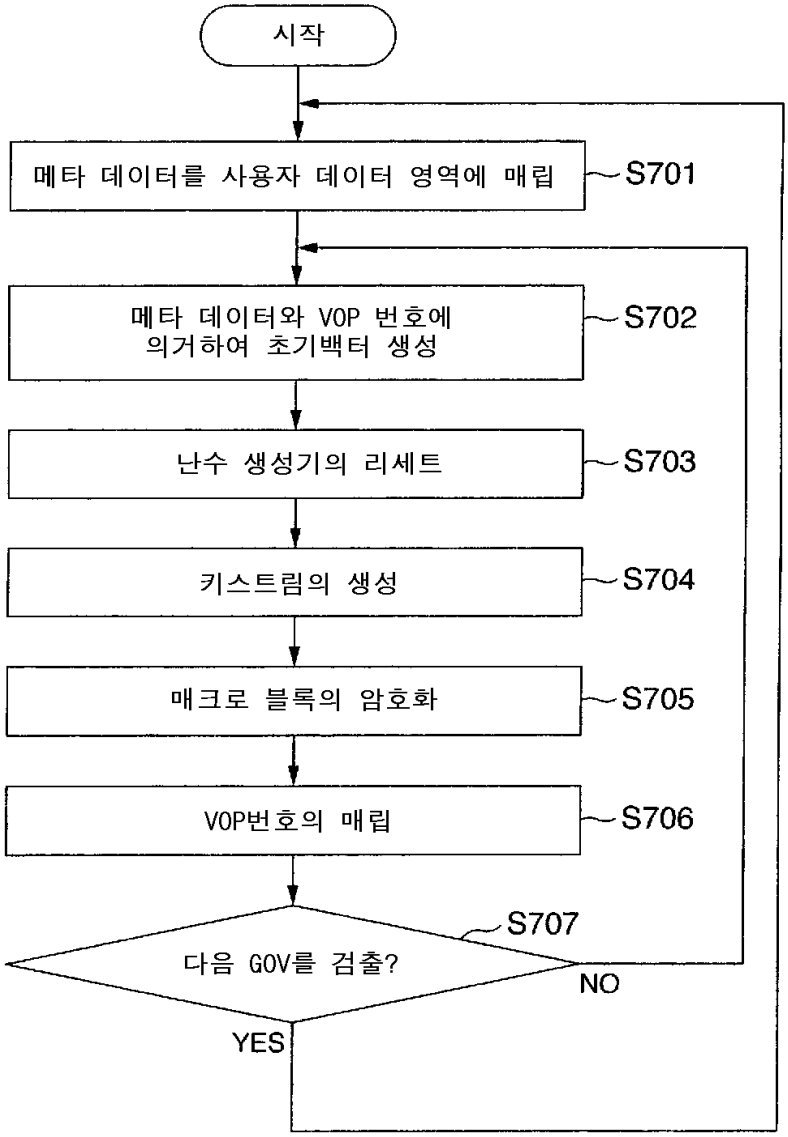
도면6


시작
메타 데이터를 사용자 데이터 영역에 매립
S601
메타 데이터에 의거하여 초기벡터 생성
S602
난수 생성기의 리세트
S603
키스트림의 생성
S604
매크로 블록의 암호화
S605
다음 GOV를 검출?
S606
NO
YES

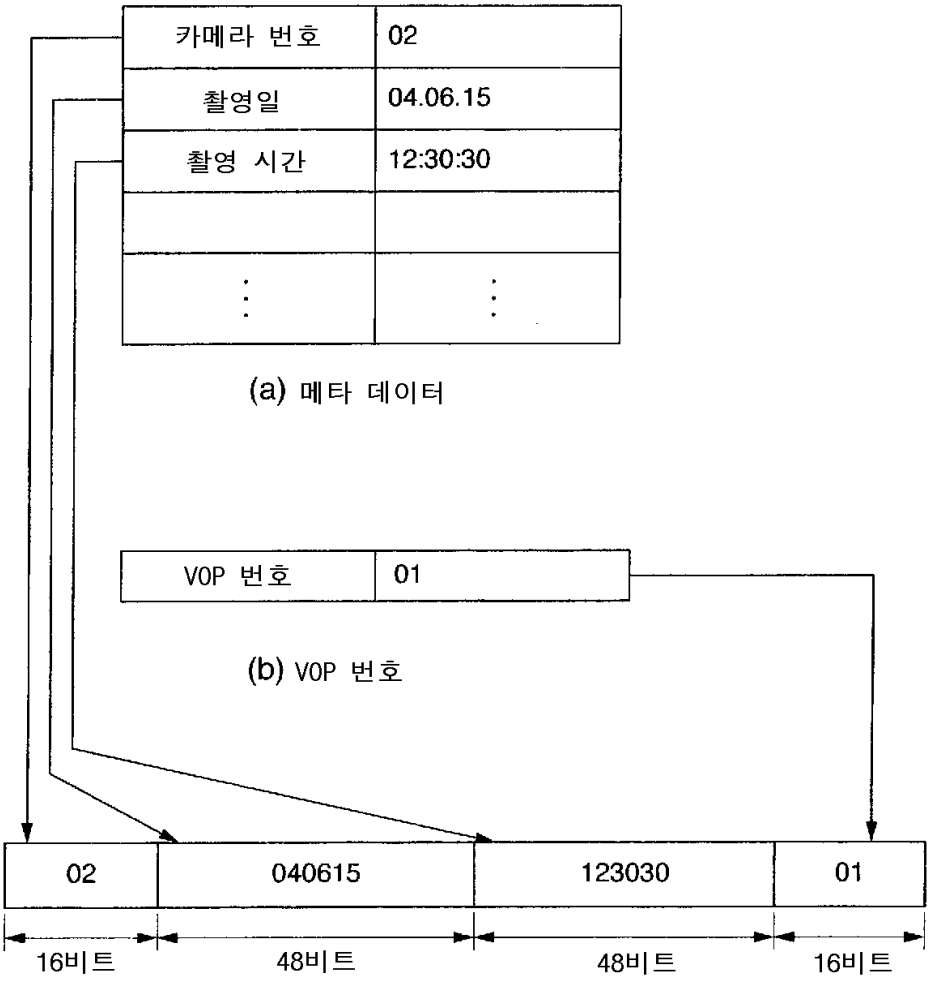
도면7


105
71
72
73
74
네트워크 인터페이스 부
암호 복호화 부
화상 복호화 부
모니터 인터페이스 부

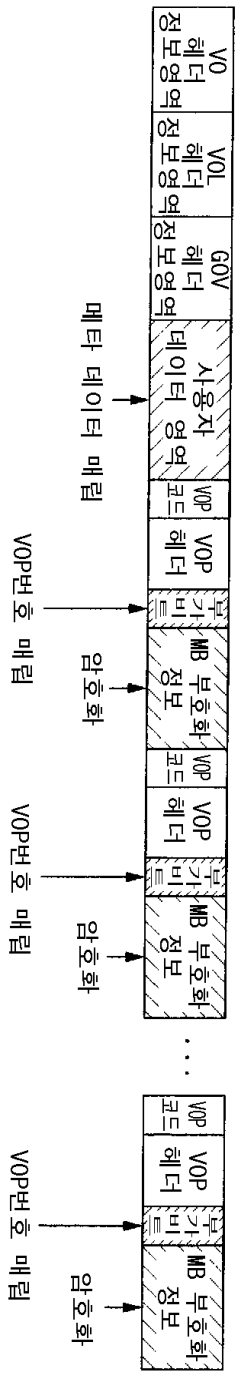
도면8


시작
메타 데이터를 사용자 데이터 영역에 매립
S701
메타 데이터와 VOP 번호에
의거하여 초기백터 생성
S702
난수 생성기의 리세트
S703
키스트림의 생성
S704
매크로 블록의 암호화
S705
VOP번호의 매립
S706
다음 GOV를 검출?
S707
NO
YES

도면9

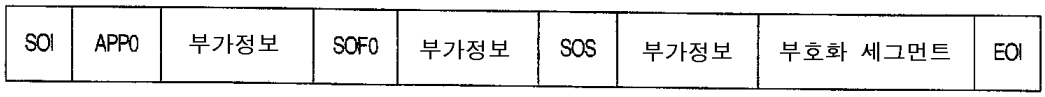

카메라 번호
02
촬영일
04.06.15
촬영 시간
12:30:30
(a) 메타 데이터
VOP 번호
01
(b) VOP 번호
02
040615
123030
01
16비트
48비트
48비트
16비트
(c) 초기 벡터(128비트)

도면10

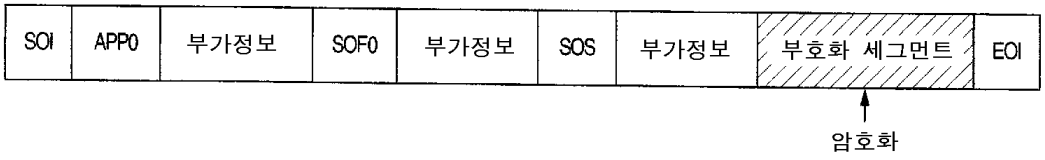

VO 헤더 정보영역
VOL 헤더 정보영역
GOV 헤더 정보영역
사용자 데이터 영역
VOP 코드
VOP 헤더
VOP번호 매립
메타 데이터 매립
뷰 가시비트
MB 부호화 정보
암호화
VOP 코드
VOP 헤더
VOP번호 매립
뷰 가시비트
MB 부호화 정보
암호화
VOP 코드
VOP 헤더
VOP번호 매립
뷰 가시비트
MB 부호화 정보
암호화

도면11

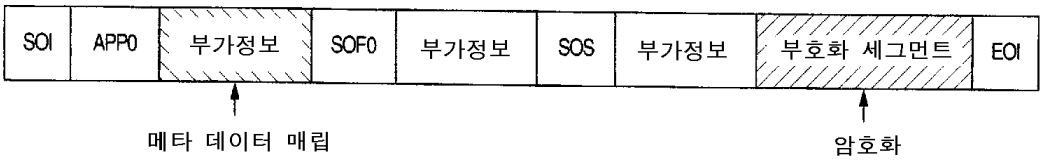
(a)


SOI
APP0
부가정보
SOF0
부가정보
SOS
부가정보
부호화 세그먼트
EOI

(b)


SOI
APP0
부가정보
SOF0
부가정보
SOS
부가정보
부호화 세그먼트
EOI
암호화

(c)


SOI
APP0
부가정보
SOF0
부가정보
SOS
부가정보
부호화 세그먼트
EOI
메타 데이터 매립
암호화