發明專利說明書 200428810

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：93112405

※ 申請日期：93.5.7　　※IPC 分類：H04K 1/00 H04L 29/06

壹、發明名稱：（中文/英文）

經 MPEG-4 IPMP 擴充之 ISMA 媒體串流收訊裝置

RECEIVER FOR RECEIVING ISMA MEDIA STREAMS SUPPORTING MPEG-4 IPMP EXTENSION

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

松下電器產業股份有限公司

MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

代表人：（中文/英文）

中村邦夫/NAKAMURA, KUNIO

住居所或營業所地址：（中文/英文）

日本國大阪府門真市大字門真 1006 番地

1006, OAZA KADOMA, KADOMA-SHI, OSAKA, 571-8501 JAPAN

國　籍：（中文/英文）

日本/JAPAN

參、發明人：（共 4 人）

姓　名：（中文/英文）

1. 吉明/JI, MING
2. 劉荊/LIU, JING
3. 申省梅/SHEN, SHENG MEI
4. 上野孝文/UENO, TAKAFUMI

住居所地址：（中文/英文）

1.新加坡#02-09 蓋良東大道 2 號大牌 10

BLOCK 10, GEYLANG EAST AVENUE 2, #02-09, 389758 SINGAPORE

2.新加坡#08-47 荷蘭村大牌 3

BLOCK 3, HOLLAND CLOSE, #08-47, 271003 SINGAPORE

3.新加坡溫德米爾#03-02 兆竹港街 64 號大牌 20

BLOCK 20, CHOA CHU KANG STREET 64, #03-02, WINDERMERE 689093 SINGAPORE

4.日本國奈良縣奈良市北登美丘 6 丁目 7-5

7-5, KITA-TOMIGAOKA 6-CHOME, NARA-SHI, NARA 631-0001 JAPAN

國　籍：（中文/英文）

1.～2.中國/CHINA　3.新加坡/SINGAPORE　4.日本/JAPAN

肆、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☑ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☑ 有主張專利法第二十七條第一項國際優先權：

1. 日本；2003.5.9；特願 2003-131856

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

發明領域

本發明係有關針對ISMA保護架構可兼容之MPEG-4 IPMP擴充。

【先前技術】

發明背景

近幾年間，對於透過網際網路的視訊和聲音傳輸提供保障的服務，在媒體內容流通業界已被廣泛的推展開來。各種標準化團體為了提供這個問題的解決對策而盡了許多努力。國際互聯網流媒體聯盟(ISMA：Internet Streaming Media Alliance)就是這種團體中的一個。供應商(vendor)為了構築可以在IP架構及網際網路上使用的視訊及聲音系統，藉明示所使用之可使用的，既存的開放標準架構來滿足此一需求。其做法雖然是假定要使用既存的MPEG技術，而主要對焦於現階段的MPEG-4，但是預計將來會包含MPEG-2及MPEG-7技術的變更和修正。

為供ISMA以及ISMA媒體串流所用，密碼化架構，亦即ISMACryp也已有了規定。此架構可以擴充到新的媒體符號化，可以對應新的密碼化，同時也可以適用於各種密碼鎖管理、安全性，或數位版權管理(DRM: Digital Right Management)系統。其亦另對適合ISMA做法的媒體串流及媒體訊息之認證用預設(default)密碼方式有所規定。第1圖所示為ISMA架構用之ISMACrpt保護的架構圖。第1圖之

ISMA DRM的範圍為ISMA媒體之密碼化及ISMA訊息之認證；在圖中標識為“ISMACryp”，ISMACryp的信號被標識為“RTSP/SDP+”(ISMA1.0 SDP definition · Plus ISMACryp信號)。主管理機構(Mastering)(1.1)負責內容的準備及發行。為了金鑰/認證管理介面而訂定之規約在ISMACryp的範圍外。另外，在第1圖中，從金鑰/認證(key/licence)管理到ISMA收訊機的金鑰(或認證)傳送，也在ISMACryp的範圍外。開發ISMACryp技術的目的係考量到要將如上所述的資訊發送到末端的安全方法。發訊機(1.2)係透過，或使用RTSP/SDP+(ISMA1.0 SDP definition · Plus ISMACryp信號)而在ISMA發訊機被發訊，或藉第3裝置被發訊之稱做“ISMACryp”的開放標準之規約，來負責對ISMA收訊機之發送工作。

在ISMA DRM架構中，ISMA收訊機可以處理被ISMA Cryp密碼化的串流、經過認證的訊息，以及發訊作業。“ISMACryp”係提供ISMA1.0媒體及具備密碼化、訊息認證、整體服務規約的技術。

第2圖更詳細地示意伴同對金鑰/認證管理(KEY MGT)、RTSP控制介面，以及ISMA資料用之密碼化服務，即ISMACryp的介面之ISMA收訊機架構。ISMACryp收訊機可以將ISMA資料密碼化、認證，並檢查其完整性。

第3圖所示為串流受到檔案控制或編碼後，直接在網路上被串流的ISMACryp環境之圖式。任何一種情形都是在發送前被密碼化，但訊息認證是在發送時執行。在收訊機(媒

體播放器/解碼器)中，串流或是由在播放器(player)、快取伺服器(cache server)的個人記錄器(personal recorder)等之檔案所接收，或是直接被解碼器所接收。ISMACryp變換是在編碼器/發訊機進行，解讀則是在以解碼器/收訊機形成終端之arc上進行。

根據ISMA宣言，係以2種收訊機，亦即ISMA專用收訊機及MPEG系統對應收訊機為對象。此處，"ISMA專用收訊機"之定義係指不對應MPEG-4，亦即無法完全處理伴同MPEG-4信號通知(發訊)以及MPEG-4(基本)媒體串流的控制(基本)串流之收訊機。相對於此，"MPEG系統對應收訊機"不僅可以處理ISMA相關資訊，也可以處理MPEG-4系統層資訊。和MPEG系統對應收訊機的相互運用可能性，可以透過至少傳送最小限度的MPEG系統訊號之MPEG IOD(初期物件描述)來實現。IOD係以其二進位SDP(session description protocol，工作階段描述規約)屬性，亦即SDP IOD而被包含。

ISMACryp同時可以適用於兩種型式的收訊機。將SDP訊息內的二進位IOD加以擴充。新的發訊(signaling)要點在於其著重在不對稱，而非ISMA發訊中所看到的冗餘性。提供SDP IOD之"最小"及"基本"發訊參數(signaling parameter)，使得和收訊機之MPEG-4 IPMP系統的相互運用性達到最大。

但是，根據現行ISMACryp規定的IOD擴充並不完全，和最新的MPEG-4 IPMP擴充標準沒有整合性。其結果，

ISMA串流有無法以MPEG-4 IPMP擴充兼容收訊機正確辨識之虞。例如，ISMACryp標準規定使用存在IOD內的IPMP_Descriptor來發出ISMACryp保護的訊號。但是，如果根據MPEG-4 IPMP擴充，當IPMP保護存在時，在IOD內就應該提示工具表單描述符。這些條件的不完整性和不整合性都有可能阻礙ISMA架構之與MPEG-4 IPMP擴充兼容收訊機的相互運用可能性。

【發明內容】

發明概要

本發明之目的在於解決以下的課題。

ISMACryp標準係透過SDP內之IOD擴充，並使用MPEG-4 IPMP，藉以規定ISMACryp保護的發訊。IOD內的IPMP_Descriptor之存在會對收訊機發出該媒體串流已受到保護的通知。在MPEG IPMP非兼容收訊機的情形中，允許用雖然獨特但是適切的方法來處理串流。例如，單純地忽視串流。但是，MPEG-4 IPMP擴充標準規定要在IOD內提示工具表單描述符並顯示IPMP保護。在標準中，並不保證為了IPMP保護，在IOD內會有IPMP_Descriptor存在。因此，在ISMACryp所規定的發訊方法中，IOD雖然包含工具表單描述符，卻有無法正確地檢知不包含IPMP_Descriptor之媒體串流已經受到保護的機構之虞。

此外，MPEG-4 IPMP擴充兼容收訊機為了要能夠接收ISMA相關資料，例如伴隨IPMP資料的密碼化資訊和KMS構成，ISMACryp標準乃依據MPEG-4 IPMP標準，以受到自

我規定的ISMACryp_Descriptor來擴充IOD內之IPMP_Descriptor。但是，因為MPEG-4 IPMP標準的改訂快速，所以IOD的語法(syntax)被變更，和ISMACryp標準所依據的舊版有所差異。這個情形所造成的問題在於，恐有無法以和最新的MPEG-4 IPMP擴充標準間具有兼容性的收訊機，來識別被容納在IPMP上下文(context)的ISMA相關資料之虞。為了讓已經完成規定的ISMA參數之變更侷限在最小限度，同時保有最新的MPEG-4 IPMP擴充標準之一貫性，根據現行MPEG-4 IPMP擴充標準來容納ISMA相關資料的動作就有必要被形成為可能的新構造，且該構造要求要與MPEG-4 IPMP擴充標準的舊版有向下兼容性(backward compatible)。

本發明之目的即在於針對ISMA保護架構提供可兼容之MPEG-4 IPMP擴充。

本發明為了處理發訊問題，對於將MPEG初期物件描述符(IOD)中之ISMACryp保護的存在做成訊號之發訊機構加以規定。使用工具表單及IPMP描述符將保護予以發訊。該方法與最新的MPEG-4 IPMP擴充標準具有兼容互換性，同時提供與MPEG系統對應ISMA收訊機之最大限的兼容性。另外，提供具彈性的方法，以識別播放內容時所需要的工具。

本發明也對容納ISMACryp參數並且變換成MPEG系統對應ISMA收訊機用之構造做成規定。可以從依據MPEG-4 IPMP擴充所規定之IPMP_Data_BaseClass擴充ISMA專用

Cryp_Data，並容納ISMACryp參數。該ISMACryp_Data因為是準據MPEG-4 IPMP擴充標準，所以可以收容成IPMP描述符或IPMP串流。

本發明之經MPEG-4 IPMP擴充的ISMA媒體串流收訊裝置，係

接收包含有顯示ISMA磁頭、內容，和前述內容之處理方法的IPMP工具表單描述符之ISMA媒體串流；

自前述ISMA媒體串流取得前述IPMP工具表單描述符；

檢查前述IPMP工具表單描述符所表示之工具是否存在於前述收訊裝置；

當前述工具存在時，用前述工具處理前述內容，無前述工具時，則在不發生停滯的情形下結束作業。

再者，所謂不發生停滯的情形下結束作業係指，執行預先設定之處理而結束作業。停滯意指，例如斷線等。

另，前述ISMA媒體串流帶有IOD；前述IPMP工具表單描述符係自前述IOD取得。

再者，本發明之經MPEG-4 IPMP擴充的ISMA媒體串流收訊裝置，係

接收包含有顯示ISMA磁頭、內容，和前述內容之處理方法的IPMP工具表單描述符之ISMA媒體串流；

自前述ISMA媒體串流取得前述IPMP描述符；

檢查前述IPMP描述符所表示之工具是否存在於前述收訊裝置；

當前述工具存在時，即用前述工具處理前述內容，無前述工具時，則在不發生停滯的情形下結束作業。

又，前述ISMA媒體串流進一步包含指定前述IPMP描述符的IPMP描述符指標(IPMP descriptor pointer)；前述收訊裝置由前述ISMA媒體串流取得前述IPMP描述符指標；

以取得前述IPMP描述符指標所指定的位址之前述IPMP描述符為宜。

再者，由前述ISMA媒體串流之ES描述符取得前述IPMP描述符指標，由前述ISMA媒體串流之OD取得前述IPMP所指定之前述IPMP描述符之構成亦佳。

另，ISMACryp解讀工具為前述IPMP描述符所指定時，起動前述ISMACryp解讀工具來執行前述內容之解讀亦可。

此外，由被前述IPMP描述符所收納之ISMACryp_Data取出ISMACryp參數，

用前述被取出之ISMACryp參數來設定ISMACryp解讀工具以執行前述內容之解讀的構成亦佳。

又，從被前述ISMA媒體串流之IPMP串流內的IPMP訊息所收納之ISMACryp_Data，取出ISMACryp參數，

用前述被取出之ISMACryp參數來設定ISMACryp解讀工具以執行前述內容之解讀的構成亦佳。

另外，前述ISMA媒體串流除了前述IPMP描述符外，進一步包含顯示前述至少一種工具的IPMP工具表單描述符，

前述收訊裝置為，取得前述IPMP工具表單描述符或前述IPMP描述符，並檢查顯示前述IPMP工具表單描述符或前述IPMP描述符之工具是否存在於前述收訊裝置的構成亦佳。

可是，IOD及OD被構成在ISMA架構內。IPMP工具表單描述符被埋入IOD內，當ISMACryp保護存在時，IPMP描述符指標及IPMP描述符被埋入IOD及OD內。

IOD及OD透過SDP IOD發訊被傳送到理解MPEG-4系統的ISMA收訊機。收訊機會解析IOD與OD。如果檢知IPMP工具表單，收訊機就會辨識到有ISMACryp保護存在的情形。如果檢知IPMO描述符指標和IPMP描述符，收訊機就可以辨識那一個串流被那一種工具所保護。

在ISMA架構內，當串流受到ISMACryp保護時，ISMACryp參數(例如密碼識別子)被ISMACryp_Data所收納，可以帶入IPMP描述符或IPMP串流內，參數之收納即會準據MPEG-4 IPMP擴充。

在收訊機側，可以從和MPEG-4 IPMP擴充同時保有兼容性的IPMP描述符或IPMP串流取出ISMACryp用的參數。接著可以用該參數來設定ISMACryp解讀工具。

透過使用本發明，ISMA保護架構可以達成和MPEG-4 IPMP擴充兼容收訊機的相互運用。

本發明用IOD內的工具表單及OD內的IPMP描述符來發出ISMACryp保護的訊號。藉此，發訊方法可以依情形做出判斷和處置，和最新的MPEG-4 IPMP擴充標準真正地具

有兼容性，因此可以使得MPEG系統對應ISMA收訊機成為可以相互運用。

本發明另外還生成從IPMP_Data_BaseClass擴充來的ISMACryp_Data。用根據本發明之ISMACryp_Data，可以收納ISMACryp參數，接著收納在IPMP描述符或IPMP串流之任一者內。ISMACryp參數之收納現在已成為IPMP擴充遵循事項了。

圖式簡單說明

第1圖所示為ISMACryp之架構。

第2圖為IPMPCryp收訊機的架構之示意圖。

第3圖係採用IPMPCryp的保護之端末間流程的示意圖。

第4圖所示為MPEG-4 IPMP擴充內容構造。

第5圖為使用IPMP描述符之保護發訊的示意圖。

第6圖為被攜入SDP內之IOD中的IPMP資訊示意圖。

第7圖係在ISMA收訊機之IPMP-X處理的流程圖。

【實施方式】

實施發明之最佳態樣

IPMP擴充發訊

現行ISMACryp對應到ISMA專用及適合MPEG收訊機之SDP IOD發訊。ISMA專用收訊機僅受理SDP FMTP發訊參數，而SDP IOD則是串流受到ISMACryp保護(最小IPMP訊號)，必須對任意的MPEG收訊機發訊。KMS也可以僅採用SDP IOD內之IPMP信號(基本IPMP信號)來將ISMACryp

予以發訊。

在本說明書中提供和MPEG-4 IPMP擴充具有兼容性之語法。用最小限度的勞動力，ISMACryp就可以容易地實現和MPEG-4 IPMP擴充的兼容性，並且提供具彈性的防護架構。

最小IPMP-X發訊

IPMP擴充規定在IOD的IPMP工具表單描述等。其後，工具表單描述符以出來的串流列來識別必要的IPMP工具清單。若依MPEG-4 IPMP擴充，當IPMP保護存在時，工具表單描述符會在IOD內被提示。因此，在最小限的IPMP-X發訊的情形中，為實現此目的，係提案以使用IOD內之IPMP工具表單描述符來取代IPMP描述符。

在被SDP攜入MPEG-4 IOD的IOD中之IPMP工具表單的位置在第6圖中表示為6.1。

根據指定密碼化及KMS資訊傳送之現行的ISMACryp方法，以至少有2個工具被提示在MPEG IPMP工具表單描述符中為宜。最初的項目為KMS工具，其他項目為ISMA解讀工具。在MPEG IPMP工具表單中之ISMACryp工具的存在會將ISMACryp保護予以發訊。

具有ISMACryp工具的工具表單描述符之例示於表1。

表1

	IPMP_工具表單描述符(ToolListDescriptor)		
1	8	IPMP_ToolListDescTag	0×60
2	16	描述符之大小	
		IPMP_Tool	
3	8	IPMP_ToolTag	0×61
4	16	描述符之大小	
5	128	IPMP_ToolID	數值由各服務供應商分配給自己的KMS工具
6	1	IsAltGroup	0
7	1	IsParameteric	0
8	6	預約	0b0000.00
9	8	工具URL的大小	
10		工具URL	
		IPMP_Tool	
11	8	IPMP_ToolTag	0×61
12	16	描述符的大小	
13	128	IPMP_ToolID	數值分配給ISMA解讀工具
14	1	IsAltGroup	0
15	1	IsParameteric	0
16	6	預約	0b0000.00
17	8	工具URL的大小	
18		工具URL	

IPMP工具表單係以示於第4圖之MPEG-4 IPMP擴充內容構造來表示。因使用IPMP工具表單(4.1)，故不僅可以容易地執行ISMACryp保護之存在的發訊工作，而且可以極為彈性地執行工具之識別。在工具表單的IPMP工具可以用3種方法來識別。第一種方法使用數值為公家登錄機關所分配之固定128 bit IPMP_ToolID (4.2)。第二種方法使用代表互為同等的替代物工具之IPMP_ToolID (4.3)的表單。藉這樣的處理方式，端末即可以更有彈性地執行自身之工具選擇。最後一種方法使用用以描述IPMP工具應該要滿足的基

準之參數表記(4.4)，惟此種情形，端末為實行必要的功能所需求之工具選擇自由度增大。

基本IPMP-X發訊

MPEG系統對應收訊機的情形因為要做IPMP相關的處理，故需要有更多的IPMP資訊。使用以下之IPMP-X發訊做為更高性能之MPEG IPMP擴充發訊的基礎。和在section 2所介紹的工具表單共同提供MPEG兼容收訊機所必要的基本資訊。相對於經密碼化的基本串流，對應的ES描述符必需包含以下的IPMP_DescriptorPointer(表2)。

表2

描述符名稱			
欄位編號	位元大小	欄位名稱	數值
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	描述符大小	5
3	8	IPMP_DescriptorID	0×FF
4	16	IPMPX_DescriptorID	0×0002/0×0003
5	16	IPMP_ES_ID	0×0000

此種IPMP擴充保護發訊的概念示於第5圖。因為ES_Descriptor內之該描述符指標(5.1及5.2)存在，故和該描述符相關之串流會顯示出是受參考IPMP_Descriptor(5.3及5.4)所指定之IPMP工具所保護及管理的對象的情況。示於表3之參考IPMP_Descriptor應該被物件描述符所收納。

在因SDP而被攜入MPEG-4 IOD內之OD串流中的IPMP描述符的位置，在第6圖係以符號6.2來表示。

表3

描述符名稱			
欄位編號	位元大小	欄位名稱	數值
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	描述符大小	23
3	8	IPMP_DescriptorID	0×FF
4	16	IPMPS_Type	0×FFF
5	16	IPMP_DescriptorIDEx	0×0002/0×0003
6	128	IPMP_ToolID	數值分配給ISMA解讀工具
7	8	控制指標碼(point code)	0×01 (解讀緩衝器與解讀器之間)
8	8	序列碼	0×80

另外，IOD必須包含以下的IPMP_DescriptorPointer(表4)。由以下之例可知，用參考描述符表示之特定的DRM工具(密碼鎖管理系統)必須使用全域範圍生成執行個體(インタンス)。

表4

描述符名稱			
欄位編號	位元大小	欄位名稱	數值
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	描述符大小	5
3	8	IPMP_DescriptorID	0×FF
4	16	IPMP_DescriptorIDEx	0×0001
5	16	IPMP_ES_ID	0×0000

上開IPMP_DescriptorPointer指定IPMP_DescriptorIDEx為0×0001之IPMP_Descriptor。接著，被指定的

IPMP_Descriptor必須被提示在IOD(表5)中。KMS的情形需留意，因描述符之控制指標顯示為全域範圍，故應設定在0×00。

表5

描述符名稱			
欄位編號	位元大小	欄位名稱	數值
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	描述符大小	22
3	8	IPMP_DescriptorID	0×FF
4	16	IPMPS_Type	0×FFF
5	16	IPMP_DescriptorIDEx	0×0001
6	128	IPMP_ToolID	數值由各服務供應商分配給KSM工具
7	8	控制指標碼(point code)	0×00 (無控制指標)

以和IPMP擴充具有兼容性的方法收納ISMACryp資料。ISMACryp採用參數的組合來描述串流的密碼化。參數的組合列表如下。

表6

參數	數值	意義	預設
Crypto-suite	1..255	密碼、模式、金鑰長度等	1 1)
IV-length	1..8	IV之位元組單位長度	4
Delta-IV-length	0..2	Delta IV之位元組單位長度	0
Selective-encyption	0..1	選擇性地使串流密碼化時設定為'1'	0
Key-indicator-per-AU	0..1	複數個key indicator出現在封包時，設定為'1'	0
Key-indicator-length	0..255	Key indicator的位元組單位長度	0

1) 節10.0之AES-CTR預設值

因為以和IPMP擴充具有兼容性的方法收納參數，故

ISMACryp_Data可因IPMP-X而從所規定之IPMP_Data_BaseClass擴充。IPMP_Data_BaseClass係如下所示，被MPEG-4所規定。

```
Abstract aligned(8) expandable(2^28-1) class
IPMP_Data_BaseClass：
    bit(8) tag=0 .. 255
    {
    bit(8)      Version;
    bit(32)     dataID;
    // Fields and data extending this message.
    }
```

ISMACryp_Data採用使用者定義的標籤而可以從上面的BaseClass擴張。接著，為了收納參數，資料可以維持自身的欄位組合。藉此，解釋相同內容串流的不同機種ISMA端末的兼容性乃獲得保證。

該ISMACryp_Data可以用標準方法收納在2個地方。第一個是收納到IPMP描述符。具有該ISMACryp_Data的IPMP描述等之例示於表7。

表7

描述符名稱			
欄位編號	位元大小	欄位名稱	數值
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	描述符大小	23
3	8	IPMP_DescriptorID	0×FF
4	16	IPMPS_Type	0×FFFF
5	16	IPMP_DescriptorIDEx	0×0002/0×0003
6	128	IPMP_ToolID	數值分配給ISMA描述符工具
7	8	控制指標碼(point code)	0×01 (解讀緩衝器與解讀器之間)
8	8	序列碼	0×80
		ISMACryp_Data	
7	8	ISMACryp_DataTag	規定預定
8	8	資料大小	20
9	8	密碼組合	密碼描述符
11	4	IV-length	初期化向量的位元組長度
12	2	Delta-IV-length	AU基礎之IV的位元組長度
13	1	Selective-encyption	採用選擇的密碼化時1
14	1	Key-indicator-per-AU	封包中出現複數個key indicator時1
15	8	Key-indicator-length	key indicator的位元組長度

依SDP被攜入MPEG-4 IOD內之IPMP描述符，在OD串流的位置係如第6圖以符號6.2所示者。

收納ISMACryp_Data的第二種方法係當做IPMP_Message內之封包承載(payload)而收納，接著再如同以MPEG-4 IPMP擴充所規定一般，收納成IPMP串流。

Aligned(8) expandable(228-1) class IPMP_Message

```
{
    bit(16)        IPMPS_Type;
    if (IPMPS_Type==0)
    (
        bit(8) URLString[sizeOfInstance-2];
    )
    else (if (IPMPS_Type==0×0001)
    (
        bit(16) IPMP_DescriptorID;
            IPMP_Data_BaseClass IPMP_ExtendedData[]
    } else {
        bit(8) IPMP_data[sizeOfInstance-2];
    }
}
```

IPMP_Message收納了ISMACryp_Data時之語法示於表8。被帶有該IPMP_DescriptorIDEx之IPMP描述符所指定的IPMP工具即IPMP_Message之收件人姓名住址。

表8

欄位編號	位元大小	欄位名稱	數值
		IPMP_Message	
1	16	訊息大小	
2	16	IPMPS_Type	0×0001
3	16	IPMP_DescriptorIDEx	
		ISMACryp_Data	
4	8	ISMACryp_DataTag	規定預定
5	8	資料大小	20
6	8	密碼組合	密碼識別子
7	4	IV-Length	初期化向量的位元組長度
8	2	Delta-IV-length	AU基礎之IV的位元組長度
9	1	Selective-encryption	使用選擇性的密碼化時1
10	1	Key-indicator-er-Au	封包中出現可設定開機的組合鍵(multikey)指標時1
11	8	Key-indicator-length	Key indicator之位元組長度

在ISMA收訊機之IPMPX發訊的處理

根據上述IPMPX發訊，可以在ISMA收訊機將串流是否受到保護予以特定，而在有保護的情形下，則可以特定以何種方式進行處理。

在ISMA收訊機取得描述被賦與關連性的媒體串流之SDP參數時(S01)、先檢查是否具有稱為MPEG-4 IOD的屬性(S02)，當這個屬性存在時，就知道那個被賦與關連性的媒體串流係與MPEG-4系統有兼容性的串流。當所檢查的屬性不存在時，以非MPEG方法加以處理(S03)。其次，檢查MPEG-4 IOD內是否存在IPMP工具表單(S04)。當MPEG-4 IOD內存在IPMP工具表單時，得知係用IPMP擴充來保護那個媒體串流。然後依據被IPMP描述符所特定之Tool_ID來起

動工具(S06)。起動KMS工具以處理金鑰管理問題；起動密碼解讀工具以在經過特定的控制點處理媒體串流的密碼解讀(S07)。另外，檢查是否有IPMP描述符或被攜入IPMP串流的ISMACryp_Data (S08)，如果有，就將之傳送到密碼解讀工具，加以設定(S09)。再者，當上述步驟S04中不存在IPMP工具表單時，以非IPMP保護之MPEG方法處理(S05)。上述呈序示於第7圖。

再者，本發明可以取各種示於實施態樣之以下的構成。根據第1種構成，在ISMA收訊機側使用MPEG-4 IPMP擴充來執行ISMA媒體串流之彈性保護的裝置係包含，

從IOD接IPMP工具表單描述符的步驟，和

檢查工具表單所示之工具，當有被工具ID所識別之ISMACryp解讀工具時，檢查前述ISMACryp解讀工具是否存在，如果不存在，收訊機就在不發生停滯下拒絕接收的步驟，和

檢查工具表單所示之工具，當有被工具ID所識別之ISMACrypKMS工具時，檢查ISMACrypKMS工具是否存在，如果不存在，收訊機就在不發生停滯下拒絕接收的步驟。

根據第2種構成，上述所載之在ISMA收訊機側使用MPEG-4 IPMP擴充來執行ISMA媒體串流的彈性保護之裝置，其前述檢查IPMP工具表單的步驟進一步包含，

從ES描述符接收IPMP描述符指標，參考IPMP描述符從OD接收信號之步驟，和

當ISMACryp解讀工具被IPMP描述符指定時，起動ISMACryp解讀工具，根據前述ES描述符之描述開始進行受到保護之媒體串流的解讀之步驟。

根據第3種構成，上述所載之在ISMA收訊機側使用MPEG-4 IPMP擴充來執行ISMA媒體串流的彈性保護之裝置，其前述檢查IPMP工具表單的步驟進一步包含，

從ES描述符接收IPMP描述符指標，參考IPMP描述符從OD接收信號之步驟，和

當ISMACryp解讀工具被IPMP描述符指定時，起動ISMACryp解讀工具之步驟，和

從被IPMP描述符所收納之ISMACryp_Data取出ISMACryp參數之步驟，和

用前述被取出之ISMACryp參數來設定ISMACryp解讀工具，參考前述ES描述符以開始進行受到保護之媒體串流的解讀之步驟。

根據第4種構成，上述所載之在ISMA收訊機側使用MPEG-4 IPMP擴充來執行ISMA媒體串流的彈性保護之裝置，其前述檢查IPMP工具表單的步驟進一步包含，

從ES描述符接收IPMP描述符指標，參考IPMP描述符從OD接收信號之步驟，和

當ISMACryp解讀工具被IPMP描述符指定時，起動ISMACryp解讀工具之步驟，和

從被IPMP串流內之IPMP訊息收納的ISMACryp_Data取出ISMACryp參數之步驟，和

用前述被取出之ISMACryp參數來設定ISMACryp解讀工具，參考前述ES描述符以開始進行受到保護之媒體串流的解讀之步驟。

如上所述，本發明雖以較佳實施態樣詳為說明，惟本發明並不限次該等態樣，在以下所載之本發明的申請專利範圍內可以做成多種合適的變形例及修正例，對於熟習此項技術者乃自明的事實。

【圖式簡單說明】

第1圖所示為ISMACryp之架構。

第2圖為IPMPCryp收訊機的架構之示意圖。

第3圖係採用IPMPCryp的保護之端末間流程的示意圖。

第4圖所示為MPEG-4 IPMP擴充內容構造。

第5圖為使用IPMP描述符之保護發訊的示意圖。

第6圖為被攜入SDP內之IOD中的IPMP資訊示意圖。

第7圖係在ISMA收訊機之IPMP-X處理的流程圖。

【圖式之主要元件代表符號表】

(無)

伍、中文發明摘要：

一種經MPEG－4 IPMP擴充之ISMA媒體串流收訊裝置，其接收包含有顯示ISMA磁頭、內容，和前述內容之處理方法的IPMP 工具表單描述符之ISMA媒體串流；自前述ISMA媒體串流取得前述IPMP工具表單描述符；檢查前述IPMP工具表單描述符所表示之工具是否存在於前述收訊裝置；當前述工具存在時，即用前述工具處理前述內容，無前述工具時，則在不發生停滯的情形下結束作業。

陸、英文發明摘要：

A Receiver receives ISMA media streams supporting MPEG-4 IPMP extension. The ISMA media stream includes an ISMA header, a content, IPMP Toollist descriptor indicating a Tool for dealing with the content. The receiver receives the ISMA media streams, acquires the IPMP Toollist descriptor from the ISMA media streams, and checks whether the Tool exists in the receiver. If the Tool exists, the receiver deals with the content by using the Tool, if the Tool does not exist, the receiver terminates gracefully.

拾、申請專利範圍：

1. 一種接收經MPEP-4 IPMP擴充之ISMA媒體串流的訊號之裝置，其係，

接收包含有顯示ISMA磁頭、內容，和前述內容之處理方法的IPMP工具表單描述符之ISMA媒體串流；

自前述ISMA媒體串流取得前述IPMP工具表單描述符；

檢查前述IPMP工具表單描述符所表示之工具是否存在於前述收訊裝置；

當前述工具存在時，即用前述工具處理前述內容，無前述工具時，則在不發生停滯的情形下結束作業之收訊裝置。

2. 如申請專利範圍第1項記載之收訊裝置，特徵在於前述ISMA媒體串流帶有IOD，前述IPMP工具表單描述符係自前述IOD取得。

3. 一種接收經MPEP-4 IPMP擴充之ISMA媒體串流的訊號之裝置，其係，

接收包含有顯示ISMA磁頭、內容，和前述內容之處理方法的IPMP工具表單描述符之ISMA媒體串流；

自前述ISMA媒體串流取得前述IPMP描述符；

檢查前述IPMP描述符所表示之工具是否存在於前述收訊裝置；

當前述工具存在時，用前述工具處理前述內容，無前述工具時，則在不發生停滯的情形下結束作業。

4. 如申請專利範圍第3項記載之收訊裝置，特徵在於，

前述ISMA媒體串流進一步包含指定前述IPMP描述符之IPMP描述符指標，且前述收訊裝置係自前述ISMA媒體串流取得前述IPMP描述符指標，

取得前述IPMP描述符指標所指定的位址之前述IPMP描述符。

5. 如申請專利範圍第4項記載之收訊裝置，特徵在於自前述ISMA媒體串流的ES描述符取得前述IPMP描述符指標，自前述ISMA媒體串流之OD取得前述IPMP描述符指標所指定之前述IPMP描述符。

6. 如申請專利範圍第3項至第5項之任一項記載的收訊裝置，特徵在於當ISMACryp解讀工具在前述IPMP描述符被指定時，即起動前述ISMACryp解讀工具，執行前述內容之解讀。

7. 如申請專利範圍第6項記載之收訊裝置，特徵在於，

從被收納在前述IPMP描述符的ISMACryp_Data取出ISMACryp參數，

用前述所取出之ISMACryp參數來設定ISMACryp解讀工具，並執行前述內容之解讀。

8. 如申請專利範圍第6項記載之收訊裝置，特徵在於，

自前述ISMA媒體串流之IPMP串流內的IPMP訊息所收納之ISMACryp_Data取出ISMACryp參數，

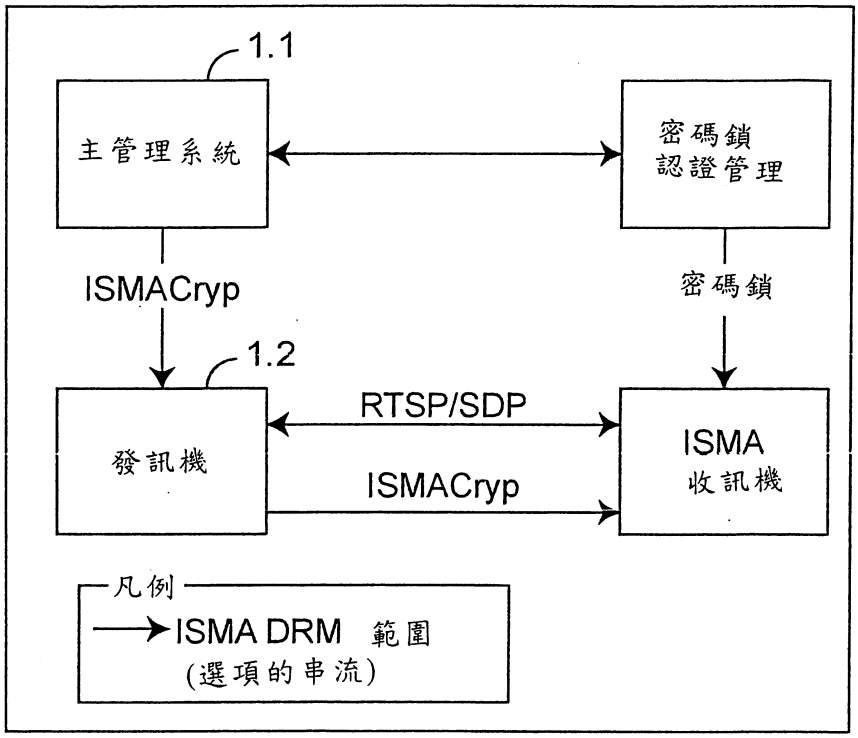
用前述所取出之ISMACryp參數來設定ISMACryp解讀工具，並執行前述內容之解讀。

9. 如申請專利範圍第3項記載之收訊裝置，特徵在於，

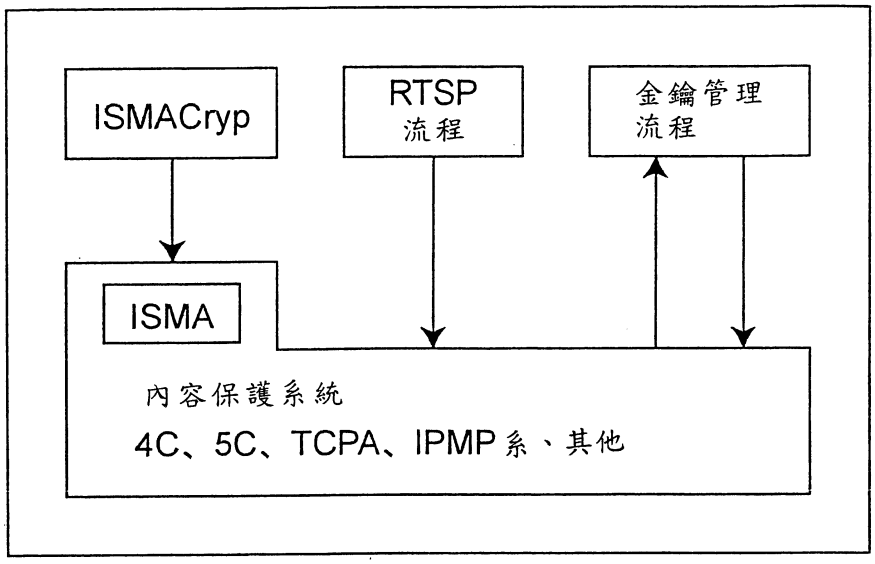
前述ISMA媒體串流除了前述IPMP描述符外，進一步包含顯示前述至少一種工具之IPMP工具表單描述符，

前述收訊裝置取得前述IPMP工具表單描述符或前述IPMP描述符，並檢查前述IPMP工具表單描述符或前述IPMP描述符所表示之工具是否存在前述收訊裝置內。

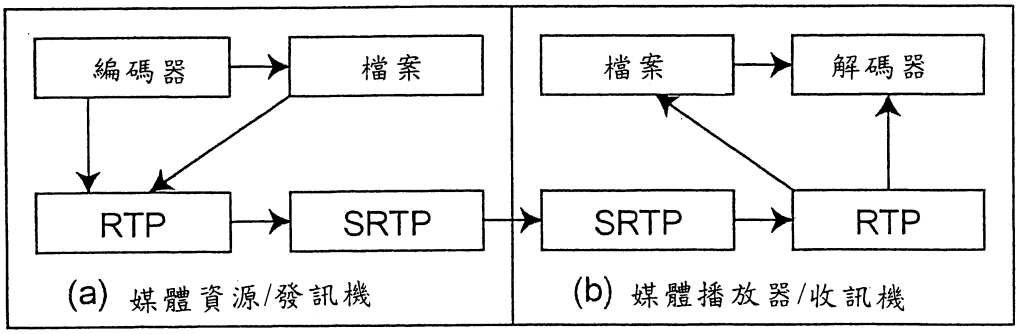
第 1 圖


1.1
主管理系統
密碼鎖
認證管理
ISMACryp
密碼鎖
1.2
RTSP/SDP
發訊機
ISMA
收訊機
ISMACryp
凡例
ISMA DRM 範圍
(選項的串流)

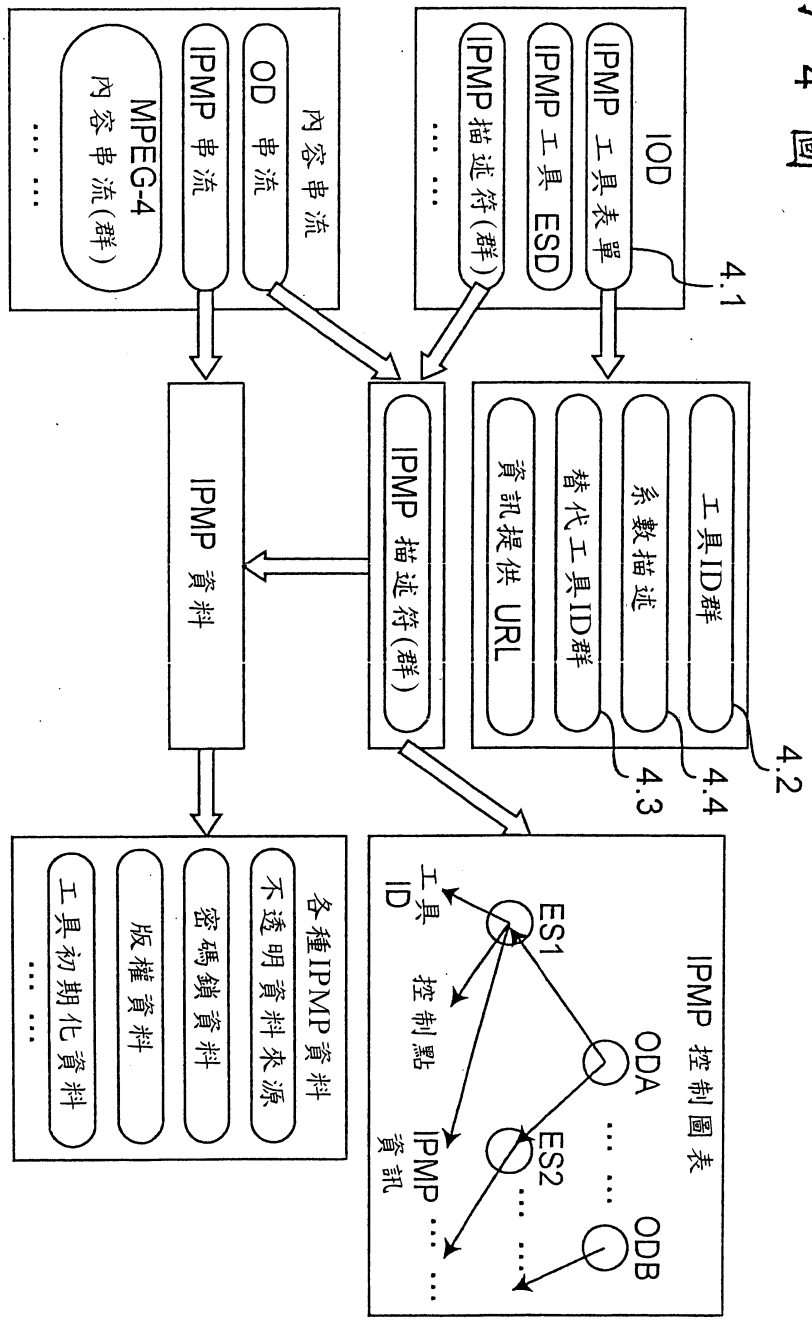
第 2 圖


ISMACryp
RTSP
流程
金鑰管理
流程
ISMA
內容保護系統
4C、5C、TCPA、IPMP系、其他

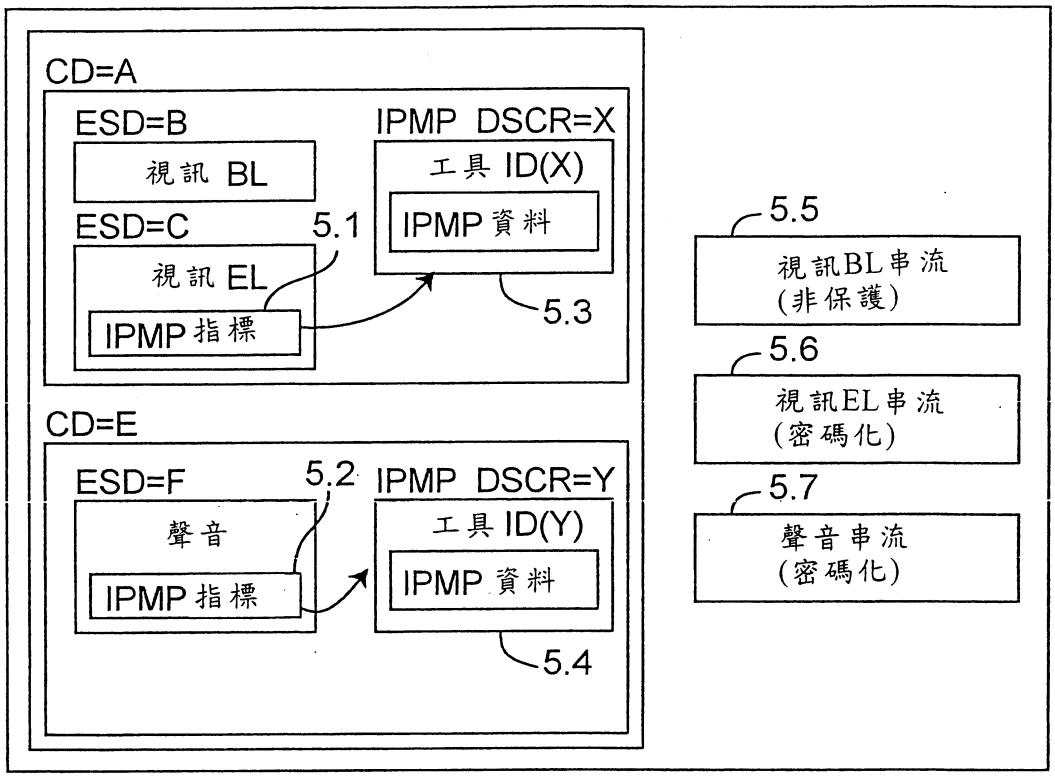
第 3 圖


編碼器
檔案
RTP
SRTP
(a) 媒體資源/發訊機
檔案
解碼器
SRTP
RTP
(b) 媒體播放器/收訊機

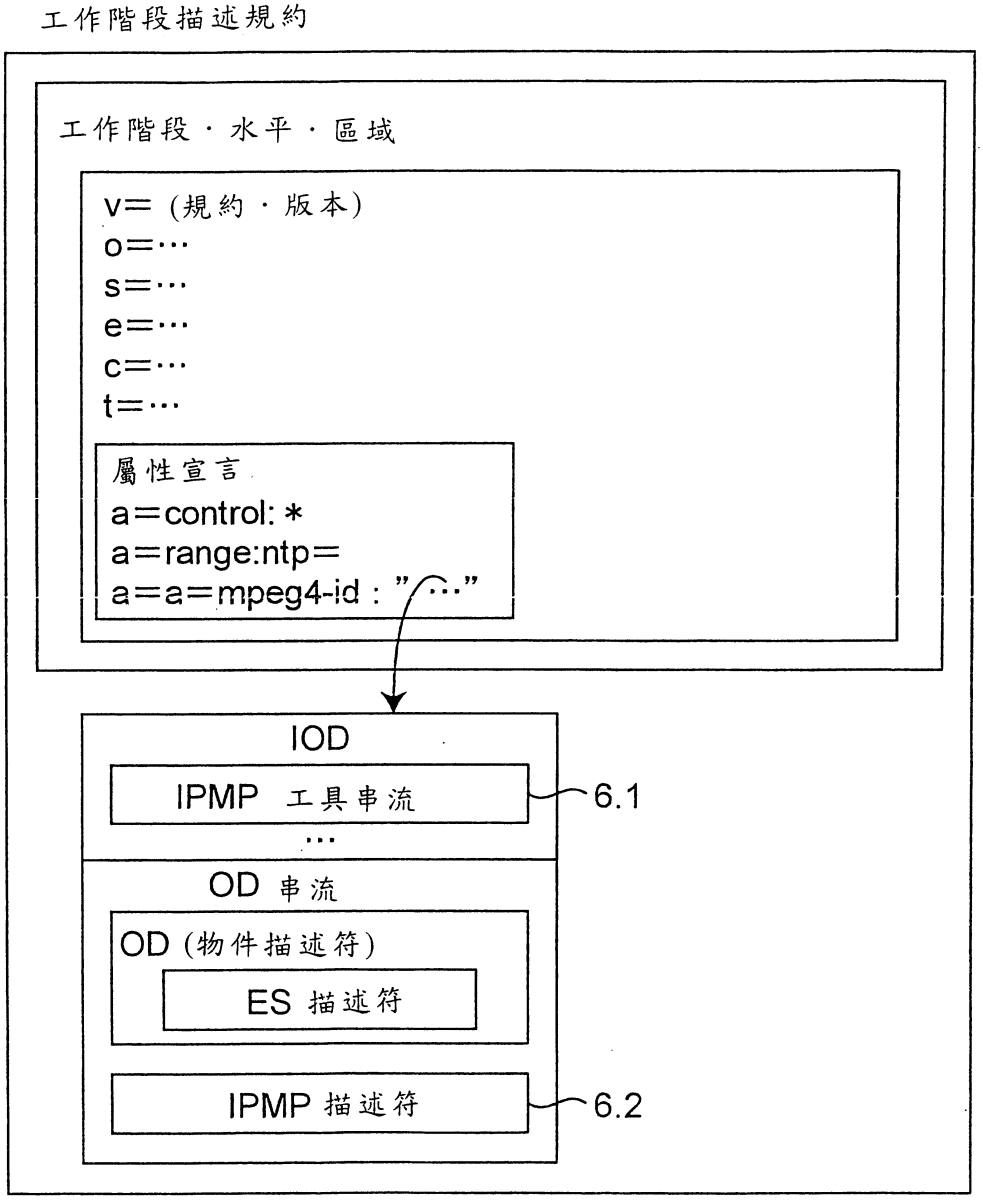
第 4 圖


IOD
IPMP 工具表單
IPMP 工具 ESD
IPMP 描述符(群)
… …
4.1
內容串流
OD 串流
IPMP 串流
MPEG-4
內容串流(群)
… …
工具ID群
系數描述
替代工具ID群
資訊提供 URL
4.2
4.4
4.3
IPMP 描述符(群)
IPMP 資料
IPMP 控制圖表
ODA
… …
ODB
ES1
ES2
… …
… …
工具 ID
控制點
IPMP 資訊
各種IPMP資料
不透明資料來源
密碼鎖資料
版權資料
工具初期化資料
… …

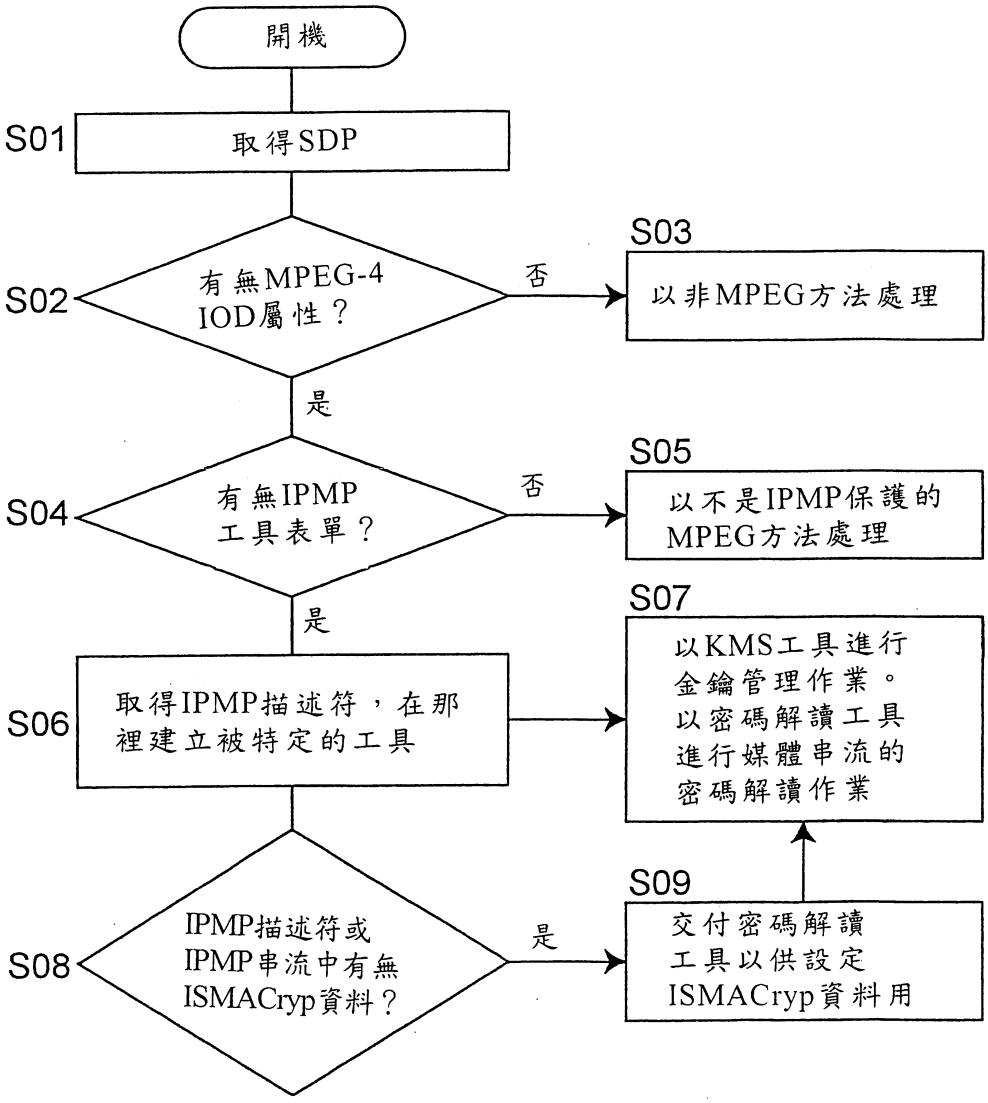
第 5 圖


CD=A
ESD=B
視訊 BL
ESD=C
視訊 EL
IPMP 指標
5.1
IPMP DSCR=X
工具 ID(X)
IPMP 資料
5.3
CD=E
ESD=F
聲音
IPMP 指標
5.2
IPMP DSCR=Y
工具 ID(Y)
IPMP 資料
5.4
5.5
視訊BL串流
(非保護)
5.6
視訊EL串流
(密碼化)
5.7
聲音串流
(密碼化)

第 6 圖


工作階段描述規約
工作階段・水平・區域
v=（規約・版本）
o=…
s=…
e=…
c=…
t=…
屬性宣言
a=control: *
a=range:ntp=
a=a=mpeg4-id：”…”
IOD
IPMP 工具串流
6.1
…
OD 串流
OD（物件描述符）
ES 描述符
IPMP 描述符
6.2

第 7 圖


開機
S01
取得SDP
S02
有無MPEG-4 IOD屬性？
否
S03
以非MPEG方法處理
是
S04
有無IPMP 工具表單？
否
S05
以不是IPMP保護的 MPEG方法處理
是
S06
取得IPMP描述符，在那裡建立被特定的工具
S07
以KMS工具進行金鑰管理作業。以密碼解讀工具進行媒體串流的密碼解讀作業
S08
IPMP描述符或IPMP串流中有無ISMACryp資料？
是
S09
交付密碼解讀工具以供設定ISMACryp資料用

柒、指定代表圖：

(一)本案指定代表圖為：第（ 4 ）圖。

(二)本代表圖之元件代表符號簡單說明：

(無)

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)