行政院國家科學委員會專題研究計畫　成果報告

子計畫五:MPEG 智財管理與保護系統及視訊小波編碼器之設計與模擬(III)

計畫類別：整合型計畫
計畫編號：NSC94-2219-E-009-011-
執行期間：94 年 08 月 01 日至 95 年 07 月 31 日
執行單位：國立交通大學電子工程學系及電子研究所

計畫主持人：杭學鳴

計畫參與人員：張峰誠，洪朝雄，呂家賢，朱浩廷，吳巧琳

報告類型：完整報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 95 年 10 月 17 日

行政院國家科學委員會補助專題研究計畫 ■ 成 果 報 告
□期中進度報告

基於 MPEG 標準之多媒體通訊整合平台及其應用(III) —子計畫五：MPEG 智財管理與保護系統及視訊小波編碼器之設計與模擬(III)
MPEG IPMP System and Interframe Wavelet Codec Design and Simulation (III)

計畫類別：□ 個別型計畫 ■ 整合型計畫
計畫編號： NSC 94-2219-E-009-011

執行期間： 94 年 8 月 1 日至 95 年 7 月 31 日

計畫主持人：杭學鳴
計畫參與人員：張峰誠 洪朝雄 呂家賢 朱浩廷 吳巧琳

成果報告類型(依經費核定清單規定繳交)：□精簡報告 ■完整報告

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學電子工程學系

中 華 民 國 95 年 10 月 15 日

行政院國家科學委員會專題研究計畫成果報告

MPEG 智財管理與保護系統及視訊小波編碼器之設計與模擬(III)

MPEG IPMP System and Interframe Wavelet Codec Design and Simulation (III)

計畫編號：NSC 94-2219-E-009 -011

執行期限：94 年 8 月 1 日至 95 年 7 月 31 日

主持人：杭學鳴　　國立交通大學電子工程學系教授

計畫參與人員：張峰誠 洪朝雄 呂家賢 朱浩廷 吳巧琳

國立交通大學電子研究所研究生

中文摘要

本報告分兩部分，第一部分是 MPEG-21 智財權系統，第二部分是輪廓轉換(contourlet transform)之研究。常見的多媒體保護機制大多使用加密演算法對內容進行保護。但是對於日趨複雜的使用環境，被動的內容加密機制已經不敷所需，必須考慮一個進階的機制來描述特定使用者的權限，因此我們透過MPEG-21權利描述語言(Rights Expression Language, REL)來滿足此需求。MPEG-21 標準的權利描述語言不但能描述使用者的權限，還能在 MPEG-21 標準所訂定的平台上流通。本研究使用 MPEG-21 IPMP、MPEG-21 REL 和 MPEG-21 Test Bed with MPEG-4 IPMPX 之觀念與工具來創建我們的系統。MPEG-21 IPMP 定義高層次的 Digital Item 保護機制。MPEG-21 REL 能夠描述廣泛的使用權利，亦提供清晰的權利認證與控管機制。然而 MPEG-21 IPMP 與 REL 僅提供概念上的定義，因此我們選用 MPEG-21 Test Bed 作為實現的平台。藉由修改 MPEG-4 IPMPX 定義的介面，我們在 Test Bed 上加入 IPMPX 功能，並據以實現數個 IPMP 與 REL 工具。最後，利用三個範例展現我們的 DRM 系統。範例(一)展示在串流應用的環境下使用即時的權利認證和內容保護的能力。範例(二)表現如何設計和使用 license 讓使用者預視影像短片。範例(三)則展現一個比較複雜的 Super Distribution 範例，利用我們設計的 REL license 提供線上與離線的驗證。

自然界的影像在經過空間轉換到頻域(frequency domain)之後，大部分的能量都集中在低頻上，搭配有效率的熵編碼(entropy coding)後，可以提升壓縮效率。近年來由於可調整性(scalability)的需求越來越熱門，因此小波轉換(wavelet transform)的研究也越來越熱門。但是小波轉換對二維訊號的表示法卻不是很理想，因為它忽略了二維方向的連續性，故後來有人提出了方向性濾波器頻帶(directional filter bank)的轉換，如曲線轉換（curvelet transform）和輪廓轉換(contourlet transform)。本研究主要基於 Minh N. Do 的輪廓轉換，觀察各次頻帶(subband)的輸出結果。影像經過兩次拉式金字塔的拆解後，把最高頻的部分作 8 個方向的 2 維方向性濾波頻帶拆解，中間的頻率部分則是作 4 個方向的頻帶拆解，最低頻的部分不作方向性的拆解。觀察實驗結果可以發現，只要影像的邊緣(edge)和某個頻帶一致性越大，在那個方向上就會有越強的訊號出現。

關鍵字: MPEG-21, IPMP, REL, 小波轉換, 方向性多重濾波, 輪廓轉換。

英文摘要

There are two parts in this report. The first part is a design and implementation of the MPEG-21 digital rights management system and the second part is to explore a recent image tool -- contourlet transform. Encryption is a widely used technique to protect digital multimedia contents. Due to the more and more complex usage scenarios, it is not sufficient to protect contents using only the passive mechanism (encryption). We need an advanced way to describe the rights of a specific user. Thus, we adopt the MPEG-21 Rights Expression Language (REL) to fulfill the requirements, which is not only able to specify the rights, but also guarantees to be interoperable among MPEG-21 compliant platforms. In this research, we incorporate MPEG-21 IPMP, MPEG-21 REL, and MPEG-21 Test Bed with MPEG-4 IPMPX concepts to construct the system. The MPEG-21 IPMP defines the high-level protection mechanism for Digital Items. The MPEG-21 REL can be used to describe a wide range of digital rights, and it also provides a clearly defined authorization mechanism. The MPEG-21 IPMP and REL define the concepts and interfaces. To implement a practical system, we choose the MPEG-21 Test Bed as the platform. By tailoring the MPEG-4 IPMPX interfaces, we extend the Test Bed with IPMPX capabilities. Based on the subsystem, we implement several IPMP and REL related tools. At the end, we demonstrate our DRM platform using three application examples. The first example demonstrates the real-time rights verification and content protection in a streaming environment; the second demonstrates the rights control of previewing a video clip; and the third one shows that a sophisticated super-distribution scenario can be achieved by using a customized REL license together with on-line/off-line authorizations.

By transforming a natural image to the frequency domain, it is known that the energy tends to be compact in the low-frequency bands. This property is useful for compressing natural images. Nowadays the demands for scalable coding become stronger and stronger. Hence, researches of wavelet transforms are getting more popular. Previous works show that the 2-D separable wavelet transform as a tool for compression has its limit, due to the ignorance of the continuity in the directions other than horizontal and vertical. Directional filter banks, such as the curvelet transform and contourlet transform, are proposed to overcome this problem. Our research is to investigate the potential coding gain of each subband decomposed by the contourlet transform, which is proposed by Minh N. Do. We use a two-level pyramid Laplacian transforms. The high-frequency part of a transformed image goes through an 8-directional filter banks; the mid-frequency part goes through a 4-directonal filter bank and the low-frequency part is kept unaltered. The results show that a stronger filtered output appears along the edge direction that is consistent with the designed direction of the corresponding filter.

Keywords: MPEG-21, IPMPX, REL, wavelet, directional filter bank, contourlet.

目錄

報告內容

第一部份 MPEG-4 IPMP 與 MPEG-21 REL 智財權系統

A. 背景與目的

隨著網路技術與數位媒體科技的進步，民眾可以輕易的創建與傳遞各種數位化的多媒體內容。如何對此種數位化的智慧財產權加以保護便成為一個重要的議題。因此現今的多媒體傳輸平台多設計相對應的機制來實現數位智財權保護與管理。

常見的多媒體保護機制大多使用各種的加密演算法對內容進行保護。但是對於日趨複雜的使用環境(特定的使用條件，例如：使用時間與實用次數的限制)，被動的內容保護機制(Encryption)已經無法確保智慧財產權不會被使用者侵犯，必須考慮一個較為特殊的機制用來描述特定使用者的特定權限，因此我們透過權利描述語言(Rights Expression Language)來滿足此需求。一般來說，權利描述語言能夠描述一個合法的使用條件：包含特定的使用者、使用條件、針對特定的內容執行被允許的動作。

目前有許多發展中的權利描述語言，其中由 MPEG-21 標準[1] 所訂定的權利描述語言(REL)不但能描述使用者的權限，還能在 MPEG-21 標準所訂定的平台上流通。這個平台讓透過不同的網路或設備取得的多媒體內容都能夠被使用。在 MPEG-21 標準中與智財權保護相關的子部分有以下兩個：(1) MPEG-21 IPMP[2] :訂定系統層之上的智慧財產權保護與管理的概念與架構、(2)MPEG-21 REL[3] :訂定權利描述語言。

在本研究中我們探討 MPEG-21 IPMP 與 REL 這兩個標準，並且透過 MPEG-4 IPMPX[4] 所定義的智財權保與及管理的系統介面來展現這兩個規範的功能。最後在 MPEG-21 的測試平台(Test Bed)[5] [6] [7] 上發展具有智財權保護及管理功能之多媒體傳輸系統。

B. 研究步驟 – MPEG-21 IPMP 與 REL 標準及架構

MPEG-21 IPMP

MPEG-21 IPMP 的目的是透過定義受保護的數位項目(Digital Item)提供權利與智財權的管理。數位項目為 MPEG-21 標準中的主要施行對象，任何可以被數位化的資源都可被稱作數位項目，例如：文字檔案、多媒體短片。為了描述各種不同類型的數位項目，MPEG-21 標準在第二個子部分 DID[8] 中訂定了數位項目描述語言(Digital Item Description Language)，以下簡稱為 DIDL。

為了保護 DI 中的重要部分，MPEG-21 IPMP 發展了一個提供保護 DI 的描述語言(IPMP DIDL)。由於 DIDL 與 IPMP DIDL 這兩種描述語言都是用來表示相同的 DI，因此他們在語意上必須互通。在 IPMP DIDL 中，每一個 DIDL 的元素都擁有可供替換的對等元素(如圖 2 所示)，以存放受保護的資料。這個受保護的資料可以選擇以加密或者不加密的形式儲存。除了表示受保護的部分外，IPMP DIDL 並提供可用來存放相關保護資訊的元素(IPMP Information Descriptor and IPMP General Information Descriptor)。例

如：工具資訊、加密方式、License。

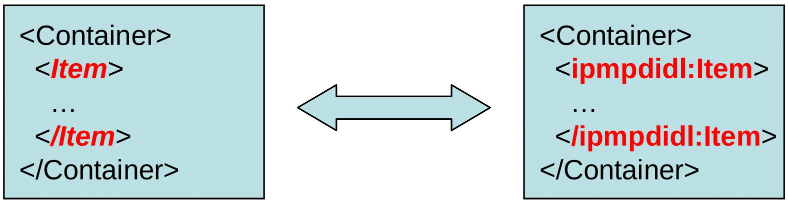


圖 2 元件可替換性

因為 IPMP DIDL 分享了大多數的 DIDL 定義，彼此的階層關係如圖 1 所示。一個 IPMP 所認可的消費者，能閱讀符合 IPMP DIDL 語法的描述子。這個語法包含了從廣義的 DID 架構與 DIDL 語法延伸而來的定義以及特定的 IPMP 定義。

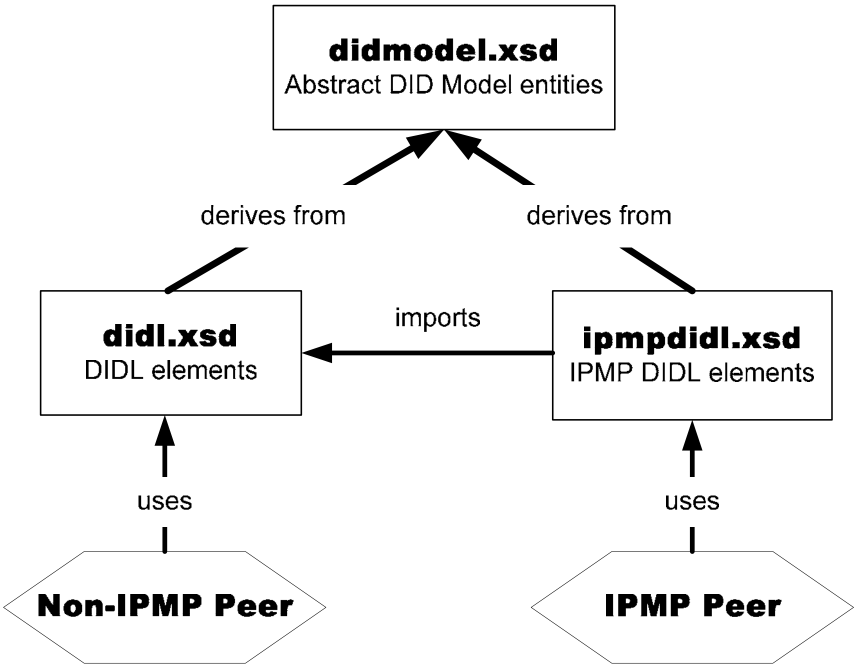


圖 1 DIDL 與 IPMP DIDL 之間的關係

MPEG-21 REL

MPEG-21 REL 是一個以 XML 為基礎的權利描述語言，定義了明確的語法以描述特定的使用者能夠在特定的條件下針對特定的資源執行被允許的行為。為滿足傳遞和保護數位內容的需求，REL 發展精確的驗證模式(Authorization Model)，可以確認記載於 License 中的使用權利是否有效。另外，為了能夠廣泛的表示各種商業模式與描述針對各式各樣的數位內容之散佈與用途，REL 具有彈性擴充的能力。

Data Model

REL 中最重要的資料模式就是 License 的架構。如圖 3 所示，一個 License 包含數個發行者(Issuer)和數個驗證內容(Grant)。發行者為簽署這份 License 的主體，可以是個

人、組織或是認證的伺服器。驗證內容代表被允許的智財權管理元件的組合，包含四個構成要素：

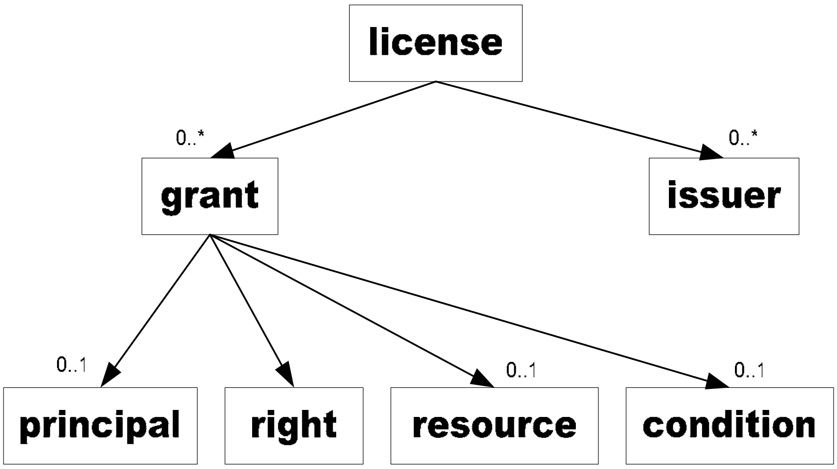


圖 3 Data model of an REL license

- 使用權利(Right)：被允許執行的行為。
- 使用者(Principal)：合法的使用對象。
- 資源(Resource)：使用權利的對象。
- 條件(Condition)：用來決定驗證內容是否為真之認證條件。

若用一句話來表示驗證內容，則為『指定的使用者在特定的條件下，被允許針對指定的資源擁有特定的使用權利』。

Authorization Model

REL 定義精確的驗證機制來決定是否允許執行權利。如圖 4 所示，用真或假來代表在驗證故事(Authorization story)的前提下，測試驗證要求(Authorization request)的驗證結果(Authorization result)。

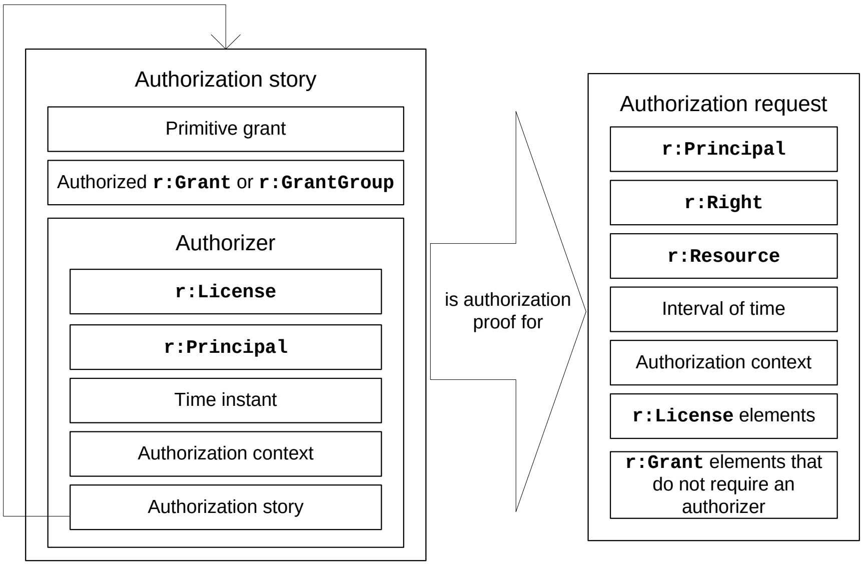


圖 4 MPEG-21 REL authorization model

驗證要求用來描述一個問題：『根據由數個已經得到的 Licenses 構成的驗證背景(Authorization context)和數個驗證內容(Grant)，是否允許使用者在特定的時間區間內，對指定的資源履行特定的使用權利？』

當收到驗證要求後，REL 的工具開始取出 Licenses 和驗證內容以建立驗證故事。每一個 License 都用來建立一個驗證器(Authorizer)，每一個驗證內容被放置在候選名單內。接著，遞迴地從驗證器產生額外的驗證內容。原生的驗證內容則由額外的驗證內容產生。以上的程序猶如反向的參照流程。結束創建所有的原生的驗證內容之後，REL 的工具開始配對使用者、使用權利、資源和條件(包含時間區間與驗證背景)。如果任何的原生的驗證內容與驗證要求相符，則回傳驗證結果為真(True);若不相符，則回傳驗證結果為假(False)。

Extensibility and Profiling

由於 REL 的語法源自於 XML 的規範[9] ，所以 REL 擁有高度彈性的擴充能力。整體的 REL 語法架構如圖 5 所示，可分為以下三類(標準延伸與多媒體延伸均從核心擴展)：

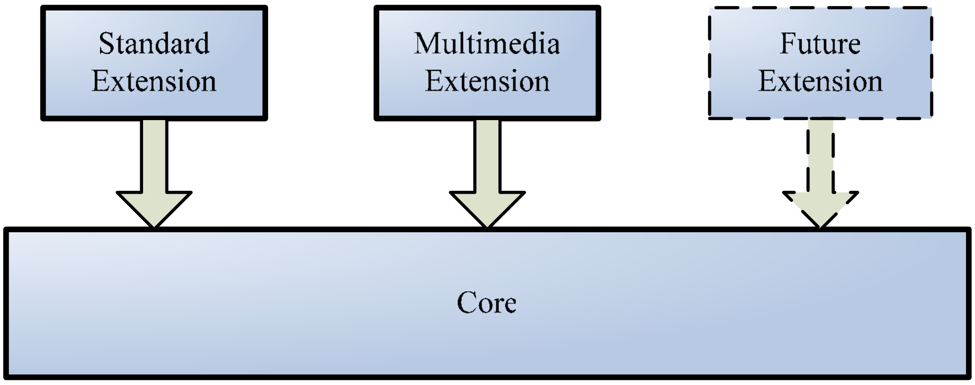


圖 5 REL Extensibility

- 核心(Core)：包含 REL 語言的架構主體之定義(特別是許可的驗證)。
- 標準延伸(Standard Extension)：包含大多數與智財權保護相關之概念與元素定義。
- 多媒體延伸(Multimedia Extension)：包含與智財權保護相關之多媒體資源的定義，例如：書本、影像、聲音等。

REL 允許但不限定使用者必須利用以上三個已定義的語法架構來描述權利。只要有需要，可以自行定義新的語法架構，唯一的限制是必須從核心語法延伸。REL 的擴充性讓各式各樣不同的應用可以與 REL 一起運作，但並非每一種應用的使用環境都需要執行 REL 的完整功能。例如：在嵌入式系統的環境中，因為系統的資源非常有限，必須量身打造每一種應用程式。往往只能採用滿足最小系統需求的智財權保護及管理系統，以有效率的利用資源。因此，透過選取需要的功能形成 REL 描述語言的子集合，以滿足特定需求，這樣的動作稱為 REL 的 Profiling。

MPEG-4 IPMPX

MPEG-4 IPMPX 在 2002 年 10 月成為標準，主要的功能是管理與保護符合 MPEG-4 格式的資料。MPEG-4 IPMPX 的系統中主要透過訊息的傳遞進行內外部的溝通。其中心架構是由一個虛擬的終端介面-Terminal(包含『工具管理員(Tool Manager)』、『訊息路由器(Message Router)』與數個『工具(IPMP Tool)』[4])來管理內部的各元件。工具或是終端介面均透過訊息和外面通訊。

一個訊息包含三個的主要基本欄位：類別(Type Field)、來源(Source Field)、目的地(Destination Field)。特別注意的是一個訊息的來源和目的地是不能相同的，也就是說不能傳遞訊息給自己。與訊息路由器互動的過程都是透過訊息介面來溝通，訊息傳遞的流程如下：

(1) 產生訊息，並且傳遞至訊息路由器。
(2) 訊息路由器傳送此訊息至正確的目的地。

工具管理員負責管理 IPMP 工具的生命週期。當 IPMP 工具被存取時，工具管理員負責安裝並初始化這個 IPMP 工具，在連結到特定的控制點(Control Point)以處理資料。使用完畢後，工具管理員則從控制點移除此 IPMP 工具，最後刪除此工具。

在 MPEG-4 系統中，存在數個可以進行額外處理資料的控制點。我們可以把控制點視為一個存放 IPMP 工具的容器，並且依序觸發工具以處理資料。對於沒有連結至任何控制點的 IPMP 工具，可以被視為系統中的一個服務。

MPEG-21 Test Bed with MPEG-4 IPMPX

MPEG-21 Test Bed 的目的是提供一個具有彈性和快速測試的環境，以驗證透過 IP 網路傳送 MPEG 內容的傳輸科技。整個系統可以分為以下三個部分：

- 伺服器端: 運用串流技術傳送數位媒體資料至客戶端。
- 客戶端：接收伺服器端傳送過來的資料，並且播放。
- 網路模擬器：模擬不同的網路條件，如：頻寬的變化、突波、封包遺失。

因為 MPEG-21 IPMP 只說明概念，我們需要一個較為完整的架構來實現這些想法。修定版本的 MPEG-21 Test Bed 將 MPEG-4 IPMPX 整合進來，在伺服器端與客戶端都有訊息路由器與工具管理員這兩件元件，因此雙方都可以擁有不同的 IPMP 工具。例如：在伺服器端擁有加密工具，相對的在客戶端有解密工具。另外，此系統上只有三個控制點：一個在 DIA 與 Streamer 之間的資料流路徑上、另外兩個分別在解碼器(Decoder)的輸入之前與輸出之後的資料流路徑上。

C. 模擬與實驗

本模擬的重點在 MPEG-21 IPMP 與 REL 的整合，系統架構參考 MPEG-4 IPMPX，並且設計符合 MPEG-21 IPMP 與 REL 功能之 IPMP Tool，最後整合至擁有 MPEG-4

IPMPX 子系統之 MPEG-21 Test Bed 平台上[10] 。

IPMP Tool Design

MPEG-21 IPMP 主要的目的為保護 Digital Item 及處理 IPMP DIDL element。另一方面，Test Bed 提供影像和聲音兩種 Digital Item。加密為其中一種有效保護資料的方式。因此，我們專注在具有加密功能的 IPMP Tool 以展現 MPEG-21 IPMP 的功能。Test Bed 採用 MPEG-4 Initial Object Descriptor (IOD)來傳輸與 IPMPX 相關的資料。所以，我們也將 IPMP DIDL element 放到相對應的 Tool Descriptor 內，並且等到初始階段時，再取出並處理 IPMP DIDL element。

MPEG-21 REL 相關之功能是產生認證的證明。根據認證的要求，相關的引擎會產生驗證故事以及驗證內容，再決定使否允許要求的事項。任何包含 REL 功能的應用都能夠控制特定的內容唯有在滿足指定條件之前提下才能被使用。

為了在 Test Bed 上實現所描述的功能，我們設計一個 IPMP 工具(稱為 IPMP_Info_Engine)。從 IPMPX 子系統的觀點而言，這個 IPMP_Info_Engine 工具擔任控制其他 IPMP 工具的中控角色。它不但是 IPMP 訊息的管理工具，還是能處理認證工作的 REL 工具。在整個系統中，IPMP_Info_Engine 工具並不直接處理任何影音資料，因此不會連結至任何的控制點。換句話說，其控制點為 CONTROL_POINT_NO (0x00)

Communication between IPMP Tools

當使用者想要播放一個影音檔案時，必須先取得相關的播放權利。在本研究提到的議題中，驗證使用者的動作如同對解密工具進行驗證。換句話說，當一個 IPMP 工具開始處理資料時，必須先聯繫 REL 工具以取得驗證的證明。解密工具(DES Tool)與 IPMP_Info_Engine 工具的互動描繪在圖 6：

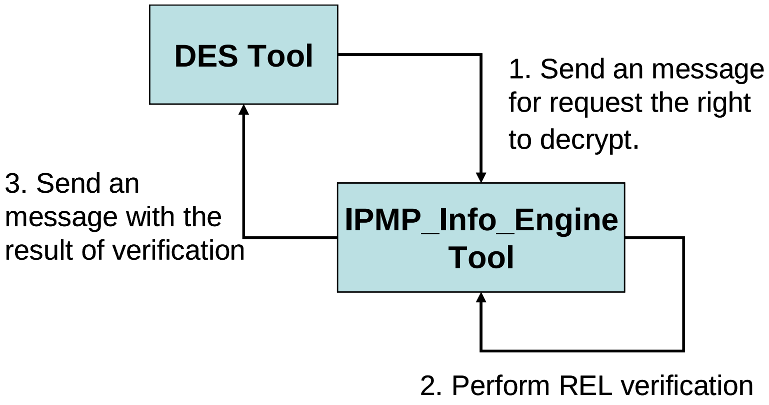

DES Tool
1. Send an message for request the right to decrypt.
3. Send an message with the result of verification
IPMP_Info_Engine Tool
2. Perform REL verification

圖 6 與 IPMP_Info_Engine Tool 之間的互動

1. DES Tool 產生要求驗證結果之訊息。
2. 訊息迴路器傳送訊息至 IPMP_Info_Engine 工具。
3. IPMP_Info_Engine 工具辨別此要求，並產生對應的驗證結果。

4. IPMP_Info_Engine 工具產生包含驗證結果的訊息。
5. 訊息迴路器傳送證明結果至 DES Tool。

根據驗證結果，DES Tool 將決定是否繼續處理資料。

Content Protection Schema

為了保護透過廣播串流的內容，本研究提出整合上述 MPEG-21 的工具。權利管理可經由辨別 license 來達成。圖 7 上展現整個保護的架構，包含雙層的加密資料。資料內容由第一層的保護機制傳輸，此處採用對稱性的 DES block Cipher 加密演算法。此處延伸出兩個議題：第一個是客戶端如何安全的接收解密金鑰以正確的還原資料、第二個是這樣簡單的 block cipher 加密演算法相較於更為複雜的演算法是比較不安全的。將解密金鑰透過一個被信任的安全通道即可解決第一個議題。第二個議題則要看整體系統設計的考量，到底要增加複雜度以獲得較高的安全性，或是降低複雜度但用較低的安全性。因此，這是複雜度與安全性的權衡。一個比較簡單的方式為利用週期性更新的金鑰，則可以在不增加系統的複雜度的前提下也可以擁有較的傳輸安全性。結合以上兩個解決方案，將傳輸模式演化為一個擁有兩層保護機制的系統設計。

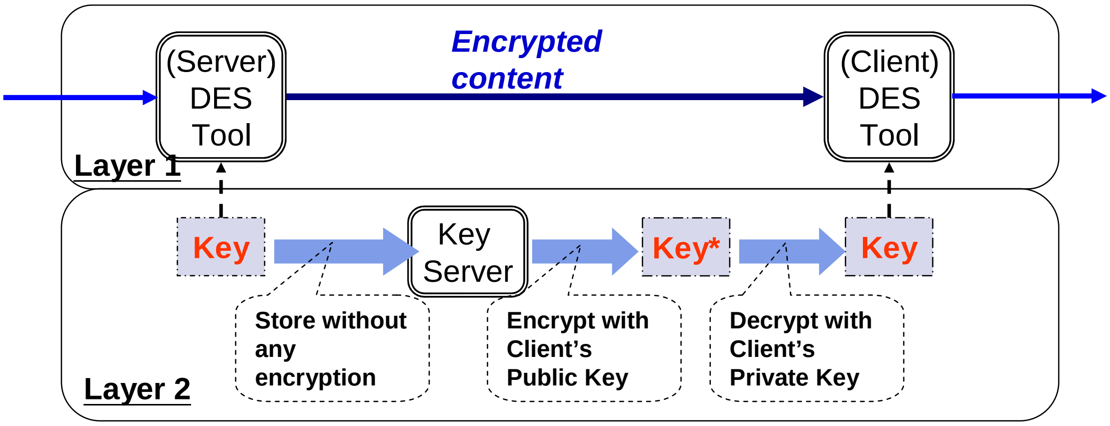

(Server) DES Tool
Encrypted content
(Client) DES Tool
Layer 1
Key
Key Server
Key*
Key
Store without any encryption
Encrypt with Client's Public Key
Decrypt with Client's Private Key
Layer 2

圖 7 Content protection scheme

第二層保護為值得信賴且安全的金鑰傳輸通道，較第一層安全的原因是第二層傳輸使用非對稱性加密演算法(RSA)保護第一層金鑰。在這裡我們架設金鑰伺服器以傳輸金鑰至客戶端，這個服務可以整合至伺服器端(Server side)或單獨成立一個遠端的服務。同時，在伺服器端的金鑰資料庫與金鑰伺服器存放的金鑰是完全相同的。客戶端與金鑰伺服器的互動流程如下：

1. 客戶端傳送包含身份資料的請求解密金鑰之訊息。
2. 金鑰伺服器搜尋資料庫以驗證使用者之身分與其他必須的條件。
3. 當請求為有效的，解密金鑰會被加密透過使用客戶的公開金鑰。
4. 金鑰伺服器把受保護的解密金鑰回傳至客戶端。
5. 客戶端則利用本身的私密金鑰取出正確的解密金鑰，再解碼以接收的資料。

使用上述的機制，可以確保受保護的資料內容只能被擁有正確身份的使用者播放。

Implementation of IPMP_Info_Engine

我們使用由 Content Guard[11] 提供的 REL 參考軟體實現 IPMP_Infor_Engine 工具。參考圖 8，利用 GUI 介面產生驗證的要求，再透過內部的 API 進行驗證。在本研究中，為了快速確認系統架構的可行性，接收端收到 REL License 會存放至本地的儲存裝置。一旦 IPMP_Info_Engine 被存取，將讀取 XML 形式的 Query(來自 request message 或已儲存的檔案)與 REL License 以產生驗證要求。其餘的步驟則與前面描述的驗證流程相同。

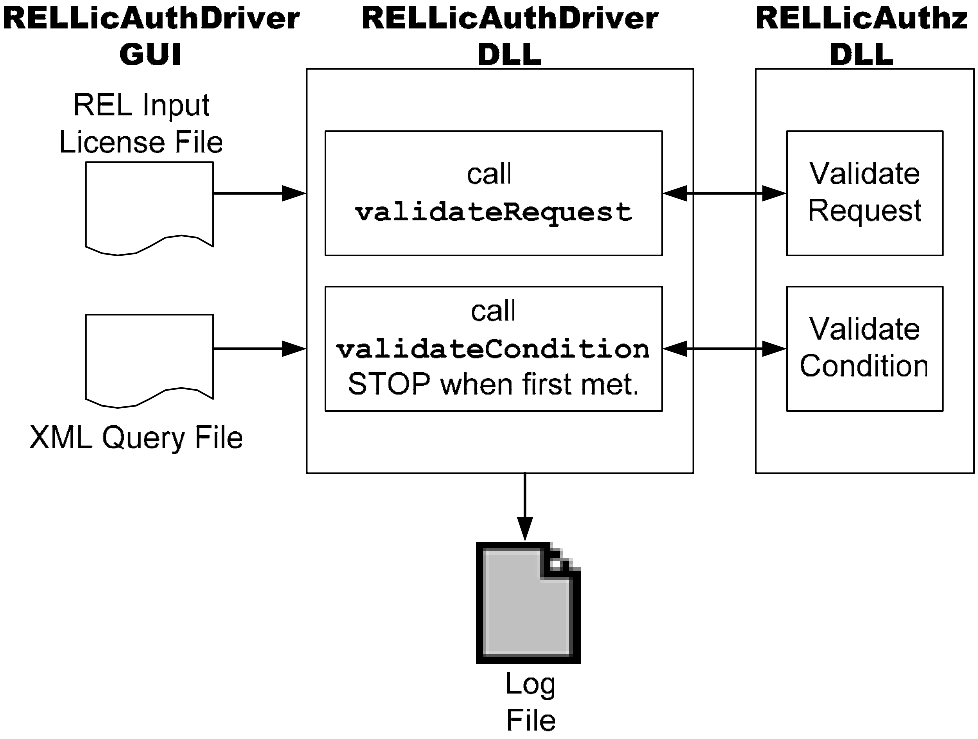


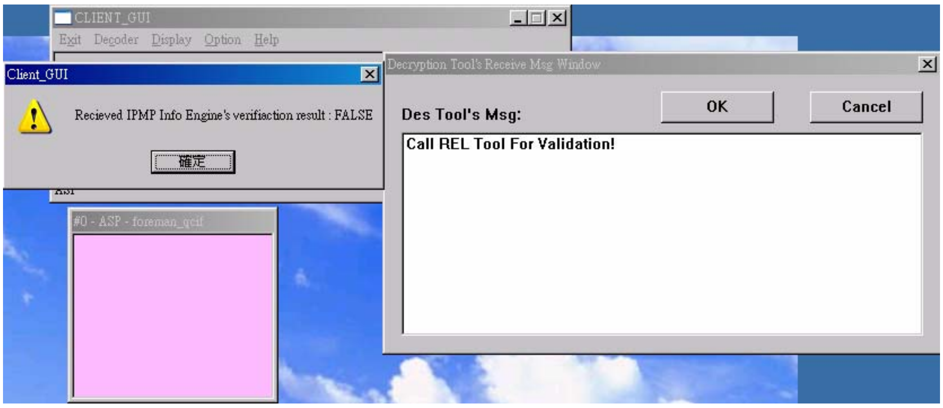
圖 8 REL 參考軟體的資料流程

Experiments

為了展示本研究中所設計的系統之特點與功能，這裡提供了三個實驗範例：(1) Online playback (2) Playback with free preview (3) Super distribution – online and offline playback

Online Playback

此範例展現如何在即時串流系統上驗證播放(play)的權利。當存取設定完成，客戶端從伺服器端接受 License。在這個基本型式的 REL License 中，主體是客戶端的身分，權利為播放，資源則是此影像檔案。比較複雜的地方是條件，我們選取”exerciseMechanism”條件(內含相關服務的參數)，讓客戶端連線到授權的遠端服務進行驗證。

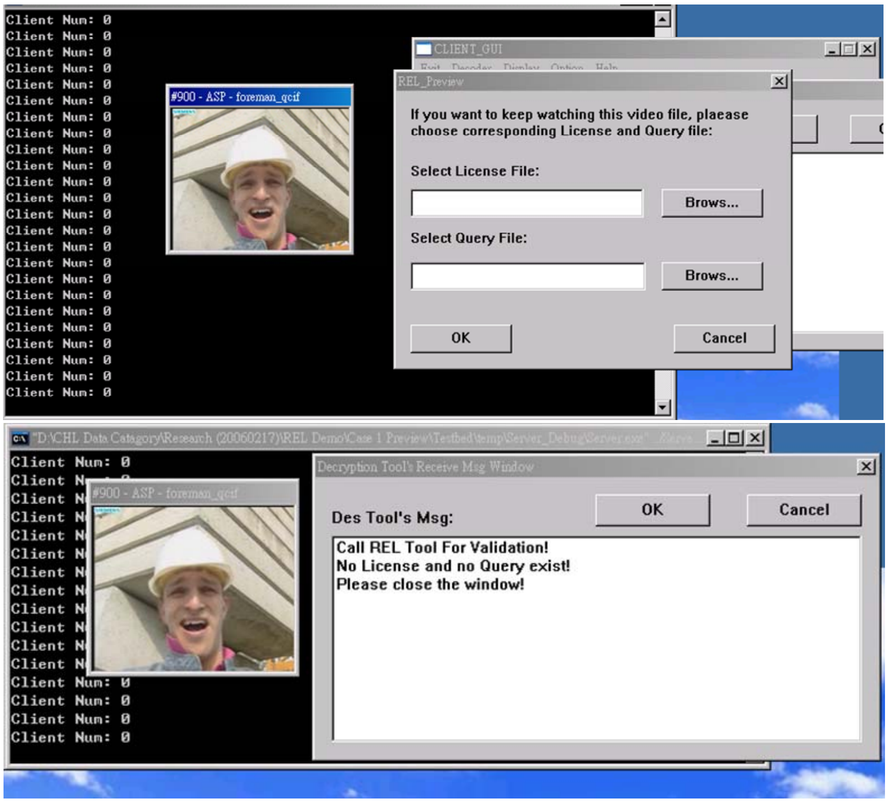

CLIENT_GUI
Exit Decoder Display Option Help
Client_GUI
確定
#0 - ASP - foreman_qcif
Decryption Tool's Receive Msg Window
OK
Cancel

Recieved IPMP Info Engine's verifiaction result : FALSE

Des Tool's Msg:

Call REL Tool For Validation!

圖 9 範例(一)之執行過程


#900 - ASP - foreman_qcif
CLIENT_GUI
REL_Preview
Brows...
Brows...
OK
Cancel
"D:\CHL Data Catagory\Research (20060217)\REL Demo\Case 1 Preview\Testbed\temp\Server_Debug\Server.exe"
#900 - ASP - foreman_qcif
Decryption Tool's Receive Msg Window
OK
Cancel

```
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
```

If you want to keep watching this video file, plaease choose corresponding License and Query file:

Select License File:

Select Query File:

```
Client Num: 0
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
```

Des Tool's Msg:

Call REL Tool For Validation!
No License and no Query exist!
Please close the window!

圖 10 範例(二)之執行過程

一旦播放開始，DES Tool 就要求 IPMP_Info_Engine 執行驗證證明的工作。IPMP_Info_Engine 根據 License 的內容來聯繫遠端伺服器並且傳送含有使用者身份資料的要求。在此系統中，此遠端伺服器不僅是驗證伺服器也是金鑰管理伺服器。如果使用者有資格播放該影像內容，遠端伺服器將會回傳受保護的解密金鑰。反之，回傳空白的解密金鑰。因為記載於 License 中的主體、權利、資源都與 REL request 相符，此驗證內容的可行性取決於條件是否吻合。如圖 9 所示，如果接收到錯誤的條件(空白金鑰) - 驗證證明為假，則 DES Tool 將拒絕繼續處理資料；反之，DES Tool 能夠運用回傳的

解密金鑰處理資料。

Preview

在典型的線上影音消費議題上，消費者常被允許可以預先觀賞部分的片段(如：影片的前 30 秒)以決定是否要購買。此範例展現運用 MPEG-21 REL 與其他 DRM 相關概念完成控制”Preview”的行為。

透過使用 DES Tool 內的計數器，我們允許使用者可以預視數秒短片不需任何的 license。計數器的內容代表剩餘可播放的 macro-block 數目，直到內容變為 0，才進行驗證證明。如圖 10 的上半部所示，IPMP_Info_Engine 將跳出對話視窗，要求使用者輸入正確的 license 與 query file。當使用者於對話視窗中輸入對應資料後，IPMP_Info_Engine 執行驗證程序。只要輸入無效的 License 或 query file，將會讓播放的程序中斷，在圖 10 的下半部展示播放過程停止的情況。

Super-Distribution

此範例展現一個在可攜式行動環境下的”Super Distribution”議題該如何進行線上與離線驗證。” Super Distribution”描述內容和使用權利的物件可以分開傳送的狀況，在現行的行動裝置上是非常實用的一個議題。內容的傳遞是以加密的方式儲存，權利物件則是指定給特定的用戶。在第一個範例中，使用者只能在網路連線存在的情況下播放影像，在離線的狀況下，完全無法播放。但對於一個行動裝置而言，不可能永遠都處於可連上網路的環境。因此，我們想要設計一種能提供線上與離線驗證的 License。

一個簡單的 License 範例顯示在圖 11，包含兩個驗證內容(Grant)。其中 Grant-1 適用連線存在的狀況，Grant-2 則適用於離線狀況。這兩個驗證內容都含有一個”allConditions”來包含一個以上以邏輯運算子”AND”連結在一起的條件元件，表示必須同時發生，此”allConditions”的條件才成立。在 Grant-1 中，”exerciseMechanism”指明

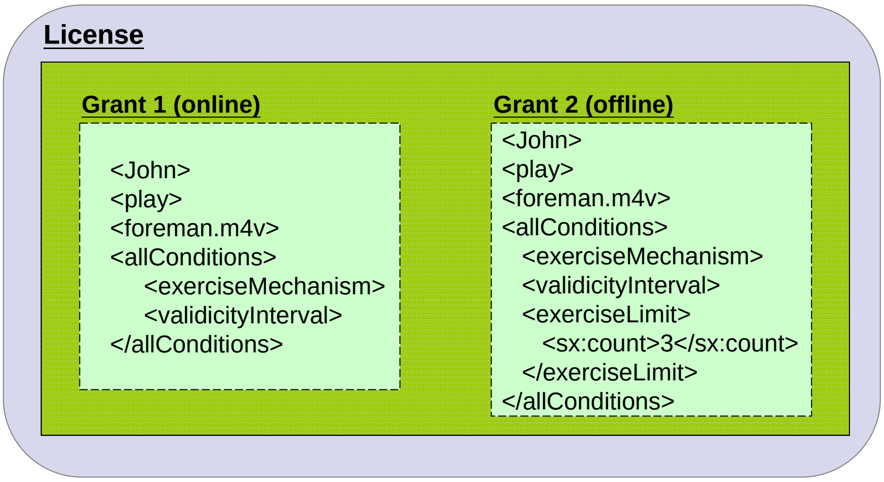


圖 11 為範例(三)所設計的 license 架構

一個遠端的伺服器，而”validicityInterval”指明有效的時間範圍。在 Grant-2 中，”exerciseMechanism”指明一個本地的驗證機制，”validicityInterval”指明有效的時間範圍，而”exerciseLimit”指明有效的離線播放次數。全部的驗證流程表現圖 12 上。

因為驗證的流程，Grant-1 的驗證順序永遠優先於 Grant-2。而且，在本範例的設計上，線上驗證的優先權必定為最高。換句話說，只要線上驗證的結果是假，則必定無法繼續播放。這個驗證的程序由不同的”validator”完成。第一個 validator 檢查網路連線，如果連線不存在，validator 回傳錯誤的條件。如果遠端伺服器回傳空的解密金鑰(代表驗證失敗)，之前得到的解密金鑰將被刪除。相反地，舊的解密金鑰將被取代。當需要驗證 Grant-2 時，第二個 validator 先確認解碼金鑰是否存在。如果不存在，則不允許播放；如果存在，檢驗播放次數。當播放次數達到所允許的數字後，驗證結果為錯誤且刪除存在的解密金鑰。兩個執行狀況的螢幕擷取圖如圖 13 所示，上面的部分是在本地驗證成功且合法播放的狀況，下面的部分則為超過可播放次數，並顯示警告訊息於視窗內。

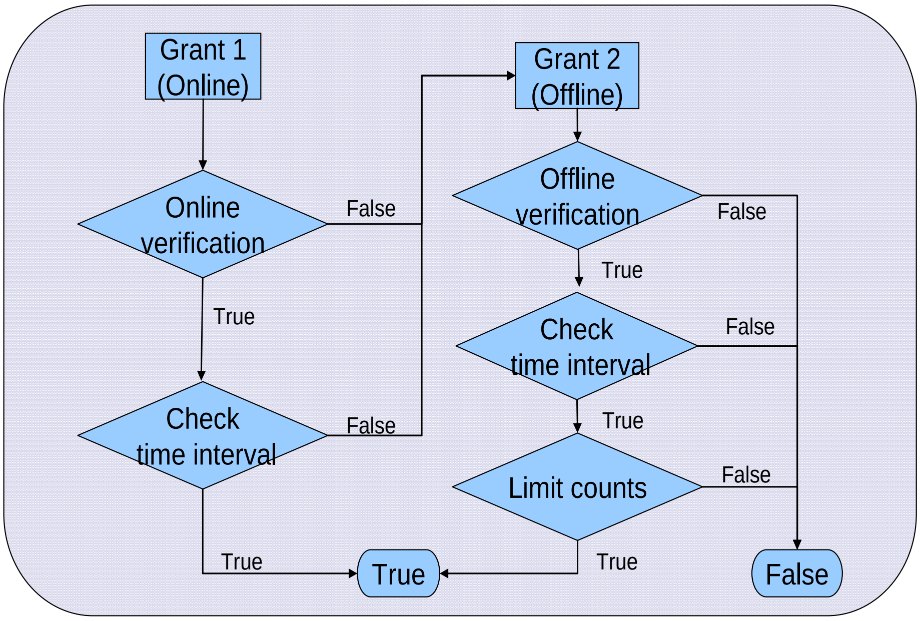


圖 12 條件驗證的流程圖

D. 結論

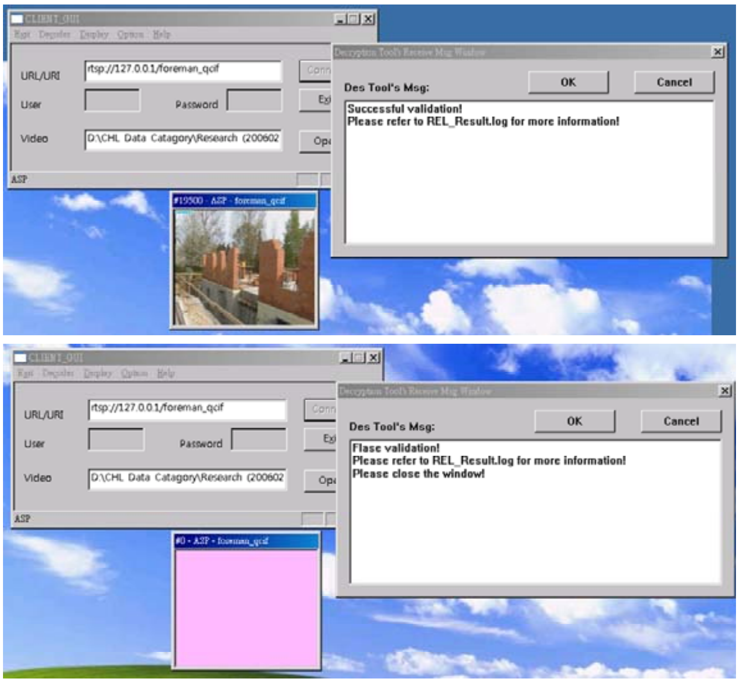
智財權保護與管理在許多多媒體應用中是相當重要的元件，因此本研究的目的是創建可以提供內容保護與權利管理的 DRM 系統。

本研究使用 MPEG-21 IPMP、MPEG-21 REL 和 MPEG-21 Test Bed with MPEG-4 IPMPX 之觀念與工具來創建我們的系統。MPEG-21 IPMP 定義高層次的 Digital Item 保護機制。MPEG-21 REL 能夠描述廣泛的使用權利，亦提供清晰的權利認證與控管機制。因為，MPEG-21 IPMP 與 REL 僅提供概念上的定義，我們選用 MPEG-21 Test Bed 作為實現的平台。在 Test Bed 上包含了修改的 IPMPX 系統(採用 MPEG-4 IPMPX 定義的介面)。

在所設計的系統中，我們還設計一個雙層的內容保護機制當傳輸與解碼多媒體內容的情形下。為了實現這個架構，修改 IOD 使得 Tool Descriptor 可以包含 License。接著我們整合 MPEG-21 REL 的參考軟體成為一個 IPMP 工具(IPMP_Info_Engine)。另外，

我們修改 DES Tool 使其能與 IPMP_Info_Engine 溝通，並取得驗證結果與解密金鑰。

最後，利用三個範例展現我們的 DRM 系統能提供不同的服務。範例(一)展示在串流應用的環境下使用即時的權利認證和內容保護的能力。範例(二)表現如何設計和使用 license 讓使用者預視影像短片。範例(三)則展現一個比較複雜的 Super Distribution 範例。我們設計一個 license 能夠提供線上與離線的驗證。


CLIENT_GUI
Exit Decoder Display Option Help
URL/URI
User
Password
Video
Conn
Exi
Ope
ASP
#19500 - ASP - foreman_qcif
Decryption Tool's Receive Msg Window
Des Tool's Msg:
OK
Cancel
#0 - ASP - foreman_qcif

URL/URI: rtsp://127.0.0.1/foreman_qcif

Video: D:\CHL Data Catagory\Research (200602

Successful validation!
Please refer to REL_Result.log for more information!

Flase validation!
Please refer to REL_Result.log for more information!
Please close the window!

圖 13 範例(三)之執行過程

第二部份 輪廓轉換(Contourlet)

A. 前言

空間轉換(spatial transform)在影像和圖片的壓縮中扮演著很重要的角色，通常自然界的影像在經過空間轉換到頻域(frequency domain)之後，大部分的能量都集中在低頻上，如果把經過轉換的資料再搭配有效率的熵編碼(entropy coding)的話，就可以提升壓縮的效率。一般常用的空間轉換方法為 FFT 和 DCT，近年來由於可調整性(scalability)的需求越來越熱門，可達成此一需求的空間轉換方式，如小波轉換(wavelet transform)的研究也越來越熱門。但是小波轉換對二維訊號的表示法卻不是很理想，因為它忽略了二維方向的連續性，故後來有研究者提出了方向性濾波器頻帶(directional filter bank)的轉換，如曲線轉換（curvelet transform）和輪廓轉換(contourlet transform)，本研究計畫主要在探討廓轉換的特性，實現輪廓轉換，並進而研究其在壓縮方面之可行性。

B. 研究目的

小波轉換的優點在於能有效的表示點和點之間的變化，也因此小波轉換在對一維的訊號的壓縮率有不錯的效果。但在處理二維的訊號時，小波轉換會把二維分成兩個一維的訊號來處理，故會忽略二維的連續性，也就是曲線的連續性還是用點來表示，也因此降低了壓縮效果。在幾年前 Candes 和 Donoho[12] 發表了新的空間分析方法，此方法叫做曲線轉換（curvelet transform），藉著這個方法來趨近二維曲線的函數。藉著曲線轉換的激發，Minh N. Do[13] 提出了輪廓轉換(contourlet transform)來建立新的圖片壓縮方法。

我們的研究會把 Minh N. Do 的輪廓轉換實現出來，然後觀察個次頻帶(subband)的輸出結果，看看是否在特定的方向上會有很有效率的表示方式，也就是會考慮到二維方向上的連續性。

C. 文獻探討

Minh N. Do 所提出的輪廓轉換綜合了曲線轉換和次頻域分解的優點的優點。主要可以分成(1)全區域的多重解析度轉換分析和(2)局部區域的方向性分析。第一個步驟的目的是為了邊界偵測並且同時把類似小波轉換的方法應用到影像分析，主要是利用 Burt 和 Adelson[14] 提出的拉氏金字塔(Laplacian pyramid)分解來實現。第二個步驟的目的是利用局部區塊方向性轉換來處理物件輪廓的區塊，主要是利用 Phoong[15] 等人所提出的扇形濾波器(fan filter)的設計方法來實現。下面分別簡述這兩個參考文獻。

拉氏金字塔分解可以達到多重解析度的分解，此分解過程可以使圖片分成高頻和低頻成分，低頻部分圖片由原始圖片產生，並且同時執行下取樣，至於經過反向預測的低頻圖片和原始圖片的差異部分就形成高頻成分圖片。高頻部分不會作向下取樣(down sampling)以避免高頻的訊號會因為向下取樣而變成低頻訊號，也就是產生頻率

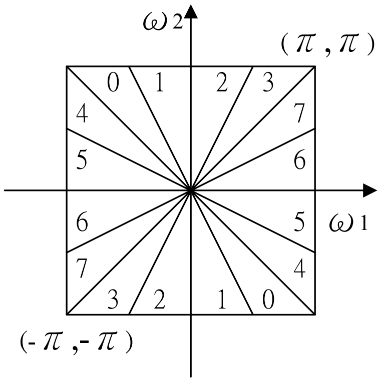


圖 14 二維方向性濾波頻帶對頻譜的分解示意圖

混合(frequency scrambling)的問題。

二維方向性濾波頻帶基本上會把頻譜分解成像風扇的樣子如圖 14 所示，這是一個 8 個方向的方向性濾波頻帶的示意圖，每一個分解區域會對應到一個次頻帶，在實現的過程中我們會使用樹狀架構，頻帶分解的個數是依照此樹狀架構的層數來決定。

D. 研究方法

D.1. 全區域的多重解析度轉換分析

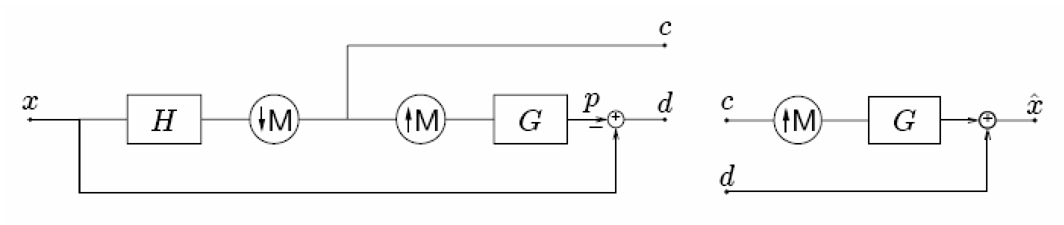


圖 15 拉式金字塔的分析端和合成端

圖 15 表示的是拉式金字塔的分析端(analysis)和合成端(synthesis)，其中 *x* 是輸入的圖片，$\hat{x}$ 為合成的圖片，*c* 是低頻訊號而 *d* 是高頻訊號，因為高頻訊號不作向下取樣的緣故，故全部的訊號量是經過小波轉換的後的訊號量的 $\frac{4}{3}$ 倍。其中的 *G* 和 *H* 使用的是 H 和 G 是使用 Daubechies 9/7 濾波器[16] 。

D.2. 局部區域的方向性分析

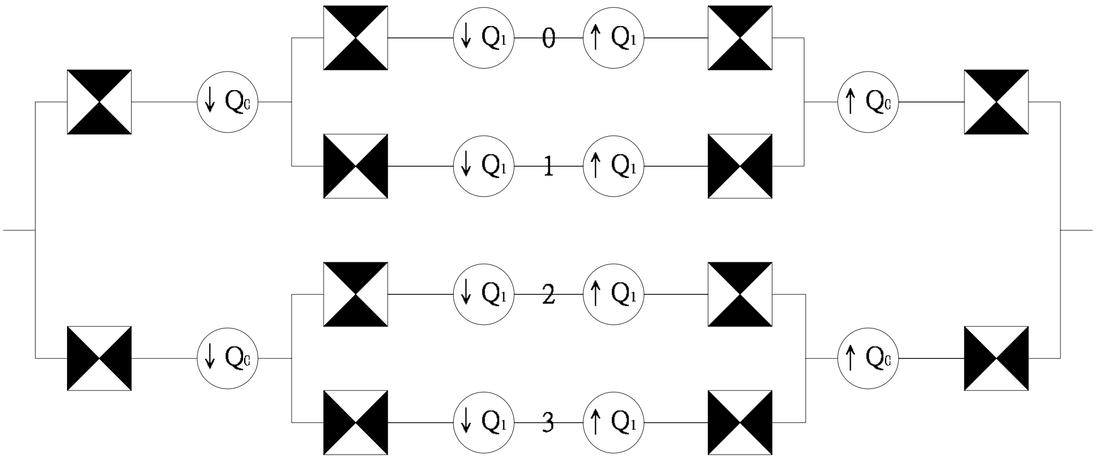


圖 16 4 個方向的 2 維方向性濾波頻帶

二維方向性濾波頻帶主要是由扇形濾波器和 quincinx 次取樣所組成，在我們實際現實時，扇形濾波器利用 Phoong 所提出的方法[15] ，再做頻域調變；quincinx 次取樣主要是參考[17] 。圖 16 為 4 個方向的 2 維方向性濾波頻帶的架構圖而圖 17 是相對應的頻譜。

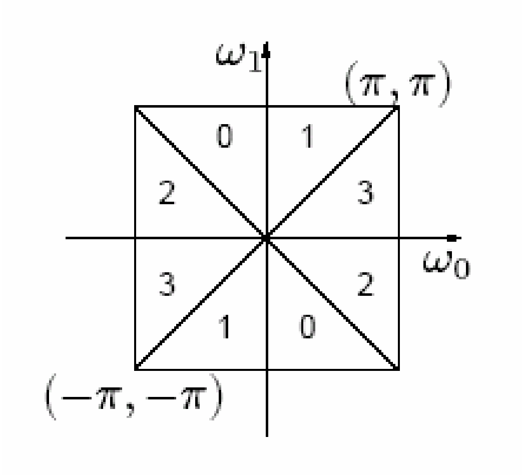


圖 18 經過 4 個方向的 2 維方向性濾波頻帶所分解得到的頻譜

E. 結果與討論

我們把先把影像經過兩次拉式金字塔的拆解，然後把最高頻的部分作 8 個方向的 2 維方向性濾波頻帶拆解，中間的頻率部分則是作 4 個方向的 2 維方向性濾波頻帶拆解，最低頻的部分不作方向性的拆解，整個拆解的架構如圖 19 左半部所示，而在頻域的分解則如圖 19 右半部所表示。

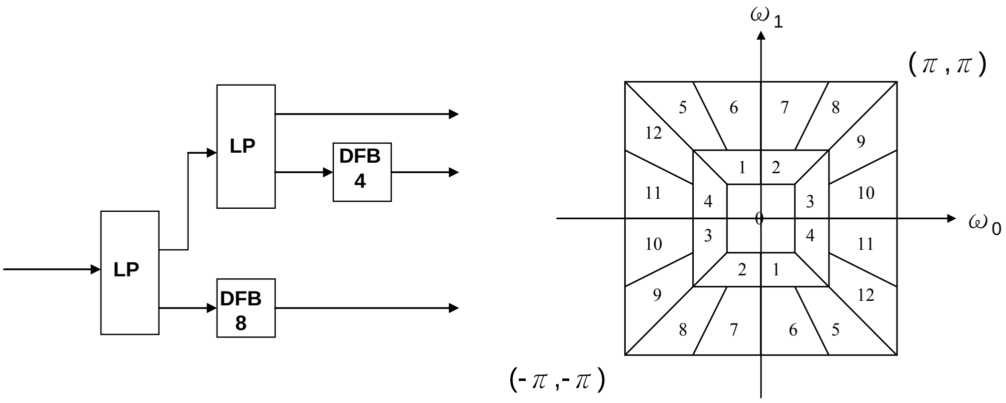


圖 19 用來作輪廓轉換的架構和所對應的頻域的分解

圖 20 是把一張圖片用圖 19 的架構拆解後的結果，我們可以發現經過拆解後的次頻帶，在相對應的方向上會有比較強的訊號出現。也就是說只要影像的邊緣(edge)和某個頻帶一致性越大，在那個方向上就會有越強的訊號出現，顯示影像連續線條可以集中在一個頻帶中，因此可以獲得較佳的壓縮效果。目前正在設計壓縮程序，希望近期內會有具體成果。

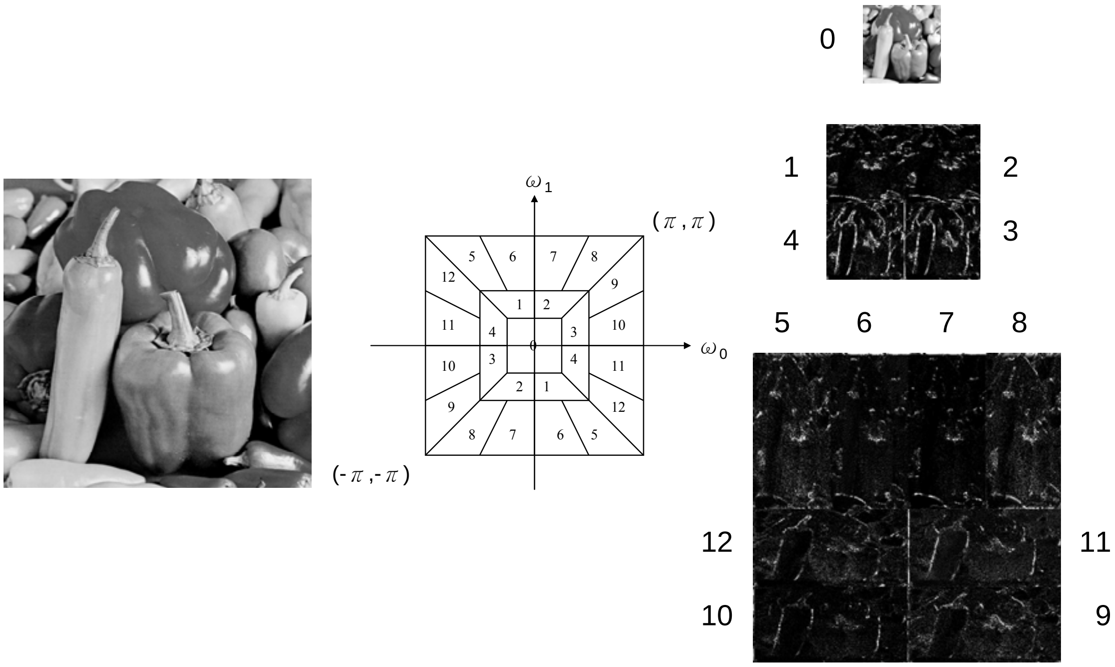


圖 20 經過拉式金字塔和 2 維方向性濾波頻帶後拆解的圖片

參考文獻

[1] J. Bormans and K. Hill, “MPEG-21 Overview v.5,” ISO/IEC JTC 1/SC 29/WG 11/N5231, Shanghai, October 2002.

[2] Study of ISO/IEC 21000-4 FCD－IPMP Components, ISO/IEC JTC 1/SC 29/WG 11/N7426 July 2005, Poznan, Poland.

[3] Information Technology－Multimedia Framework (MPEG-21)-Part 5: Rights Expression Language, ISO/IEC 21000-5:2004, May 2004.

[4] C.A. Schultz, “Study of FPDAM ISO/IEC 14496-1:2001/ADM3,” ISO/IEC JTC 1/SC 29/WG11 N4849, Klagenfurt, July 2002.

[5] C.J. Tsai, M. van der Shaar and Y.K. Lim, “Working Draft 3.0 of ISO/IEC TR2100-12 Multimedia Test Bed for Resource Delivery,” ISO/IEC JTC1/SC29/WG11 MPEG2003/M10299, Hawaii, December 2003.

[6] Information Technology－Multimedia Framework (MPEG-21)-Part 12: Test Bed for MPEG-21 Resource Delivery, ISO/IEC 21000-12:2005, Apr. 2005.

[7] C.N. Wang, et al., “FGS-Based Video Streaming Test Bed for MPEG-21 Universal Multimedia Access with Digital Item Adaptation,” ISO/IEC JTC1/SC29/WG11 MPEG2003/M8887, October 2002.

[8] Information Technology－Multimedia Framework (MPEG-21)-Part 2: Digital Item Declaration, ISO/IEC 21000-2:2003, Mar. 2003.

[9] W3C (2001) XML Schema, http://www.w3.org/TR/2001//REC-xmlschema-1-20010502/

[10] C.-W. Fan, "MPEG-4 IPMPX Design and Implementation on MPEG-21 Test Bed," M.S. thesis, Dept. Electrical Engineering, National Chiao Tung University, Hsinchu, Taiwan, R.O.C., June 2004.

[11] X. Wang, et al., "An Example Implementation of MPEG-21 REL Reference Software," ISO/IEC JTC1/SC29/WG11 MPEG2003/M9581, March 2003.

[12] E. J. Cand`es. "Ridgelets: Theory and Applications", Ph.D. Thesis, Department of Statistics, Stanford University, 1998.

[13] M. N. Do, *Directional Multiresolution Image Representations*, Ph.D. Thesis, Department of Communication Systems, Swiss Federal Institute of Technology Lausanne, November 2001.

[14] P. J. Burt and E. H. Adelson. "The Laplacian pyramid as a compact image code", IEEE Transactions on Communications, vol. 31:4, pp 532–540, April 1983.

[15] S.-M. Phoong, C. W. Kim, P. P. Vaidyanathan, and R. Ansari. "A new class of two-channel biorthogonal filter banks and wavelet bases", IEEE Transactions on Signal Processing, vol. 43:3, pp 649–665, Mar. 1995.

[16] A. Cohen, I. Daubechies, and J.-C. Feauveau. "Biorthogonal bases of compactly supported wavelets". Commun. on Pure and Appl. Math., vol.45, pp 485–560, 1992.

[17] M. Vetterli. "Multidimensional subband coding: Some theory and algorithms", Signal Processing, vol. 6:2, pp 97–112, Feb. 1984.

計畫成果自評

本計畫有以下幾類成果。第一類為MPEG-21 IPMP/REL System與Contourlet所發展出的技術、經驗及成品與國際 MPEG 標準直接相關，極具實用價值，可促進國內工業研發技術開發。第二類為將上述技術提案至 MPEG 標準組織，有助我國技術之進入國際舞台。第三類為計畫執行過程所獲得之研究成果論文四篇，已發表於國內外學術會議。其四，參與計畫之同學可獲得國際多媒體最先進的MPEG-4與MPEG-21相關技術及多媒體系統設計經驗，畢業後進入產業，直接有助於產業界開發新產品，提昇我國工業技術能力。達到人才培育之目的。

綜合評估：本計畫產出相當多具有學術與應用價值的成果，特別是直接參與國際標準會議，在國際上展示成果。並培育高科技人才培育，整體成效可稱良好。已發表(含接受)學術論文五篇，博士學位論文一冊，以及碩士學位論文二冊如下表。

Publications

(1) F.-C. Chang and H.-M. Hang, “A relevance feedback image retrieval scheme using multi-instance and pseudo image concepts,” *IEICE Transsactions on Information and Systems*, pp.1720-1731, May 2006. (SCI, EI) [NSC 91-2219-E-009-041]

(2) F.-C. Chang, H.-C. Huang and H.-M. Hang, “Layered access control schemes on watermarked scalable media,” *J. VLSI Signal Proc Systems for Signal, Image, and Video Technology*, to be published. (SCI, EI) [NSC 92-2219-E-009-008]

(3) C.-H. Lu, F.-C. Chang, and H.-M. Hang, “Design and Implementation of MPEG-21 IPMP and REL on MPEG-21 Testbed using IPMPX Framework”, in *2006 Conf. on Computer Vision, Graphics, and Image Processing*, Tao-yuan, Taiwan, Aug. 2006.

(4) C.-H. Lu, F.-C. Chang, and H.-M. Hang, “A Content Protection Scheme Using MPEG-21 Concepts and Tool,” in *Europe-China Conference on Intellectual Property in Digital Media (IPDM)*, Shanghai, Oct. 2006.

(5) Y.-T. Shih, F.-C. Chang, and H.-M. Hang, “A Digital Content Protection Scheme Using MPEG-21 REL with Applications to DVB systems,” in *2006 IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP-2006)*, Pasadena, Dec. 2006.

(6) Feng-Cheng Chang 張峰誠, *Digital Image Retrieval and Scalable Media Protection*, Ph.D. Dissertation, NCTU, May 2006

(7) Ying-Tzu Shih 施瑛姿, *A Digital Content Protection Scheme Using MPEG-21 REL with Applications to DVB Systems*, MS Thesis, NCTU, November 2005.

(8) Chia-Hsien Lu 呂家賢, *An Implementation of MPEG-21 IPMP and REL with MPEG-4 IPMPX Framework on MPEG-21 Testbed*, MS Thesis, NCTU, June 2006.

DESIGN AND IMPLEMENTATION OF MPEG-21 IPMP AND REL ON MPEG-21 TESTBED USING IPMPX FRAMEWORK

Chia-Hsien Lu (*呂家賢*), *Feng-Cheng Chang* (*張峰誠*), *and Hsueh-Ming Hang* (*杭學鳴*)

Dept. of Electronics Engineering, National Chiao Tung University

chl0113.ee93g@nctu.edu.tw, breeze@alumni.nctu.edu.tw, hmhamg@mail.nctu.edu.tw

ABSTRACT

Due to the fast advances in consumer electronics and broadband networks, people nowadays can easily create and distribute digital contents. How to effectively manage and protect the rights of consuming digital contents becomes an important issue. In this paper, the technologies of MPEG-21 IPMP (Intellectual Property Management and Protection) and REL (Rights Expression Language) are adopted to construct a DRM system. The MPEG-4 IPMPX (Intellectual Property Management and Protection Extension) system is also used as the basic framework in our implementation. The MPEG-21 IPMP provides ways to protect a digital element. The MPEG-21 REL is able to describe various kinds of rights and it provides an authorization model to generate an authorization proof to manage the rights. To implement these standard specifications, we design a set of IPMP Tools, which carry the functionalities of the MPEG-21 IPMP and REL. We then integrate this set of tools into the MPEG-4 IPMPX framework on the MPEG-21 Test Bed. At the end, we develop three application examples to demonstrate that our system can successfully safeguard digital resources and effectively manage the rights.

1. INTRODUCTION

As the network and digital media technologies advance, it is easy nowadays for everyone to create and distribute digital multimedia contents. The intellectual property protection and management becomes an important issue. Therefore, modern multimedia system designs often include digital rights management (DRM) as an essential component.

To protect digital contents from eavesdropping, encryption is an important tool. Thus, most of the popular DRM systems incorporate the encryption functionality. However, encryption alone is not sufficient to provide a more sophisticated service such as a right that authorizes to the users to consume the resource under specific conditions or constraints. A complete DRM system requires a means to describe who owns a piece of content and how it can be used. This can be achieved by incorporating a rights expression language. Generally speaking, a rights expression language is able to describe the rights holder of a certain resource, the target consumer of the resource, the allowed rights on the resource, and the necessary conditions for resource consumption. There are a few rights expression languages defined for various application fields. One of them is defined by the MPEG committee for the use in connection with the MPEG-21 multimedia framework.

MPEG-21 [1] is a set of specifications defined as "*a multimedia framework to enable transparent and augmented use of multimedia resources across a wide range of networks and devices used by different communities.*[1]" There are two parts in MPEG-21 that constitute the basis of a DRM system. The MPEG-21 Part 4 [2] defines the high level concepts and schema for Intellectual Property Management and Protection (IPMP); and the MPEG-21 Part 5 [3] defines the Rights Expression Language (REL).

The MPEG-21 REL is an XML-based language that can declare an authorized distribution for the use of any content, resource, or service owned by specific users. It provides flexible, exact, and rich representation of rights. It can be used in various applications due to the interoperability of this language. According to a specific application, users who use REL for rights management can define their own extensions as well as create a specific profile. The other parts of MPEG-21 are also related to specific aspects of a DRM system.

In this paper, we study and implement the MPEG-21 IPMP and REL specifications. By analyzing several typical multimedia DRM scenarios, we design a DRM scheme to protect the digital assets and to perform the rights management. Its functionality is compliant to the MPEG-21 IPMP and REL concepts. Because the specifications in MPEG-21 IPMP are abstract, we map its DRM functionality to the MPEG-4 IPMP Extension (IPMPX) [4] architecture. To verify the feasibility of our design, we choose the MPEG-21 Test Bed [5][6][7] as the content delivery platform. In addition to the ability of simulating a basic real-time content delivery system, it also has a simple implementation of the IPMPX architecture inside. Hence, we implement our DRM by integrating the MPEG-21 IPMP, the MPEG-21 REL, together with IPMPX on the Test Bed.

This paper is organized as follows. We first introduce the concepts and specifications of the MPEG-21 IPMP in Sec. 2. Second, the REL concepts and specifications are discussed in Sec. 3. Then, Sec. 4 gives a brief overview of the MPEG-21 Test Bed with IPMPX. In Sec. 5, we describe the details of our design and implementation of the MEPG-21 IPMP and REL within the MPEG-4 IPMPX framework on the MPEG-21 Test Bed. Finally, we design three application examples to demonstrate the functionalities of our designed DRM system. A few conclusion remarks of our work are given in Sec. 7.

2. MPEG-21 IPMP

The goal of the MPEG-21 IPMP is to provide the management of rights and intellectual property through the use of protected Digital Items. A Digital Item (DI) is the subject that the MPEG-21 technology applies to. It can be a multimedia clip, a document, or even a service which provides sort of "digital content". To describe the properties of a DI, the MPEG-21 developed the Digital Item Declaration Language (DIDL), which is an XML-based expression defined in the MPEG-21 Digital Item Description (DID) specifications [8].

A DID is a plain-text description format of a DI. However, in many multimedia protection schemes, not only the content itself but also the meta-data of the content should be protected against unauthorized access. Therefore, an additional secure representation of DI is developed. A protected representation of DID Model Structure is proposed as IPMP DIDL.

Both representations (in DIDL and in IPMP DIDL) are semantically equivalent. They refer to the identical digital item by different syntax. For every DIDL element, there is an interchangeable IPMP DIDL element which carries valuable content (as shown in Fig. 1). The carried content can be encapsulated in either the unprotected or the protected form. For a protected element, the additional side information is required in order to recover it to its original (unprotected) form. In the specifications, the IPMP Information Descriptor and IPMP General Information Descriptor are defined for representing the necessary side information including tools, mechanisms, and licenses.

Since the IPMP DIDL shares a vast amount of definitions with the DIDL, the hierarchical relationships are illustrated in Fig. 2. For an IPMP capable consumer, it reads in the description using the IPMP DIDL schema. This schema consists of the definitions derived from the generic DID model, the definitions from the DIDL schema, and its own IPMP specific definitions.

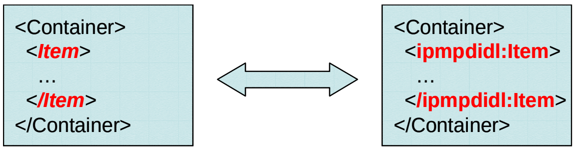


Fig. 1 Element interchangeability.

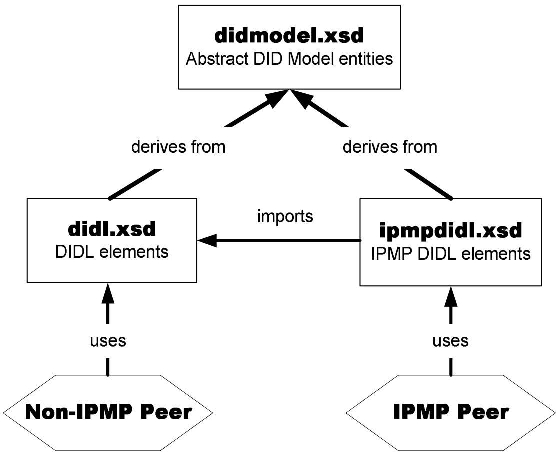


Fig. 2 Relationship between DID and IPMP DID.

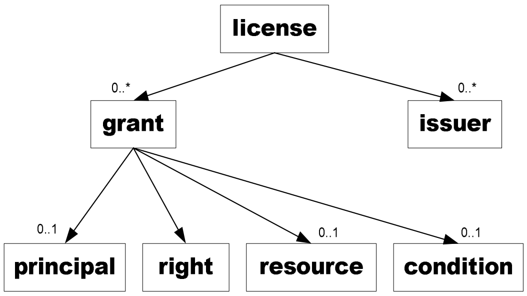


Fig. 3 Data model of an REL license.

3. MPEG-21 REL

The MPEG-21 REL is an XML-based and machine-interpretable rights expression language that declares an authorized distribution for the use of any content, resource, or service owned by specific users. It defines an unambiguous syntax to specify rights.

To fulfill the demand of distribution and protection of digital contents, it is essential that the language provides an authorization model for checking whether the rights specified in the license is validate. To be able express a wide variety of business models and to enable multimedia distribution and usage of all types of digital resources, the MPEG-21 REL is designed to be extensible and flexible.

3.1. Data Model

The most important data model in the MPEG-21 REL is the license structure. As shown in Fig. 3, a license may contain any number of issuers and grants. An issuer is a subject who issues the license. It could be a person, an organization, or a license service. A grant represents a permitted combination of the digital rights management entities.

A grant is constructed by four components. The only mandatory component is the Right, which specifies the allowed action. The Principal component specifies the target to which the license is issued. The Resource component specifies the target which the action is applied to. The Condition component specifies the criterion for deciding the validity of the grant.

In a syntactical expression, the Principal is the subject; the Right is the verb; the Resource is the object; and the Condition is the terms, conditions, and obligations under which the right can be exercised. Hence, a grant is equivalent to the sentence: "under the Condition, the Principal is allowed to exercise the Right on the Resource."

3.2. Authorization Model

To determine the permission of exercising a certain right, an authorization model is defined in the MPEG-21 REL. As shown in Fig. 4, an authorization proof is the binary result (true or false) of testing the authorization request against the authorization story.

An authorization request is composed of several items. They form a structure to express the question: "is it permitted for the *principal* to perform the *right* upon the *resource* during the *time interval*, according to the *authorization context*, the set of obtained *licenses*, and the set of trusted *grants*?" The authorization context is used to hold additional properties of the request, to be matched with the conditions of the grants.

Upon receiving the request, the REL tool extracts the licenses and grants to construct an authorization story. Each license is used to construct an authorizer (which may contain a story), and the extracted grants are put into the pool of authorized grants. Then, additional authorized grants are derived from the authorizer, recursively. The primitive grants are derived from the authorized grants. The process is equivalent to a de-reference procedure. After all the primitive grants are resolved, the tool starts to match the principal, right, resource, and condition (both the time interval and the context). If the request matches any of the primitive grants, the result is true. Otherwise, the proof is failed.

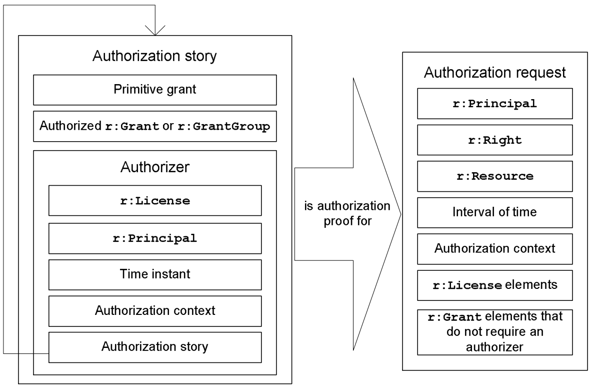


Fig. 4 MPEG-21 REL authorization model.

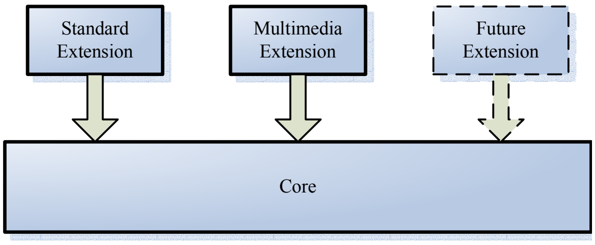


Fig. 5 REL Extensibility.

3.3. Extensibility and Profiling

Because the syntax of the REL are described using the XML Schema [9], the MPEG-21 REL can offer a high degree of flexibility in its extensibility. The schema can be organized into three categories: core, standard extension, and multimedia extension (Fig. 5).

The core schema defines the general concepts that form the basic architecture of the language, particularly the ones strongly related to a trust evaluation. The standard extension schema defines the concepts that are generally and broadly useful and applicable to DRM scenarios. The multimedia extension schema defines the DRM concepts specifically related to the multimedia content such as books, video, and audio. Both the standard and the multimedia extensions are extended from the core schema. The REL allows, but not limited, to express rights using the defined schemas. Future applications may extend the core schema to define new expression elements.

The extensibility enables the REL to cooperate with a wide range of applications. However, not all applications require the full support of REL. Especially for an embedded application, the limited resource of the device would restrict the DRM functionality to a subset of the REL elements. The profiling process of the REL is to select a set of items for a specific purpose. This process produces a subset of the language, and the REL peers are able to determine whether they are interoperable or not.

4. MPEG-21 TESTBED

The MPEG-21 Test Bed is chosen as our implementation platform. We briefly describe the structure of the Test Bed and the existing MPEG-4 IPMPX on it in this section.

4.1. MPEG-4 IPMPX

The MPEG-4 IPMPX system became an ISO standard in October 2002. It provides the functionality to protect and manage the MPEG-4 contents. The MPEG-4 IPMPX system is message-based. The concept of an IPMPX system is a Virtual Terminal that contains a Tool Manager (TM), a Message Router (MR) [4], and several other IPMP Tools. A Tool or the terminal may generate or receive messages to communicate with the others. A message has three basic fields. The type field denotes the type of the message; the source field denotes the component which sends the message; and the destination field denotes the recipient of the message.

To send a message, the originator passes the message to the Message Router. Then, the MR transports the message to the destination component. The interaction to and from the MR are through the message interface. The Tool Manager manages the lifecycle of an IPMP Tool. When a tool is accessed, the TM is responsible for the instantiation, initialization, and connection to the specified control point. After the use of a Tool, the TM disconnects, uninitializes, and destructs it.

In an MPEG-4 elementary stream data path, there exist several *control points*. A control point is a virtual container in which the triggered IPMP Tools process the content one after another. For the tools that do not associate with a control point, they act like a service in the system. We will describe a design of REL service in Sec. 5.

4.2. MPEG-21 Test Bed with IPMPX

The purpose of the MPEG-21 Test Bed is to provide a flexible and fair test environment for evaluating delivery technologies for MPEG contents over IP network. The entire system is divided into three parts: server, client, and network. The server is to deliver digital media content with streaming technology to the Clients. The Client receives the media data from the server through the Network Interface and playbacks the media content such as video, audio, or both. The network emulator provides a real-time emulation of various network conditions, such as bandwidth variation, jitter, and packet loss.

Since the MPEG-21 IPMP specifies only the abstract concepts, a concrete architecture is required to realize those concepts. In the Test Bed, a modified version of the MPEG-4 IPMPX is integrated. Based on the MPEG-4 IPMPX specifications, it has components such as Message Router, Tool Manager, and IPMP Tools. Because of the client-server architecture of the Test Bed, the MR and TM exist in both sides. Thus, certain IPMP Tools are implemented in two counterparts. For example, an encryption tool at the server side corresponds to a decryption tool at the client side. The modified IPMPX version on the Test Bed has only three control points. One resides between the DIA and the streamer (PostDIAFilter); and two reside at the input and the output data path of the decoder (PreDecoderFilter and PostDecoderFilter).

5. SYSTEM DESIGN AND IMPLEMENTATION

In this section, we describe the implementation of the MPEG-21 IPMP and REL on the MPEG-21 Test Bed. We design and modify IPMP Tools to provide MPEG-21 IPMP and REL functionality, and map the design to the IPMPX subsystem on the Test Bed [10].

5.1. IPMP Tool for the MPEG-21 IPMP and REL

The major goals of the MPEG-21 IPMP are to protect digital items and to process the IPMP DIDL elements. On the one hand, the Test Bed supports two kinds of digital items, namely, video and audio. An effective way to protect them is to encrypt the data. Therefore, we focus on the cryptographic tool(s) for providing the MPEG-21 protection functionality. On the other hand, the Test Bed adopts the MPEG-4 Initial Object Descriptor (IOD) to transfer the IPMPX related information. Therefore, we place the IPMP DIDL elements into the corresponding Tool Descriptor. The IPMP DIDL elements are extracted and processed at tool initialization stage.

The functionality related to the MPEG-21 REL is the authorization proof. According to the authorization request, the proof engine derives the stories and/or grants, and determines whether the request is granted or not. Any application that incorporates the REL technology can control the consumption of specific content under specific conditions

In order to provide the above functionalities on the Test Bed, we design an IPMP Tool called `IPMP_Info_Engine`. From the viewpoint of the IPMP sub-system, it serves as the central control element for the other tools. It is an IPMP information management tool which processes the information obtained via local/remote access. In addition, it is also an REL tool which generates an authorization proof upon receiving a request. The implementation details are described in Sec. 5.4.

The `IPMP_Info_Engine` is designed to authorize the user for consuming the right for a specific content and to manage the IPMP DIDL elements. It does not process audio-visual data directly. Thus, the `IPMP_Info_Engine` Tool is not associated with any IPMP Filters. In other words, the control point code should be CONTROL_POINT_NO (0x00).

5.2. Communication between IPMP Tools

For a user to be able to consume a given content, he/she should have appropriate rights on using this resource. As mentioned in the previous sections, in our scenario, the authorization to a user is equivalent to the authorization to the decryption tool. In other words, when an IPMP tool starts to process the data, it must contact the REL tool to obtain the authorization proof. The interactions between the decryption tool (the DES Tool) and the `REL_Info_Engine` are illustrated by Fig. 6:

1. The DES Tool generates a message to request for the authorization proof.
2. The Message Router delivers the message to the `IPMP_Info_Engine`.
3. The `IPMP_Info_Engine` verifies the request and exercises the authorization proof.
4. The `IPMP_Info_Engine` generates a message containing the result of proof checking.
5. The Message Router delivers the proof result message to the DES Tool.

According to the proof result, the DES Tool decides whether it can process the incoming data or not.

5.3. Content Protection Scheme

To protect a broadcast streaming content, we propose a scheme which incorporates the aforementioned MPEG-21 tools. The rights management aspect is achieved by verifying the license, as mentioned in the previous section. The protection aspect is shown in Fig. 7. There are two layers of encrypted streams. The content stream is delivered through the Layer-1 protection. We use the DES block cipher in this layer. Since the DES encryption/decryption is symmetric and simple, it is suitable for bulky data. However, there are two major issues using this technique. The first one is how a client can securely receive the key decrypting the data; and the second is that a simple block cipher is less secure than a complicated cipher. The first issue can be solved by transmitting the key through a trusted secure channel. The solution to the second issue is a trade-off between computation complexity and security. Since the streaming data is very large in size, it is costly to replace the simple cipher with a complicated one. An acceptable solution is applying the simple cipher on the bulky data but with frequent key change. Combining the above two solutions leads to the design of a two-layer protection scheme.

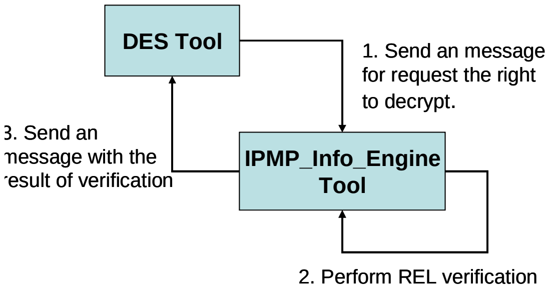

DES Tool
1. Send an message for request the right to decrypt.
3. Send an message with the result of verification
IPMP_Info_Engine Tool
2. Perform REL verification

Fig. 6 Collaboration with IPMP_Info_Engine Tool

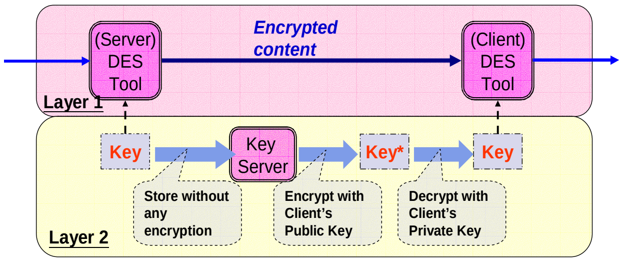

(Server) DES Tool
Encrypted content
(Client) DES Tool
Layer 1
Key
Key Server
Key*
Key
Store without any encryption
Encrypt with Client's Public Key
Decrypt with Client's Private Key
Layer 2

Fig. 7 Content protection scheme

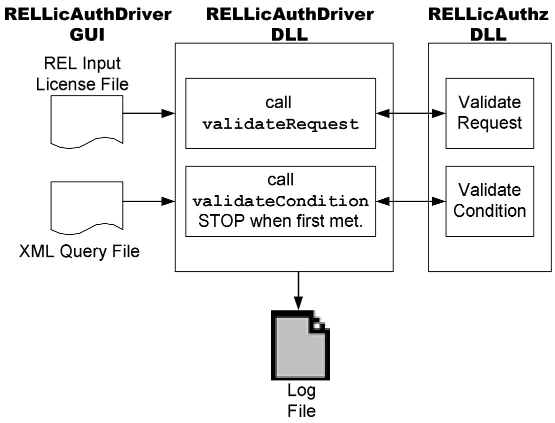


Fig. 8 Dataflow of the REL Reference Software

The Layer-2 protection is a reliable and secure channel for delivering the Layer-1 keys. It is more secure than Layer-1 channel because keys are encrypted using the asymmetric cryptographic (public key) algorithms. We assume that the transmission of the keys is handled by a key server. It may be a locally integrated unit of the streaming server, or a separate remote service. The key databases located at the streaming server and the key server are perfectly synchronized. The synchronization mechanism is implementation dependent and is out of the scope of this paper. The interactions between the client and the key server are specified as follows:

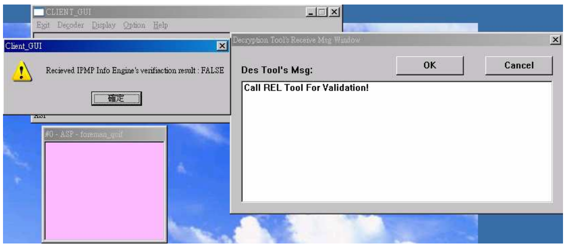
1. The client requests the decryption key by sending a request with its identity.

2. The key server looks up the database to check the request identity and the other required conditions.
3. If the request is valid, the key server encrypts the data decryption keys using the client's public key.
4. The key server sends the returned message containing the encrypted data keys.
5. The client recovers the data keys using its own private key. Then the data keys can be used to decrypt the content bit stream.

Using the above mechanism, the encrypted content can only be decrypted by a client who has the right identity.

5.4. Implementation of IPMP_Info_Engine

We use the REL reference software provided by Content Guard [11] to implement the `IPMP_Info_Engine`. As shown in Fig. 8, the reference software delegates the generation of an authentication request to the GUI frontend. However, in a typical scenario, it should be seamlessly integrated into the entire process and handled automatically rather than manually instructed by the user. But our focus here is a feasibility check of our system. In this implementation, the received REL licenses are stored in a local storage. When the `IPMP_Info_Engine` is accessed, it reads in an XML Query (from the request message or from a local file) and the REL licenses to generate an authorization request. The rest of steps are the same as those of invoking the authorization procedure.

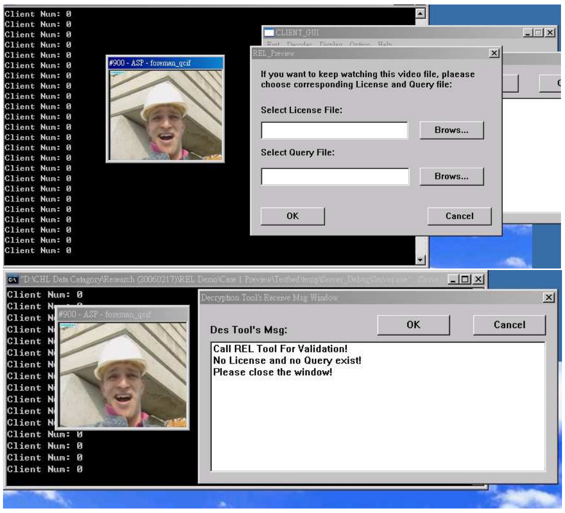

CLIENT_GUI
Exit Decoder Display Option Help
Client_GUI
確定
#0 - ASP - foreman_qcif
Decryption Tool's Receive Msg Window
OK
Cancel

Recieved IPMP Info Engine's verifiaction result : FALSE

Des Tool's Msg:

Call REL Tool For Validation!

Fig. 9 Screenshot from Application Example 1.


#900 - ASP - foreman_qcif
CLIENT_GUI
Exit Decoder Display Option Help
REL_Preview
Brows...
Brows...
OK
Cancel
"D:\CHL Data Catagory\Research (20060217)\REL Demo\Case 1 Preview\Testbed\temp\Server_Debug\Server.exe"
#900 - ASP - foreman_qcif
Decryption Tool's Receive Msg Window
OK
Cancel

```
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
```

If you want to keep watching this video file, plaease choose corresponding License and Query file:

Select License File:

Select Query File:

```
Client Num: 0
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client N
Client Num: 0
Client Num: 0
Client Num: 0
Client Num: 0
```

Des Tool's Msg:

Call REL Tool For Validation!
No License and no Query exist!
Please close the window!

Fig. 10 Screenshots from Application Example 2.

6. APPLICATION EXAMPLES

To demonstrate the features and capability of our design and implementation, we construct three application examples. The first case is secured online playback; the second one is playback with free preview; and the third one is super distribution – online and offline playback.

6.1. Application Example 1: Online Playback

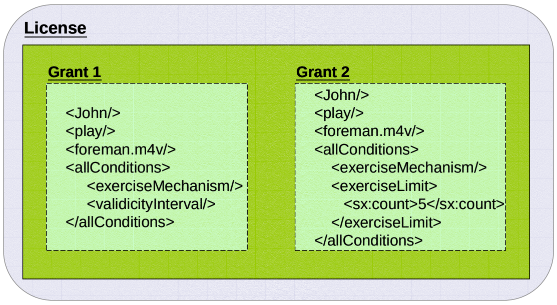
This scenario demonstrates how the "playback" right is exercised in a real-time streaming system. After the session setup, the client receives a license from the server. In this basic-form grant, the principal is the client's identity, the right is "play", and the resource is the video's identity. The tricky item is the condition. We choose the "exerciseMechanism" condition with server parameters to delegate the authorization decision to a remote server.

Upon consuming the video stream, the DES Tool asks the `IPMP_Info_Engine` to do an authorization proof. According to the license, the engine contacts the remote server and sends out the request with the client's identity. The server in this system plays both roles as an authorization server and also a key server. If the client is entitled to consume this video bit stream, the server returns a message containing the data keys which are encrypted using the Layer-2 technique. If the client is not allowed to playback this video stream, the server responds with an empty key set. Since the principal, the right, and the resource are matched with the REL request, the validity of the grant depends only on the condition. If we receive a "false" condition (empty key), the authorization proof fails and the DES Tool refuses to consume the data (Fig. 9). Otherwise, the DES Tool can decrypt the data using the returned keys.

6.2. Application Example 2: Preview

In a typical video/audio online shopping scenario, it often allows the consumers to preview a short video clip, say, for 30 seconds before starting the purchase transaction. This example demonstrates how to implement and control the "preview" behavior using the MPEG-21 REL and DRM concepts.

We assume that the customers can preview a few seconds of a video clip without any license. It is achieved by using a counter in the DES Tool. The counter indicates the remaining number of macro-blocks of a video stream that can be viewed. The authorization proof is delayed until the counter reaches zero. Then, the `IPMP_Info_Engine` pops up a dialog box asking the user to input a valid license and a query file (upper portion of Fig. 10).



```
<John/>
<play/>
<foreman.m4v/>
<allConditions>
    <exerciseMechanism/>
    <validicityInterval/>
</allConditions>
```

```
<John/>
<play/>
<foreman.m4v/>
<allConditions>
    <exerciseMechanism/>
    <exerciseLimit>
        <sx:count>5</sx:count>
    </exerciseLimit>
</allConditions>
```

Fig. 11 Structure of the license in Application Example 3.

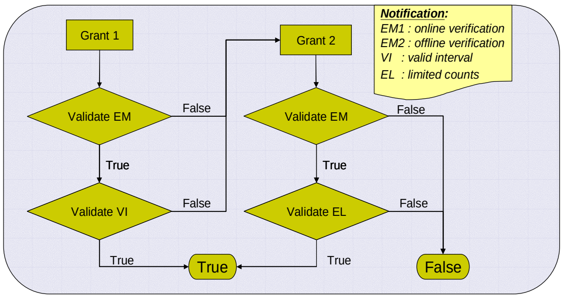


Fig. 12 Flowchart of validating conditions.

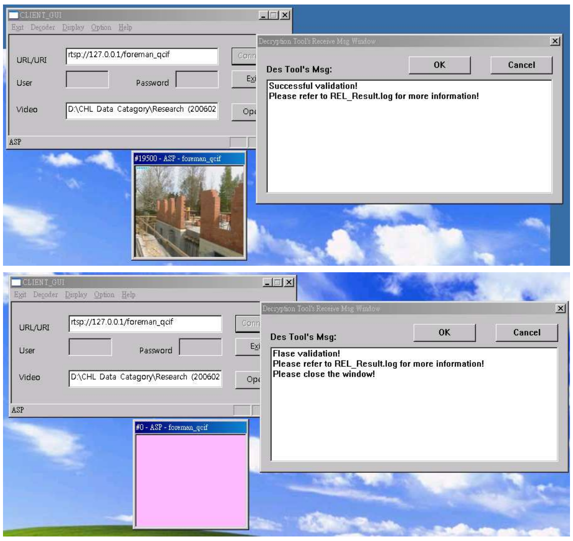
After the user enters the data into the dialog window, the IPMP_Info_Engine performs the authorization proof process. An invalid license or query file would fail the proof and discontinue the playback operation. The lower portion of Fig. **10** shows that the playing operation is stopped in a false case.

6.3. Application Example 3: Super Distribution

This example shows a scenario that occurs in the portable device applications. The so-called "Super Distribution" describes the situation that the content and the right object (the license) are delivered separately. In the following application, we are able to perform online authorization as well as offline verification. It is a very useful scenario for producing and distributing contents for mobile devices. The content is delivered in a protected form. In the first application example, the verification of playback right is performed online in real time. Therefore, we cannot play it back offline. On the other hand, a mobile device may not always be connected to a network. We thus like to design a license that supports both online and offline verification.

A sample license that allows both online and offline verification is shown in Fig. **11**. The license contains two grants. Grant-1 is for online situation, and Grant-2 for offline situation. The condition elements in both grants are encapsulated in an "allConditions" element which means the logical "AND" operation is applied to all the declared conditions inside. In Grant-1, the "exerciseMechanism" specifies a remote authorization server, and the "validicityInterval" specifies the validate execution duration. In Grant-2, the "exerciseMechanism" specifies a local verification, and the "exerciseLimit" specifies a valid number of offline playback times. The verification flow of this license is shown in Fig. 12.

Because the authorization proof process guarantees the matching order of grants, Grant-1 is always verified before Grant-2. In addition, the online verification in our design is the ultimate verification authority. Once an "unauthorized" result is returned from the server, the subsequent local verification should fail. This rule is implemented by the "validators". The first validator checks the network connection first. If the network is unreachable, the validator simply returns a false condition. If the remote server returns an empty decryption key set (means unauthorized), the previously obtained decryption keys are deleted. Otherwise, the keys are replaced with the new set. Whenever Grant-2 should be verified, the second validator checks the decryption keys first. If there are no decryption keys, the playback is not authorized. Otherwise, the exerciseLimit is examined. If it reaches the maximum number of local verifications, the result is false and the keys are deleted.


CLIENT_GUI
Exit Decoder Display Option Help
Conn
Exi
Ope
ASP
#19500 - ASP - foreman_qcif
Decryption Tool's Receive Msg Window
OK
Cancel
CLIENT_GUI
Exit Decoder Display Option Help
Conn
Exi
Ope
ASP
#0 - ASP - foreman_qcif
Decryption Tool's Receive Msg Window
OK
Cancel

URL/URI rtsp://127.0.0.1/foreman_qcif
User
Password
Video D:\CHL Data Catagory\Research (200602

Des Tool's Msg:

```
Successful validation!
Please refer to REL_Result.log for more information!
```

URL/URI rtsp://127.0.0.1/foreman_qcif
User
Password
Video D:\CHL Data Catagory\Research (200602

Des Tool's Msg:

```
Flase validation!
Please refer to REL_Result.log for more information!
Please close the window!
```

Fig. 13 Screenshots from Application Example 3.

Two execution screenshots are shown in Fig. **13**. The upper one shows that a local verification is passed, and the lower one shows a warning message indicating that the maximum number of local verification is reached.

7. CONCLUSIONS

DRM is an important entity in many multimedia applications. Our aim is to construct a DRM system which can provide both content protection and rights management.

In constructing our system in this paper, we use the concepts and tools of MPEG-21 IPMP, MPEG-21 REL, and the MPEG-21Test Bed with MPEG-4 IPMPX. The MPEG-21 IPMP defines high level concepts for protecting Digital Items. The MPEG-21 REL is able to implement a broad range of rights expressions. It also provides an unambiguous right authorization and control model. Because both IPMP and REL are defined at conceptual level, we choose the MPEG-21 Test Bed as our implementation platform. The Test Bed includes an implementation of a modified IPMPX, which adopts many interfaces defined in the MPEG-4 IPMPX.

We designed a two-layer content protection scheme in delivering and decrypting the multimedia contents. To implement the scheme, the IOD was modified to carry a license in the Tool Descriptor. Then, the MPEG-21 REL reference software was integrated into the Test Bed as an IPMP Tool (`IPMP_Info_Engine`). We also modified the DES Tool so that it communicates with the `IPMP_Info_Engine` for receiving the authorization and the decryption keys.

Finally, we constructed three examples to show that our DRM system can provide many types of practical services. The first example demonstrates the content protection with real-time right verification in a streaming application. The second one shows how to design and to use a license for allowing users to preview video clips. The last one shows a more complicated case -- rights management for Super Distribution. In this case, we design a license which enables both online authorization as well as offline verification.

8. ACKNOWLEDGEMENT

This work was supported by National Science Council (Taiwan, ROC) under Grant NSC 94-2219-E-009 -011.

9. REFERENCES

[1] J. Bormans, and K. Hill, “MPEG-21 Overview v.5,” ISO/IEC JTC1/SC29/WG 11 N5231, Shanghai, October 2002.

[2] Study of ISO/IEC 21000-4 FCD – IPMP Components, ISO/IEC JTC1/SC29/WG11 N7426 July 2005, Poznan, Poland.

[3] *Information Technology — Multimedia Framework (MPEG-21)-Part 5: Rights Expression Language*, ISO/IEC 21000-5:2004, May 2004.

[4] C.A. Schultz, "Study of FPDAM ISO/IEC 14496-1:2001/AMD3," ISO/IEC JTC1/SC29/WG11 N4849, Klagenfurt, July 2002.

[5] C.J. Tsai, M. van der Shaar and Y.K. Lim, “PDTR of ISO/IEC TR21000-12 Test Bed for MPEG-21 Resource Delivery,” ISO/IEC JTC1/SC29/WG11 N6255, Hawaii, December 2003.

[6] *Information Technology - Multimedia Framework (MPEG-21) – Part 12: Test Bed for MPEG-21 Resource Delivery*, ISO/IEC 21000-12:2005, Apr. 2005.

[7] C.N. Wang, et al., “FGS-Based Video Streaming Test Bed for MPEG-21 Universal Multimedia Access with Digital Item Adaptation,” ISO/IEC JTC1/SC29/WG11 M8887, October 2002.

[8] *Information Technology — Multimedia Framework (MPEG-21)-Part 2: Digital Item Declaration*, ISO/IEC 21000-2:2003, Mar. 2003.

[9] W3C. (2001) XML Schema, http://www.w3.org/TR/2001//REC-xmlschema-1-20010502/

[10] C.-W. Fan, “MPEG-4 IPMPX Design and Implementation on MPEG-21 Test Bed,” M.S. thesis, Dept. Electrical Engineering, National Chiao Tung University, Hsinchu, Taiwan, R.O.C., June 2004.

[11] X. Wang, et al., “An Exmple Implementation of MPEG-21 REL Reference Software,” ISO/IEC JTC1/SC29/WG11 M9581, March 2003.