國 立 交 通 大 學

資訊學院　資訊學程

碩 士 論 文

應用 Partial DRM 於 DICOM 醫療資訊之版權管理方法

A Study of Partial DRM Application on DICOM Information Protection

研 究 生：徐祥欽

指導教授：陳登吉　教授

中 華 民 國 九 十 九 年 七 月

應用 Partial DRM 於 DICOM 醫療資訊之版權管理方法

A Study of Partial DRM Application on DICOM Information Protection

研 究 生：徐祥欽　　Student：Hsiang-Chin Hsu

指導教授：陳登吉　　Advisor：Deng-Jyi Chen

國 立 交 通 大 學

資訊學院 資訊學程

碩 士 論 文

A Thesis

Submitted to College of Computer Science

National Chiao Tung University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

in

Computer Science

July 2010

Hsinchu, Taiwan, Republic of China

中 華 民 國 九 十 九 年 七 月

應用 Partial DRM 於 DICOM 醫療資訊之版權管理方法

學生：徐祥欽　　指導教授：陳登吉　博士

國 立 交 通 大 學　　資 訊 學 院　　資 訊 學 程 碩 士 班

摘要

隨著資訊科技與網路的發展，數位化的儀器設備及數位化的資訊內容，在各領域的使用需求不斷地成長，所以如何保護一個數位內容裡的資料，則是一個重要的議題。有別於探討版權管理安全性的問題，本研究則是專注在如何將 DRM 機制，用更適當的版權管理方式，來保護所要保護的標的物，以解決不同型態的數位內容在實際運用版權管理保護過程中產生的問題。

在各式各樣的數位內容中，並不是靠一個固定模式的 DRM 保護方式，就能適用於任何的數位內容，如影音資料、多媒體教材、醫療影像資訊的不同等等，本研究提出一套可以應用於醫療影像資訊的版權管理方式，藉由此方式所提供的問題解決方案，協助醫療影像資訊系統的開發人員可以更有彈性的使用版權管理機制來保護他們所要保護的醫療影像內容，以提升開發的品質。

針對醫療影像資訊的特性，我們提出局部性(Partially)的保護方式，讓醫療影像資訊可以針對實務應用的需要，選擇性的對特定項目(Data Element)進行 Partial DRM 的保護，如醫療影像資訊裡的個人隱私資料的保護，醫師對醫療影像所作的專業見解資訊的保護，以及特定影像(Frame)的保護等等，協助開發人員透過此保護模式，來開發特定用途的醫療資訊系統，如醫療知識學習平台、醫療報告查詢平台等等。讓開發者可以避免在醫療資訊的版權保護上將會遭遇到的問題。

我們提出的 Partial DRM 的保護方式，不僅可用於醫療影像資訊上，也可以將此解決模式的框架套用於其他需要 Partial DRM 的應用上；讓日益重要的 DRM 機制，能夠更加符合實務上應用的需求，進而提升版權管理的適用性。

A Study of Partial DRM Application on DICOM Information Protection

Student：Hsiang-Chin Hsu Advisor：Dr. Deng-Jyi Chen

Degree Program of Computer Science
National Chiao Tung University

ABSTRACT

With the development of information technology, the demand of the digital contents and the applications have grown up. Digital content protection has become an important issue in all fields including business, medical information, and etc.. In this thesis, we proposed a special DRM mechanism for the management on particular digital contents with special practical conditions.

It is impractical to apply a fixed DRM protection mode on all kinds of different contents such as video, multimedia learning contents (MLCs), digital image in medicine and etc.. This paper proposed a methodology of partial DRM application on DICOM file for providing the DRM protection on medical images.

Our proposed partial DRM mechanism provides arbitrary user defied protection on medical information, such as medical image frames, doctor's comments, annotations, and personal information. The mechanism would be applied on medical information system, e-learning system and some digital content system in other fields. It would make the DRM mechanism becomes more flexible in more practical applications.

誌謝

衷心感謝陳登吉教授耐心的指導，並在研究過程中，時時給予建議，指引正確的方向，才能順利完成本論文。

感謝博士班學長鎮宇、瑞斌及同窗好友仲智、詩雯、國峰的互相鼓勵與一同進行研究，透過分享與討論，讓本論文可以更好。

最後，要感謝我的家人，在求學的這一段期間內給予的支持與鼓勵，特別要感謝我的父母親對我的照顧與付出，才能成就我的理想，感謝您們!!

目錄

摘要 i
ABSTRACT ii
誌謝 iii
目錄 iv
表目錄 vii
圖目錄 viii
一、 緒論 1
1.1 研究背景 1
1.2 研究動機 2
1.3 研究目標 3
1.4 章節概要 4
二、 相關研究 5
2.1 DICOM 的簡介 5
2.2 典型的 DICOM Network 介紹 5
2.3 DICOM Standard 2009 6
2.4 DICOM 資料結構 7
2.5 DICOM 檔案內容 9
2.6 DICOM 組成元素: Data Element 9
2.7 Data Element 的內部結構 10
2.8 DICOM Value Representations 範例 11
2.9 DICOM 的實際資料內容 11
2.10 DICOM 的 Binary 原始資料 12
2.11 Annotation 的儲存方式 12
2.11.1 以 DICOM 標準格式存放 13
2.11.2 以自訂欄位存放 17
2.11.3 以外掛檔案存放 18
2.12 DICOM 中的個人資料 19
三、 系統分析與設計 20
3.1 系統需求說明 20
3.2 系統架構說明 20
3.3 使用案例圖(use case) 21
3.4 各 Module 說明 22
3.5 DICOM 的解析及資料結構 23
3.5.1 加密流程與資料結構的說明 25
3.5.2 解密流程與資料結構的說明 25

3.6 DICOM 加解密的限制 25
3.6.1 不加密的項目 25
3.6.2 不單獨加密的項目 26
3.6.3 需加密的項目 26
3.7 Key 的設定策略 26
3.8 加密流程 27
3.9 解密流程 28
3.10 授權檔(License.xml) 29
3.11 授權管理視窗流程圖 30
3.12 播放視窗流程圖 31
3.13 Sequence Diagram 32
四、 討論 33
4.1 相容性問題探討 33
4.2 Key 的設定探討 33
五、 實作展示 34
5.1 展示說明 34
5.2 授權管理畫面操作說明 35
5.2.1 登入授權管理程式 35
5.2.2 完成登入 35
5.2.3 顯示 DICOM 列表 36
5.2.4 選擇要授權的 DI COM 檔案 36
5.2.5 選擇要授權的 DI COM 檔案 37
5.2.6 選擇要保護的模式 1 37
5.2.7 選擇要保護的模式 2 38
5.2.8 選擇要保護的模式 3 38
5.2.9 進行加密編碼 39
5.2.10 完成加密編碼 39
5.3 播放畫面操作說明 40
5.3.1 連線至 DRM Server 40
5.3.2 選擇使用者帳號 40
5.3.3 選擇 DICOM 檔案 41
5.3.4 進行檔案下載 41
5.3.5 進行授權檔下載 42
5.3.6 未取得授權畫面 42
5.3.7 取得授權畫面 43
5.3.8 進行解密 43
5.3.9 顯示畫面 44
六、 結論 45

6.1 總結 45
6.2 未來發展方向 45
REFERENCES 46

表目錄

表 1 DICOM Value Representations 11
表 2 Annotation 組成結構 13
表 3 Annotation 的一個範例 14
表 4 DICOM 中的個人資料 19
表 5 資料結構程式碼 24
表 6 常見的 UID 類型 25
表 7 描述影像的 Data Element 26
表 8 未來發展方向 45

圖目錄

圖 1 醫療資訊內的隱私資料 2
圖 2 DRM 面臨著多樣性的應用需求 3
圖 3 一個數位內容檔案 3
圖 4 Partial DRM 的示意圖 4
圖 5 醫療影像儀器的資訊交換 5
圖 6 DICOM Network 6
圖 7 Example of Mapping CT Series 8
圖 8 DICOM 檔案內容 9
圖 9 Data Element 10
圖 10 Data Element 的內部結構 10
圖 11 Data Element 實際範例 11
圖 12 DICOM 的 Binary 原始資料及說明 12
圖 13 自訂欄位範例 17
圖 14 外掛檔案的關連 18
圖 15 系統架構圖 21
圖 16 使用案例圖 21
圖 17 各模組的關係 23
圖 18 加密資料結構圖 23
圖 19 加密流程 27
圖 20 解密流程 28
圖 21 授權檔格式 29
圖 22 授權管理視窗流程圖 30
圖 23 播放視窗流程圖 31
圖 24 Sequence Diagram 32
圖 25 展示說明 34
圖 26 登入授權管理程式 35
圖 27 顯示登入成功訊息 35
圖 28 顯示 DICOM 檔案列表 36
圖 29 顯示 DICOM 內部資訊 36
圖 30 選擇被授權者 37
圖 31 保護模式 - DRM 37
圖 32 保護模式 - Partial DRM 38
圖 33 保護模式 - 不進行保護 38
圖 34 執行加密編碼 39
圖 35 加密編碼完成訊息 39

圖 36　選擇 DRM Server.....40
圖 37　使用者登入.....40
圖 38　選擇 DICOM 檔案.....41
圖 39　下載完成訊息.....41
圖 40　下載授權檔.....42
圖 41　瀏覽時以 Partial 的方式顯示.....42
圖 42　授權檔取得成功訊息.....43
圖 43　解密完成訊息.....43
圖 44　顯示所有授權內容.....44

一、緒論

1.1 研究背景

隨著資訊科技與網路的發展，數位媒體內容的傳播變得相當的快速，因此，數位版權管理的議題也愈來愈受到重視。如果沒有版權保護的機制，那麼創作者的智慧財產就沒有受到保護，數位內容裡的隱私的資料也將被任意取得及使用，因此數位內容的保護更顯得重要且急迫。

在醫療領域中，數位化的醫療設備，也逐漸的取代了傳統的醫療設備，因此，醫療資訊系統在數位化的環境中，扮演著非常重要的角色。為了使醫療資訊系統間能夠互相交換資訊，醫療影像資訊檔案(DICOM)成為了醫療資訊系統間傳遞資料的標準格式。

我們的研究背景，是緣由一個實務上的需求，要達到這樣的需求，會面臨一個與 DICOM 保護的相關問題，我們在論文中提出的方法，就是為了解決這個所遇到的問題，進而使未來發展需求中所提及的系統或相關系統的研究者，得以使用我們的解決方案，來輕鬆的達到他們想完成的功能。而這個需求的簡要描述如下: 當我們去看醫生時，都會關心自己的病情，於是醫師就需向病患解釋原因，而病患也會詢問一些通常性的問題，也就是大家都常會問的問題，於是，醫師就會不斷的回覆每個病患相同的問題，這不僅讓醫療資源無法充份運用，也增加了病患大排長龍的等候時間。因此，醫院希望能有一個醫療知識學習平台，能夠提供民眾/病患/家屬可以獲得療前教育與照護知識，以及提供病患查詢/了解自我病歷與檢查報告或給醫學院學生進行專業研究。

於是，在這樣的需求中，很快的面臨了一個問題，因為在這樣一個教學平台中，其中有一項特別的素材，叫做數位醫療影像(DICOM)， 數位醫療影像中，有所謂的隱私權及智慧財產權的問題，因為醫療影像中包含了許多的資訊，如病人的隱私資料，醫師的診斷見解等。但不是每個病患都願意公開自己的資料。也不是每個醫師都願意開放自己的專業見解。因此，本論文提出的" 應用 Partial DRM 於 DICOM 醫療資訊之版權管理方法"，就是為了解決這個問題。

如前面所提，醫療資訊的隱私問題，在近幾年來，逐漸的受到了重視，如 Health Insurance Portability and Accountability Act, HIPAA (醫療保險轉移和責任法)，就是為了針對醫療資訊的隱私問題，所提出的規範，它規範了醫療資訊的可攜性及保護病患的隱私權等相關問題。並且也成為了美國於 1996 年所通過的法案。HIPAA 提出了的 5 個要求，簡略說明如下:

(1) Patient's Understanding:
病患有權利知道，自己的資料如何為使用及保存。

(2) Confidentiality:

說明了醫療資訊的機密性及對醫療資訊加密的必要。

(3) Patient's Control

病患要能夠掌控誰有權存取或使用資料。

(4) Data Integrity

說明了醫療資料的完整性，如藥物過敏記錄必須完整。

(5) Consent Exception

說明例外情況，如 life-saving purposes，將高於隱私的議題。

從以上可看出，醫療資訊的隱私議題，相當的重要，反之，如果沒有做好隱私的保護， 就會如下圖所示，一個醫療影像內的隱私資料，可以被輕易取得。在圖中，我們可以看到病患的姓名(Patient's Name)，身份證字號(Patient ID)，生日(Patient Date of Birth)、性別(Patient Sex)等等。

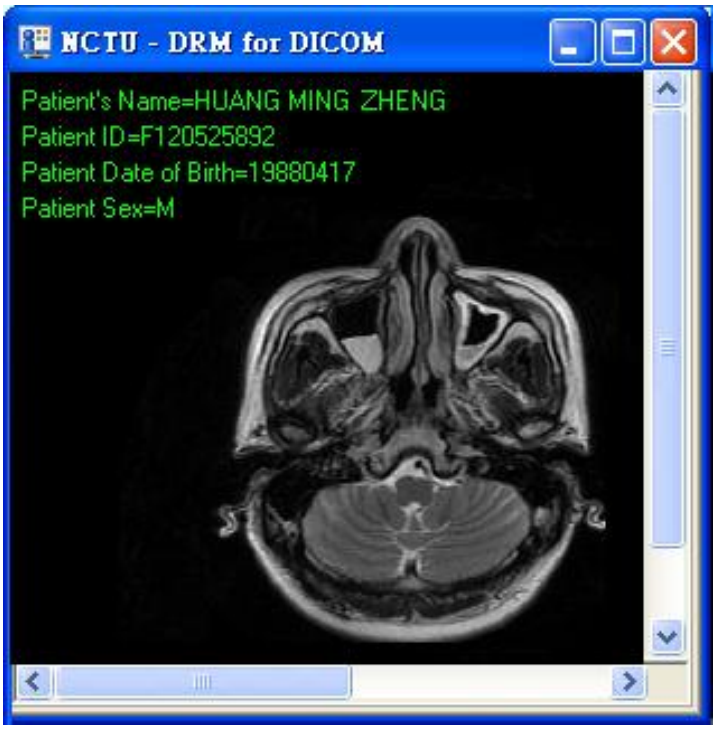

圖 1　醫療資訊內的隱私資料

1.2　研究動機

一般的 DRM 機制在醫療影像資訊的應用上，不夠完備的地方:

- 情況 1:應用於 e-Learning 時

如果獲得了某個 DICOM 檔案，除了取得醫療影像，也取得了病患的個人隱私資料。

- 情況 2:病歷資料有需要被攜帶/移轉至其它醫院時

原醫院醫生的診斷見解無法獲得保護。

本論文希望有一種方式能解決上面所遇到的問題，也由於各種數位內容的商業行為非常的多樣化，因此 DRM 機制也需因應不同的需求做變化，來符合真實世界的各項應用。因此，本論文提出了更有彈性的 DRM 機制---Partial DRM，以符合多樣性的商業應用需求。

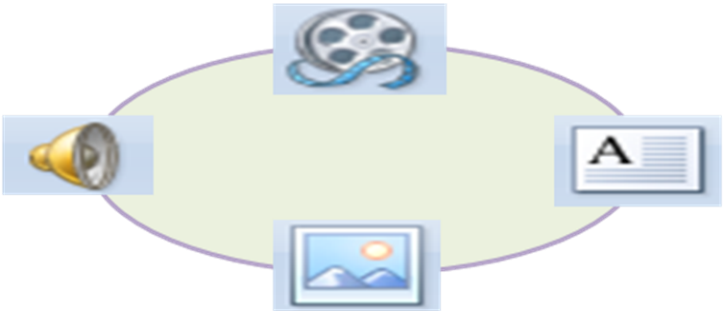

圖 2　DRM 面臨著多樣性的應用需求

1.3　研究目標

我們透過一個有別於傳統 DRM 的加密方式，以 Partial DRM 的方式保護 DICOM 數位內容裡的特定資料群組，做局部性保護，以符合實際應用上的需要。

1.3.1　Partial DRM 的概念:

將一個數位內容檔案，分析其內部結構，只針對所需保護的模組，做局部性保護的版權控管方式。而同時也希望實作出的 Partial DRM 框架，不僅能解決醫療影像的問題，也可依不同的需求作修改，套用於其他需要 Partial DRM 的應用上。

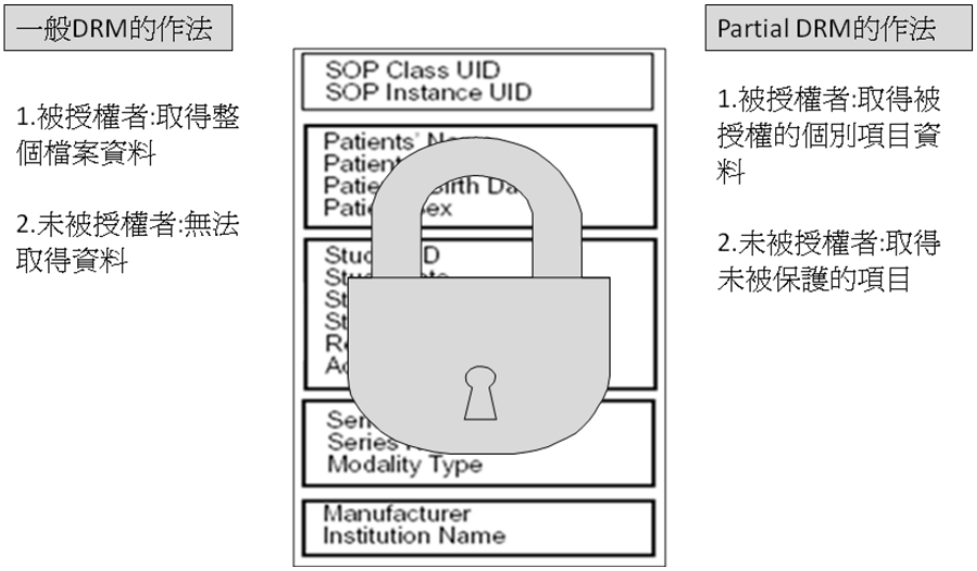

圖 3　一個數位內容檔案

1.3.2 Partial DRM 的實例應用:

我們將應用 Partial DRM 於 DICOM 數位醫療影像，並以實例來解釋 Partial DRM 機制。

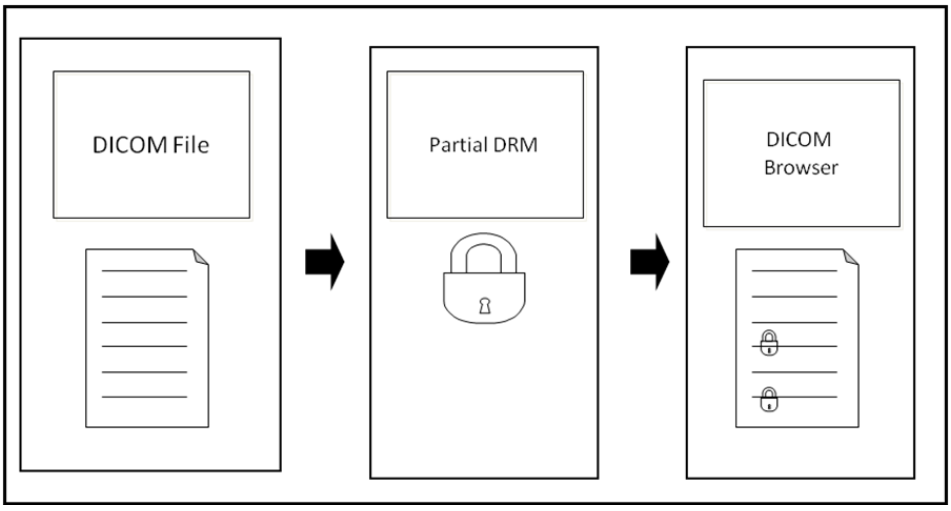

圖 4 Partial DRM 的示意圖

1.4 章節概要

本論文的章節內容摘要如下：

第一章「緒論」，說明本論文的研究背景與動機，以及研究的目標。

第二章「相關研究」，探討與研究相關的文獻。

第三章「系統分析與設計」，對系統的需求及設計做說明。

第四章「討論」，對系統所面臨的問題進行討論及說明。

第五章「實例展示」，透過範例的展示，說明如何使用本論文提出的 Partial DRM 機制。

第六章「結論」，做出總結，並建議未來可以繼續發展的方向。

二、相關研究

2.1 DICOM 的簡介

DICOM(Digital Imaging and Communications in Medicine-醫療數位影像傳輸協定)。在 1982 年時,有鑑於各種醫療影像儀器間的訊息無法傳遞,於是 ACR(American College of Radiology,美國放射學會）和 NEMA（National Electrical Manufacturers Association,國家電子製造商協會）制定出 DICOM 標準,，用於數位化醫學影像傳送、顯示與存儲。在 1993 年正式定名為 DICOM 3.0 已被美國、歐洲、日本等地正式接受並列入國家規範。在台灣地區，中央標準局也已以 DICOM 作為醫療影像資訊交換的標準。

舊式的醫療設備，以 X 光影像為例，在攝影完成後，尚須經過沖片的過程才將肉眼可見的影像呈現在底片上供醫師觀察；但現今數位化的醫療設備及 DICOM 標準的輔助，不同廠商的醫療影像儀器，可藉由 DICOM 格式的檔案，來互相接收與交換影像及病人資料，達到無片化的環境，如下圖所示:

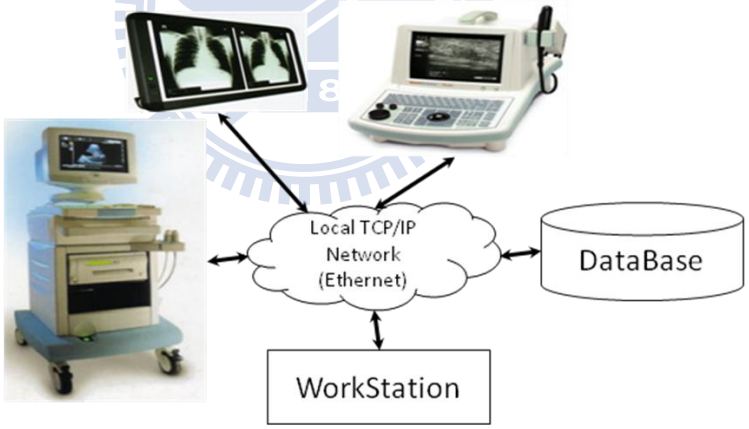

圖 5　醫療影像儀器的資訊交換

2.2 典型的 DICOM Network 介紹

一個 DICOM 的產生過程可分成下面步驟:

- Step1. A CT (Computed Tomography) scan is performed.
- Step2.The scanner constructs a set of images (study).
- Step3.The scanner sends the study to a PACS (Picture Archiving and Communication System - 影像擷取暨傳輸系統).
- Step4. A workstation queries the PACS and retrieves the study.

- Step5. Reconstructions or reformats.

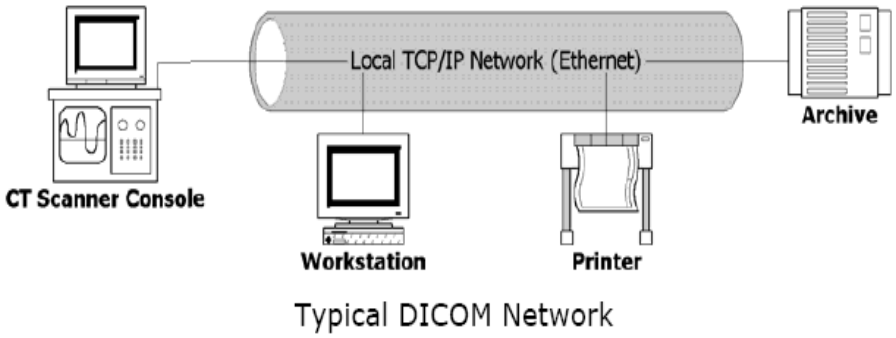

圖 6　DICOM Network
(資料來源：The DICOM standard White Paper v2)

2.3　DICOM Standard 2009

以下為 DICOM 各 Part 的簡略說明:

- Part 1 Introduction and Overview
  引言與概述，簡要介紹了 DICOM 的概念及其組成。
- Part 2 Conformance
  相容性,定義了聲明 DICOM 要求製造商精確地描述其產品的 DICOM 相容性，即構造一個該產品的 DICOM 相容性聲明，它包括選擇什麼樣的資訊物件、服務類、資料編碼方法等，每一個用戶都可以從製造商處得到這樣一份聲明。
- Part 3 Information Object Definitions
  分別定義每種 DICOM 物件(CT,MR, Ultrasound) 等所包含的內容
- Part 4 Service Class Specifications
  服務類詳細論述了作用與資訊物件上的命令及其產生的結果。如儲存、查詢、擷取、列印等。
- Part 5 Data Structures and Encoding
  定義 DICOM 物件的資料結構及語義，描述了怎樣對資訊物件類和服務類進行構造和編碼
- Part 6 Data Dictionary
  說明 DICOM 所定義的每個 Tag 及 UID
- Part 7 Message Exchange
  訂定 DICOM Command Request and Response 的內容
- Part 8 Network Communication Support for Message Exchange
  網路連結建立及資料傳輸的方式。
- Part 9 Retired
- Part10: Media Storage and File Format for Media Interchange

定義 DICOM 物件存檔資料時檔案目錄及檔案本身的格式

- Part11: Media Storage Application Profiles
  定義應用軟體可具備的 DICOM File Service 存取功能
- Part12: Formats and Physical Media
  說明各種儲存媒體儲存 DICOM 資料時的格式
- Part13 Retired
- Part 14: Grayscale Standard Display Function
  說明 DICOM 影像在螢幕顯示以及列印時的規格及要求。
- Part15:Security Profiles
  說明 DICOM 資料在網路傳輸時加密的方式以及利用電子簽章簽認 DICOM 影像及報告的方式
- Part 16: Content Mapping Resource
  規範 DICOM 引用之醫學相關標準詞彙及詞彙格式
- Part17: Explanatory Information
  人體部位及各種檢查報告之說明
- Part 18: Web Access to DICOM Persistent Objects (WADO)
  規範 DICOM server 網路功能

2.4 DICOM 資料結構

以一個實際情況說明，假設一個病患到醫院就診，為了判斷病情，醫師指定了各種不同的檢查，如電腦斷層影像(CT)、核磁共振影像(MR)，每一個檢查項目都需要一個相對應的儀器來完成，但影像儀器所產生的往往不是單張而是一系列的影像（假設 MR 產生一組 10 張，CT 產生兩組各 6、10 張影像），那麼這些影像要如何使用 DICOM 規範保存呢?

從 DICOM 的資料結構來看，分成了 Patient、Study、Series、View 四個層級來儲存上述的例子，Patient 中包含了病患的所有基本資料，Patient 底下的 Study 有二組 ，一組為 MR，另一組為 CT，在 CT 這個 Study 下，又分為二個 Series，這二個 Series 又各有 6 張和 8 張影像。當醫師需要調閱影像時，只要輸入病患相關資料，就能依據這一連串的資料結構找到病患所做過的檢查，及其中包含的所有醫學影像。

我們將資料整理如下:

- 核磁共振影像(MR)x1 組(10 張影像)
- 電腦斷層影像(CT)x2 組(6 張及 8 張影像)

從 DICOM 的資料結構來看:

Patient
|--Study 1(MR)
| |--Series 1

| | |-- View 1(Acquisition)
| | | |--Image 1~10
|
|-- Study 2(CT)
| |-- Series 1
| | |-- View 1
| | | |--Reference Image
| | |-- View 2
| | | |--Image 1~6
| |
| |-- Series 2
| | |-- View 1
| | |-- Image 1~8

以圖形更能看出它們之間的關係:

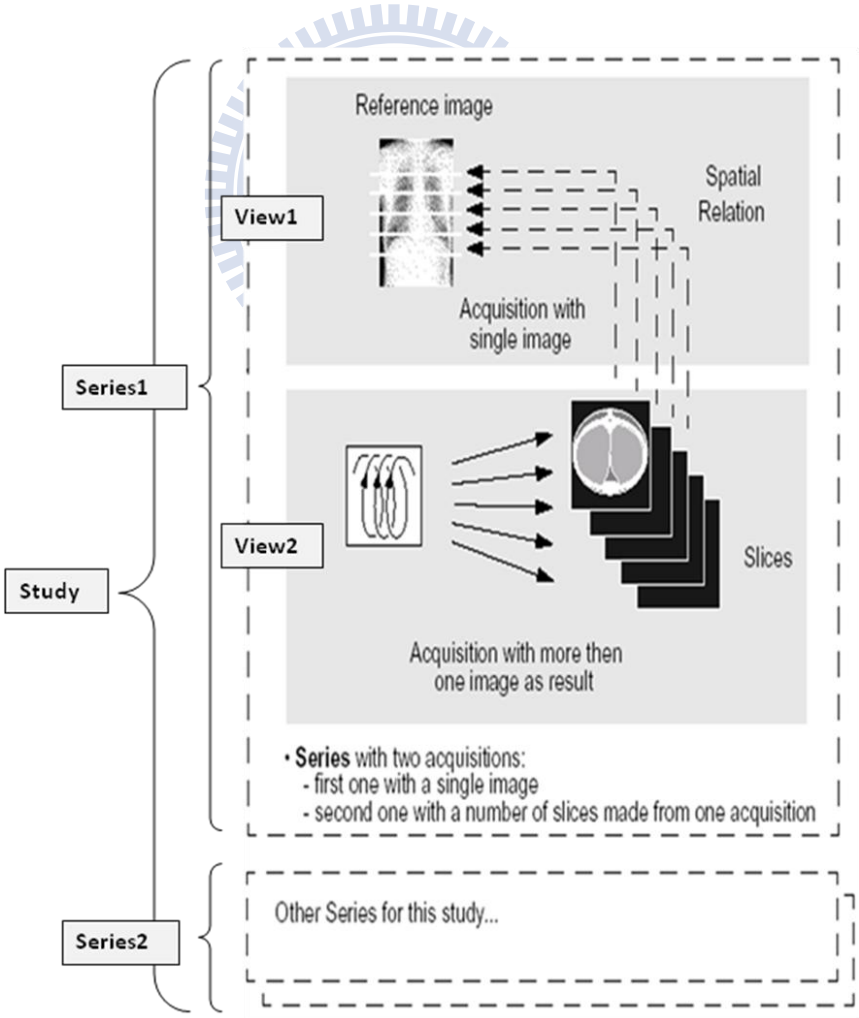

圖 7　Example of Mapping CT Series

2.5 DICOM 檔案內容

以下列出了一個 DICOM 檔案的內容，各個 Group 分別描述了 Patient/ Study/ Series/ Equipment/Image 等資訊。

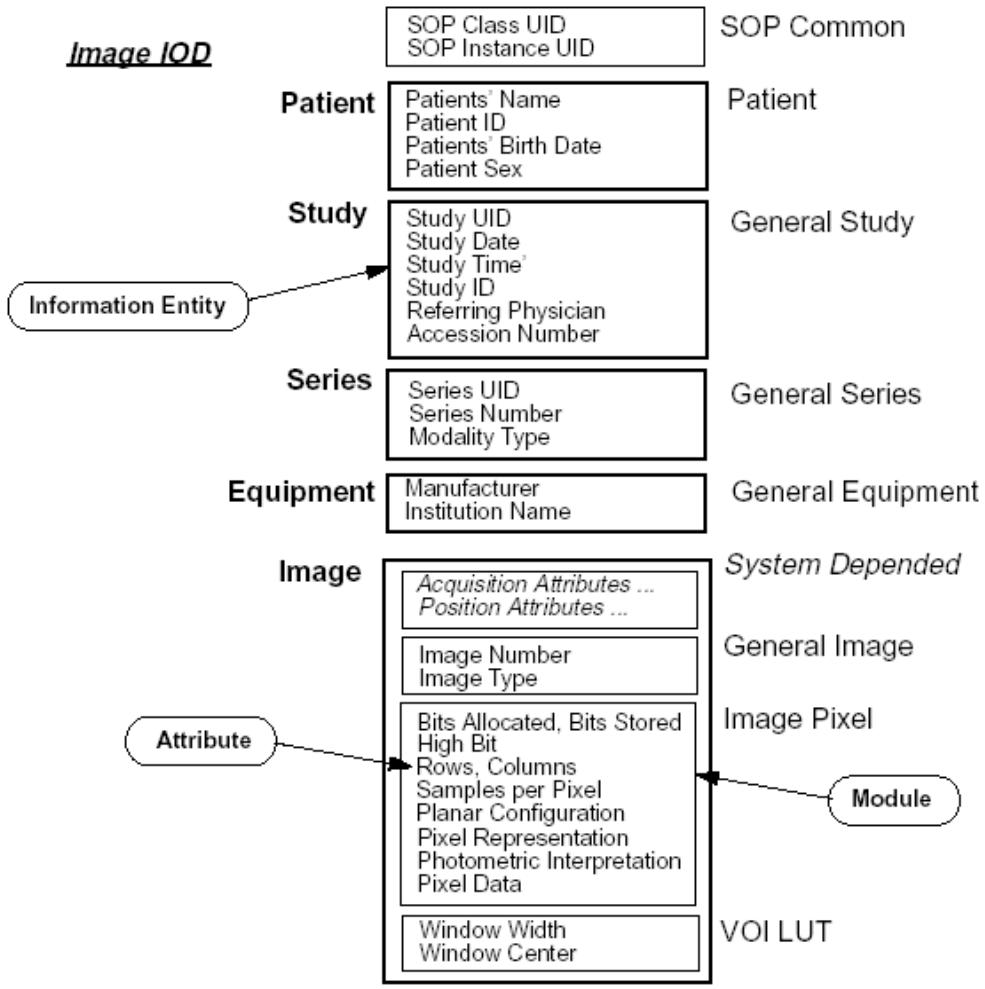

圖 8 DICOM 檔案內容

2.6 DICOM 組成元素: Data Element

從上圖來看，每一個檔案由許多 Group 所組成，每一個 Group 又由許多的小項目組成，而這個最小單位的小項目我們稱為 Data Element，每個 Data Element 又由下面欄位組成，所以可將一個 DICOM 檔案視為是一連串的 Data Element 所組成。

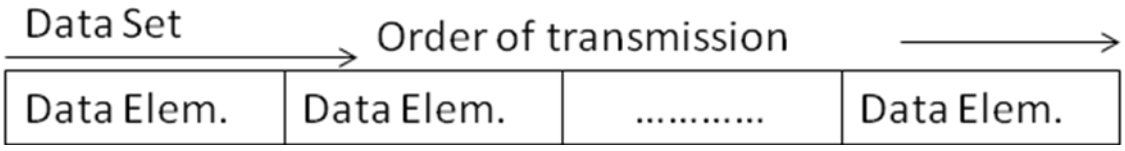

圖 9　Data Element

2.7　Data Element 的內部結構

將每個 Data Element 放大來看，可分解成四部分 TAG, VR, Value Length, Value Field，TAG 是由類似(Group ID, Element ID)這樣的排列組成，數字是採 HEX 來表示，如(0010,0010)就是 Patient Name 的 TAG 識別碼，而(0008,103E)是序列描述 (series description) 的 TAG 識別碼。

VR 是 Value Representation 的縮寫，它所代表的是 data element 的資料型別，如前例，(0010, 0010) = Patient Name,其 VR = PN，代表若是(Group ID, Element ID)之 VR=PN, 我們預期應該是有關名字的描述，如果 VR = DA，則表示 date，為日期的資料型別，VR=TM 表示 time，為時間的資料型別，而 VR =UI，則表示 UID 為唯一識別碼的資料型別，VR 事實上是一個 option 的欄位，它端視在傳輸過程中之協定(transfer syntax)來決定是否要在 data element 中加上這個欄位，如果是 explicit 格式，data element 必須將 VR 明確表示，若是 implicit 則可隱藏不需明示。

Value Length 則是表示在 Value Field 中之實際資料長度，而 Value Field 則是存放該 data element 的實際文字，數值或圖形資料。

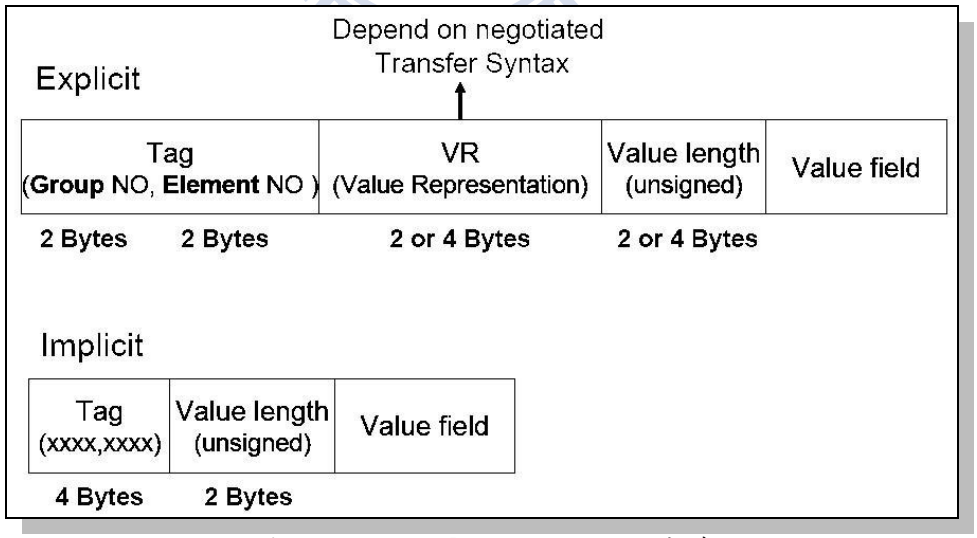

圖 10　Data Element 的內部結構

2.8 DICOM Value Representations 範例

表 1 列出了部份的 VR 資料。

表 1 DICOM Value Representations

VR Name	Definition
DA	Date
DT	Date Time
FL	Floating Point
LO	Long String
PN	Person Name
TM	Time
SQ	Sequence of Items
OB	Other Byte String
UI	Unique Identifier (UID)
UL	Unsigned Long
US	Unsigned Short
…..	

(資料來源：DICOM Spec. 5-Table 6.2-1)

2.9 DICOM 的實際資料內容

底下為一個應用程式對 DICOM 做 Parsing 後得到的結果。

Group - Element	Description	Type	Length	Value
0002 0000	Group Length	UL	4	192
0002 0001	File Meta Information Version	OB	2	(binary data)
0002 0002	Media Storage SOP Class UID	UI	28	1.2.840.10008.5.1.4.1.1.1.1
0002 0003	Media Storage SOP Instance UID	UI	46	1.2.840.113681.2162644097.6...
0002 0010	Transfer Syntax UID	UI	18	1.2.840.10008.1.2
0002 0012	Implementation Class UID	UI	16	1.2.804.114118.3
0002 0013	Implementation Version Name	SH	6	eFilm
0002 0016	Source Application Entity Title	AE	16	
0008 0000	Group Length	UL	4	852
0008 0005	Specific Character Set	CS	10	ISO_IR 100
0008 0008	Image Type	CS	18	DERIVED\PRIMARY\IT
0008 0016	SOP Class UID	UI	28	1.2.840.10008.5.1.4.1.1.1.1
0008 0018	SOP Instance UID	UI	46	1.2.840.113681.2162644097.6...
0008 0020	Study Date	DA	8	20020123
0008 0021	Series Date	DA	8	20020123
0008 0022	Acquisition Date	DA	8	20020123
0008 0023	Image Date	DA	8	20020123
0008 0030	Study Time	TM	6	170048
0008 0031	Series Time	TM	6	170049
0008 0032	Acquisition Time	TM	6	170331
0008 0033	Image Time	TM	6	170331
0008 0050	Accession Number	SH	8	20044731
0008 0060	Modality	CS	2	DX
0008 0068	Presentation Intent Type	CS	16	FOR PRESENTATION
0008 0070	Manufacturer	LO	14	HOLOGIC, Inc.

圖 11 Data Element 實際範例

2.10 DICOM 的 Binary 原始資料

底下以二進制(binary)原始資料方式顯示 DICOM 的內容，這部份也是在我們在第四章實作 DICOM Parser 時，所處理的資料來源。

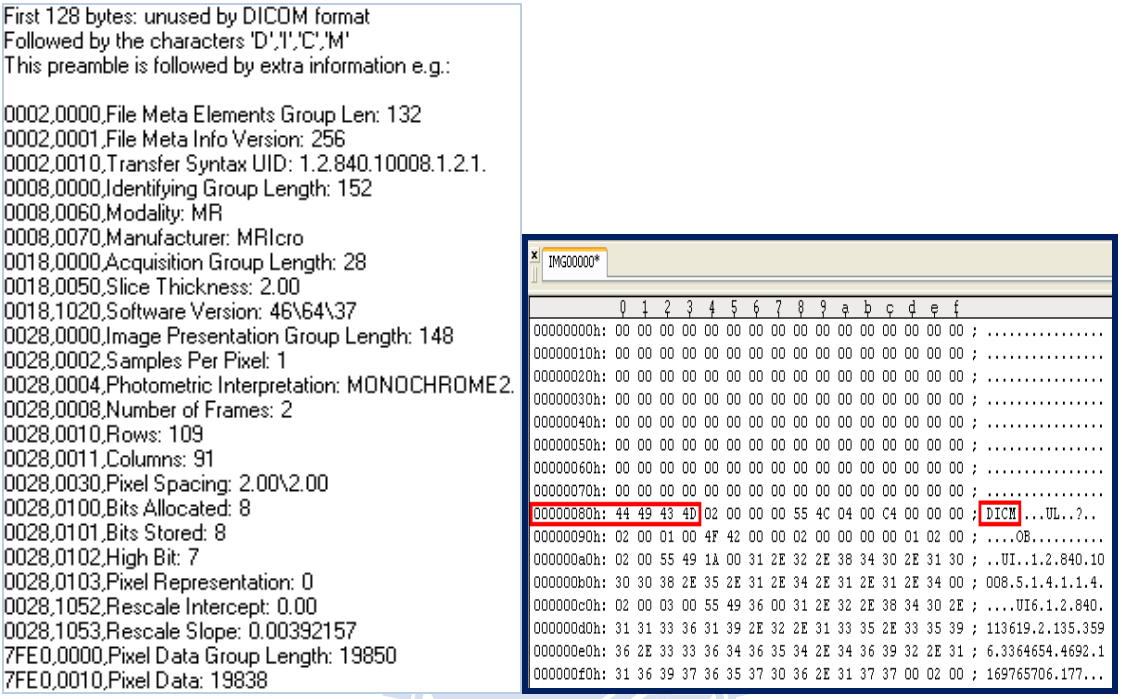

圖 12 DICOM 的 Binary 原始資料及說明

2.11 Annotation 的儲存方式

在 DICOM 內部，儲存 Annotation 的方式，大致有以下三種，

1.以 DICOM 標準格式存放

2.以自訂欄位存放

3.以外掛檔案存放

說明如下:

2.11.1 以 DICOM 標準格式存放

在下表中，顯示了 Annotation 的基本結構:

表 2　Annotation 組成結構

GraphicAnnotationSequence

(0070,0001) GraphicAnnotationSequence
{
(0008,1140) ReferencedImageSequence
(0070,0002) GraphicLayer
(0070,0008) TextObjectSequence
(0070,0009) GraphicObjectSequence
}

ReferencedImageSequence

(0008,1140) ReferencedImageSequence
{
(0008,1150) ReferencedSOPClassUID
(0008,1155) ReferencedSOPInstanceUID
(0008,1160) ReferencedFrameNumber
}

TextObjectSequence

(0070,0008) TextObjectSequence
{
(0070,0003) BoundingBoxAnnotationUnits
(0070,0006) UnformattedTextValue
(0070,0010) BoundingBoxTopLeftHandCorner
(0070,0011) BoundingBoxBottomRightHandCorner
(0070,0012) BoundingBoxTextHorizontalJustification
}

GraphicObjectSequence

(0070,0009) GraphicObjectSequence
{
(0070,0005) GraphicAnnotationUnits
(0070,0020) GraphicDimensions
(0070,0021) NumberOfGraphicPoints
(0070,0022) GraphicData
(0070,0023) GraphicType
(0070,0024) GraphicFilled
}

從上表中可以看出，首先由 (0070,0001)開始進入一個巢狀的 annotation 結構, 內部可能包含了很多組的 ReferencedImageSequence 、 GraphicLayer 、 TextObjectSequence、GraphicObjectSequence 等等，以 TextObjectSequence 來說，(0070,0006)記錄了一個文字類型的 annotation，(0070,0010)和(0070,0011)記錄了此 annotation 的座標，以 GraphicObjectSequence 來說，(0070,0023) 記錄了 POLYLINE、CIRCLE 等圖形；因此，利用這些組合，即可組成一個 DICOM 裡的 annotation 描述。下表為一個更細部的 Annotation 範例:

表 3　Annotation 的一個範例

GraphicAnnotationSequence
(0070,0001) SQ (Sequence with explicit Length #=2) # 1096, 1 GraphicAnnotationSequence
(fffe,e000) na (Item with explicit Length #=4) # 820, 1 Item
(0008,1140) SQ (Sequence with explicit Length #=1) # 122, 1 ReferencedImageSequence
(fffe,e000) na (Item with explicit Length #=3) # 114, 1 Item
(0008,1150) UI =SecondaryCaptureImageStorage # 26, 1 ReferencedSOPClassUID
(0008,1155) UI [1.2.826.0.1.36809.29274.2156968137] # 62, 1 ReferencedSOPInstanceUID
(0008,1160) IS [1] # 2, 1 ReferencedFrameNumber
(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem
(fffe,e0dd) na (SequenceDelimitationItem for re-enc.) # 0, 1 SequenceDelimitationItem
(0070,0002) CS [TESTLAYER_1 0] # 14, 1 GraphicLayer
(0070,0008) SQ (Sequence with explicit Length #=1) # 102, 1 TextObjectSequence
(fffe,e000) na (Item with explicit Length #=5) # 94, 1 Item
(0070,0003) CS [PIXEL] # 6, 1 BoundingBoxAnnotationUnits
(0070,0006) ST [This is my text annotation] # 28, 1 UnformattedTextValue
(0070,0010) FL 123.492\238.041 # 8, 2 BoundingBoxTopLeftHandCorner
(0070,0011) FL 136.451\71.1288 # 8, 2 BoundingBoxBottomRightHandCorner
(0070,0012) CS [LEFT] # 4, 1 BoundingBoxTextHorizontalJustification
(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem
(fffe,e0dd) na (SequenceDelimitationItem for re-enc.) # 0, 1 SequenceDelimitationItem
(0070,0009) SQ (Sequence with explicit Length #=5) # 538, 1 GraphicObjectSequence
(fffe,e000) na (Item with explicit Length #=6) # 84, 1 Item
(0070,0005) CS [PIXEL] # 6, 1 GraphicAnnotationUnits
(0070,0020) US 2 # 2, 1 GraphicDimensions
(0070,0021) US 2 # 2, 1 NumberOfGraphicPoints
(0070,0022) FL 227.627\118.285... # 16, 4 GraphicData
(0070,0023) CS [POLYLINE] # 8, 1 GraphicType
(0070,0024) CS [N] # 2, 1 GraphicFilled
(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e000) na (Item with explicit Length #=6) # 108, 1 Item

(0070,0005) CS [PIXEL] # 6, 1 GraphicAnnotationUnits

(0070,0020) US 2 # 2, 1 GraphicDimensions

(0070,0021) US 5 # 2, 1 NumberOfGraphicPoints

(0070,0022) FL 64.4814\179.031... # 40, 10 GraphicData

(0070,0023) CS [POLYLINE] # 8, 1 GraphicType

(0070,0024) CS [N] # 2, 1 GraphicFilled

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e000) na (Item with explicit Length #=6) # 82, 1 Item

(0070,0005) CS [PIXEL] # 6, 1 GraphicAnnotationUnits

(0070,0020) US 2 # 2, 1 GraphicDimensions

(0070,0021) US 2 # 2, 1 NumberOfGraphicPoints

(0070,0022) FL 223.288\395.98... # 16, 4 GraphicData

(0070,0023) CS [CIRCLE] # 6, 1 GraphicType

(0070,0024) CS [N] # 2, 1 GraphicFilled

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e000) na (Item with explicit Length #=6) # 100, 1 Item

(0070,0005) CS [PIXEL] # 6, 1 GraphicAnnotationUnits

(0070,0020) US 2 # 2, 1 GraphicDimensions

(0070,0021) US 4 # 2, 1 NumberOfGraphicPoints

(0070,0022) FL 415.939\238.041... # 32, 8 GraphicData

(0070,0023) CS [ELLIPSE] # 8, 1 GraphicType

(0070,0024) CS [N] # 2, 1 GraphicFilled

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e000) na (Item with explicit Length #=6) # 124, 1 Item

(0070,0005) CS [PIXEL] # 6, 1 GraphicAnnotationUnits

(0070,0020) US 2 # 2, 1 GraphicDimensions

(0070,0021) US 7 # 2, 1 NumberOfGraphicPoints

(0070,0022) FL 358.664\308.332... # 56, 14 GraphicData

(0070,0023) CS [POLYLINE] # 8, 1 GraphicType

(0070,0024) CS [N] # 2, 1 GraphicFilled

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e0dd) na (SequenceDelimitationItem for re-enc.) # 0, 1 SequenceDelimitationItem

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e000) na (Item with explicit Length #=3) # 260, 1 Item

(0008,1140) SQ (Sequence with explicit Length #=1) # 122, 1 ReferencedImageSequence

(fffe,e000) na (Item with explicit Length #=3) # 114, 1 Item

(0008,1150) UI =SecondaryCaptureImageStorage # 26, 1 ReferencedSOPClassUID

(0008,1155) UI [1.2.826.0.1.36800.29274.2156968137] # 62, 1 ReferencedSOPInstanceUID

(0008,1160) IS [1] # 2, 1 ReferencedFrameNumber

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e0dd) na (SequenceDelimitationItem for re-enc.) # 0, 1 SequenceDelimitationItem

(0070,0002) CS [TESTLAYER_2 1] # 14, 1 GraphicLayer

(0070,0009) SQ (Sequence with explicit Length #=1) # 92, 1 GraphicObjectSequence

(fffe,e000) na (Item with explicit Length #=6) # 84, 1 Item

(0070,0005) CS [PIXEL] # 6, 1 GraphicAnnotationUnits

(0070,0020) US 2 # 2, 1 GraphicDimensions

(0070,0021) US 2 # 2, 1 NumberOfGraphicPoints

(0070,0022) FL 104.4\64.4814... # 16, 4 GraphicData

(0070,0023) CS [POLYLINE] # 8, 1 GraphicType

(0070,0024) CS [N] # 2, 1 GraphicFilled

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e0dd) na (SequenceDelimitationItem for re-enc.) # 0, 1 SequenceDelimitationItem

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e0dd) na (SequenceDelimitationItem for re-enc.) # 0, 1 SequenceDelimitationItem

(0070,0041) CS [N] # 2, 1 ImageHorizontalFlip

(0070,0042) US 90 # 2, 1 ImageRotation

(0070,005a) SQ (Sequence with explicit Length #=1) # 212, 1 DisplayedAreaSelectionSequence

(fffe,e000) na (Item with explicit Length #=6) # 204, 1 Item

(0008,1140) SQ (Sequence with explicit Length #=1) # 112, 1 ReferencedImageSequence

(fffe,e000) na (Item with explicit Length #=2) # 104, 1 Item

(0008,1150) UI =SecondaryCaptureImageStorage # 26, 1 ReferencedSOPClassUID

(0008,1155) UI [1.2.826.0.1.3680.29274.2156968137] # 62, 1 ReferencedSOPInstanceUID

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e0dd) na (SequenceDelimitationItem for re-enc.) # 0, 1 SequenceDelimitationItem

(0070,0052) SL 1\1 # 8, 2 DisplayedAreaTopLeftHandCorner

(0070,0053) SL 512\512 # 8, 2 DisplayedAreaBottomRightHandCorner

(0070,0100) CS [MAGNIFY] # 8, 1 PresentationSizeMode

(0070,0102) IS [10000\10000] # 12, 2 PresentationPixelAspectRatio

(0070,0103) FL 1.15234 # 4, 1 PresentationPixelMagnificationRatio

(fffe,e00d) na (ItemDelimitationItem for re-encoding) # 0, 1 ItemDelimitationItem

(fffe,e0dd) na (SequenceDelimitationItem for re-enc.) # 0, 1 SequenceDelimitationItem

(0070,0060) SQ (Sequence with explicit Length #=2) # 156, 1 GraphicLayerSequence

(fffe,e000) na (Item with explicit Length #=4) # 70, 1 Item

(0070,0002) CS [TESTLAYER_1 0] # 14, 1 GraphicLayer

(0070,0062) IS [1] # 2, 1 GraphicLayerOrder

```
(0070,0066) US       65535                    #       2,  1  GraphicLayerRecommendedDisplayGrayscaleValue
(0070,0068) LO       [sample test layer 1]                   #      20,  1  GraphicLayerDescription
(fffe,e00d) na       (ItemDelimitationItem for re-encoding) #       0,  1  ItemDelimitationItem
(fffe,e000) na       (Item with explicit Length   #=4)       #      70,  1  Item
(0070,0002) CS       [TESTLAYER_2 1]                         #      14,  1  GraphicLayer
(0070,0062) IS       [2]                                     #       2,  1  GraphicLayerOrder
(0070,0066) US       65535                    #       2,  1  GraphicLayerRecommendedDisplayGrayscaleValue
(0070,0068) LO       [sample test layer 2]                   #      20,  1  GraphicLayerDescription
(fffe,e00d) na       (ItemDelimitationItem for re-encoding) #       0,  1  ItemDelimitationItem
(fffe,e0dd) na       (SequenceDelimitationItem for re-enc.) #       0,  1  SequenceDelimitationItem
```

2.11.2 以自訂欄位存放

由於 Annotation 的形式各式各樣，甚至可能包含了影音及其他多媒體的素材，使得 Annotation 的儲存變得相當複雜，因此，也可以使用自訂欄位的方式儲存，方法為新增一組新的 Tag，並依照 DICOM 的標準 Data Element 格式，定義出自己所需的結構。

Tag (Group NO, Element NO)	VR (Value Representation)	Value Length	Value Field
DFFD,0001	OB	0x0180	DcESAe3fV....

圖 13　自訂欄位範例

2.11.3 以外掛檔案存放

相對於 DICOM 標準的 Annotation 的形式，外掛檔案方式是存放於 DICOM 檔案外部，並且在外掛的 Annotation 檔案中，使用 UID 的方式，與 DICOM 檔案做關聯。

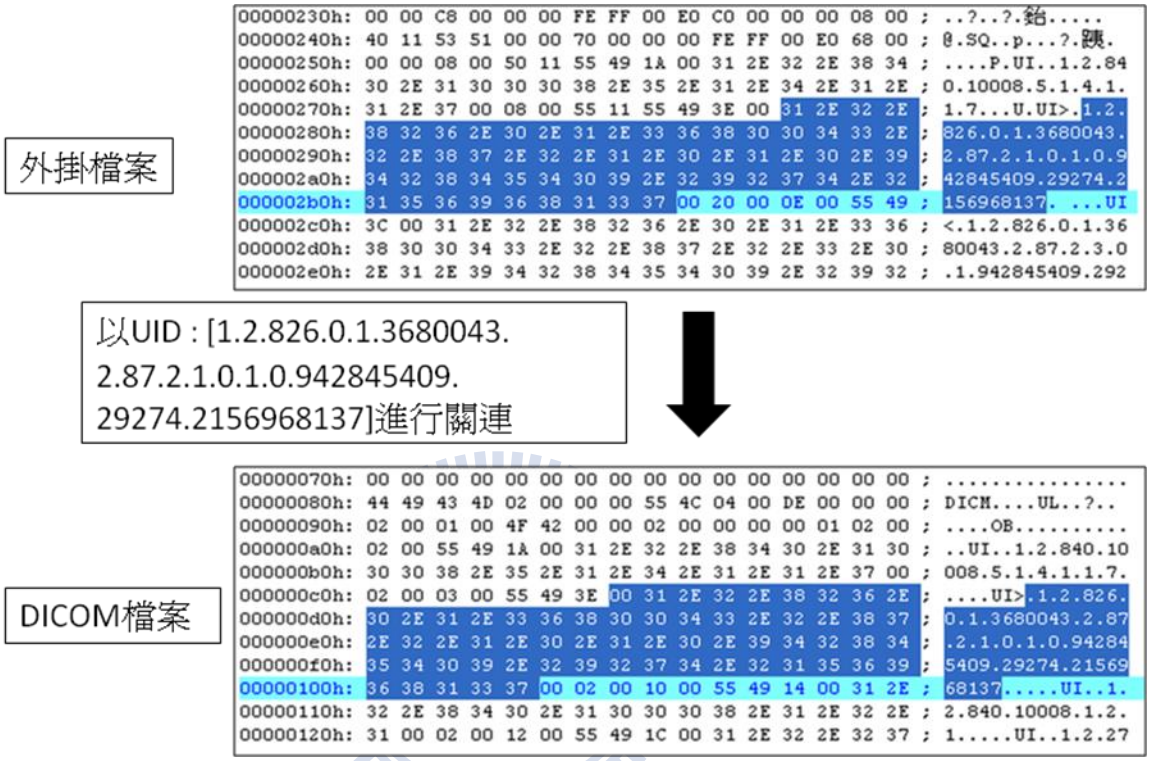

圖 14　外掛檔案的關連

2.12 DICOM 中的個人資料

在 DICOM 中，有關個人的隱私資料是放在 Patient Identification Module 裡，如下表所示:

表 4　DICOM 中的個人資料

Attribute Name	Tag	Attribute Description
Patient's Name	(0010,0010)	Patient's full legal name
Patient ID	(0010,0020)	Primary hospital identification number or code for the patient
Issuer of Patient ID	(0010,0021)	Name of healthcare provider which issued the Patient ID
Other Patient IDs	(0010,1000)	Other identification numbers or codes used to identify the patient
Other Patient Names	(0010,1001)	Other names used to identify the patient
Patient's Birth Name	(0010,1005)	Patient's birth name
Patient's Mother's Birth Name	(0010,1060)	Birth name of patient's mother
Medical Record Locator	(0010,1090)	An identifier used to find the patient's existing medical record (e.g. film jacket)

三、系統分析與設計

3.1 系統需求說明

在這一章節一開始，我們再重新定義一次整個系統的需求：

由於 DICOM 的數位內容資料中，可能夾帶有醫師的專業見解資料 (註解) 以及病人敏感的隱私資料和多個醫療影像圖層。因為在實際應用上，我們需要局部性的去保護某些項目。因此，我們的要實作一個應用程式，來對 DICOM 檔案進行 Partial DRM 的版權保護。

前面所提到的醫師的專業見解資料(註解)，在 DICOM 中，將以 Annotation 的型式存放，一般 Annotation 的存放方式可略分為下面三種:

1.以 DICOM 標準格式存放

2.以自訂欄位存放

3.以外掛檔案存放

在我們的實作中，我們會以自訂欄位方式存放，當然這部份也可以依實際的應用需要來修改成其他的存放方式。

對 DICOM 做了 Partial DRM 後，可運用在什麼地方?

我們制作了 Partial DRM 的框架，是為了解決 DRM 在 DICOM 醫療影像的應用上不夠完備的地方，那麼解決這個問題之後，又能提供給醫療程式開發者哪方面的應用?

我們提出了幾個方向，如醫療影像教材:

例 1.經過授權的人員，可以看到醫師的見解資料(註解)。

例 2.經過授權的人員，才能取得病人隱私資料。

3.2 系統架構說明

在我們實作的系統中，主要將系統分為三個部份，第一部份，為 DRM Server，第二部份，為管理者建立授權方式的視窗，稱之為授權管理視窗，第三部份，為使用者瀏覽 DICOM 的視窗，稱之為播放視窗。

在程式的架構中，主要由管理者經由授權管理視窗，建立授權規則，並對授權檔案進行加密，而播放視窗則提供使用者登入，經由 DRM Server 的認證，下載被授權閱覽的醫療影像，進行解密及播放。以下為系統架構圖:

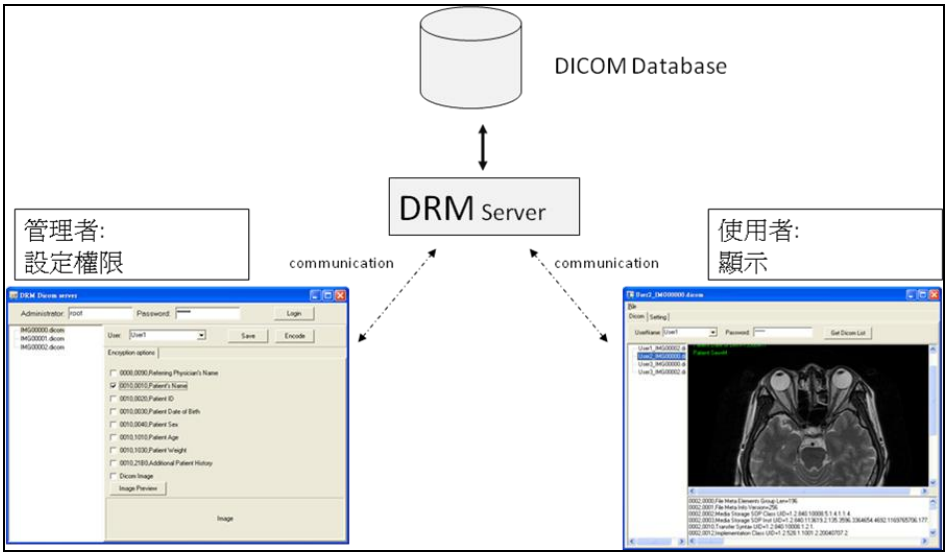

圖 15　系統架構圖

3.3　使用案例圖(use case)

在使用案例圖中，說明了參與系統使用的角色，與系統之間的關係，首先，管理者可以進行:

1.管理 DICOM 的資料

2.建立 DICOM 檔案的 DRM 或 Partial DRM 或不保護的授權設定

3.建立被授權者的權限

使用者端可進行的操作有:

1.取得 DICOM 影像

2.閱覽被授權的內容

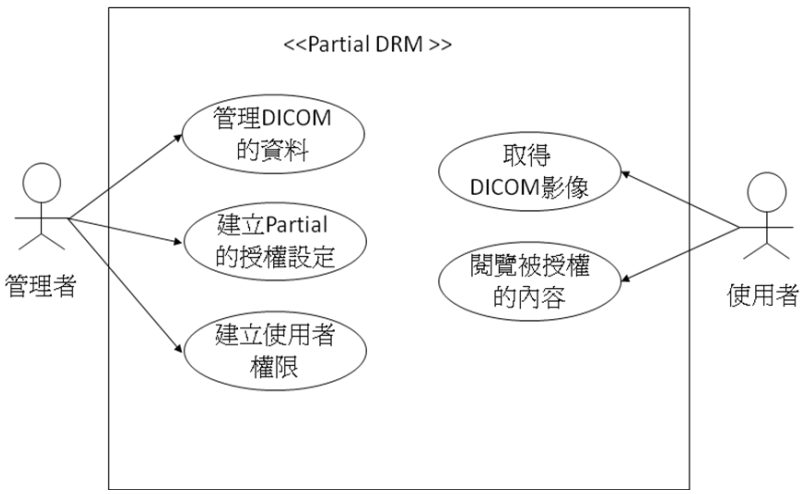

圖 16　使用案例圖

3.4 各 Module 說明

在系統中，我們以各 function 面區分成單獨的模組，每個模組可以實際的需要做抽換，例如，今天要將 AES 加解密模組替換成 DES 的加解密方式，只需單獨將 AES 的模組取代即可，不需更動系統的其他模組，其他模組同理，可依實際需要做適當的搭配組合。

各模組之間的運作，可略分成管理介面和播放介面，首先說明管理介面的功能:

1. 管理者經由授權管理介面，選擇 DRM 的保護方式，進而產生授權 Rule。
2. 此時系統會依授權 Rule，將 DICOM 檔案送至 AES Encrypter 進行加密。
3. 接著 AES Encrypter 會產生一個加密後的 DICOM 檔。
4. 同時，授權 Rule 也會被送進 XML Creator 模組裡，產生一個相對應的授權檔。
5. 這些檔案都將存放在 DRM Server 裡。

在播放介面中的功能:

1. 使用者登入系統時，會向 DRM Server 進行身份驗證。
2. 身份驗證通過之後，會向 DRM Server 取得該使用者有權利閱覽的 DICOM 檔。
3. 同時，使用者也取得相對應的 License 檔。
4. 接著，系統會將授權檔以 XML Parser 來讀取其授權資訊。
5. 取得授權資訊後，也會取得相對應的 Key，此時系統把 DICOM 檔案及 Key 送進 AES decrypter 進行解密。
6. 解密完成之後，會將 DICOM 送進 DICOM Parser 進行檔案的分析與解讀。
7. 解讀完成之後，將被授權閱覽的內容，顯示在畫面上，完成閱覽動作。

各模組的關係如下圖所示:

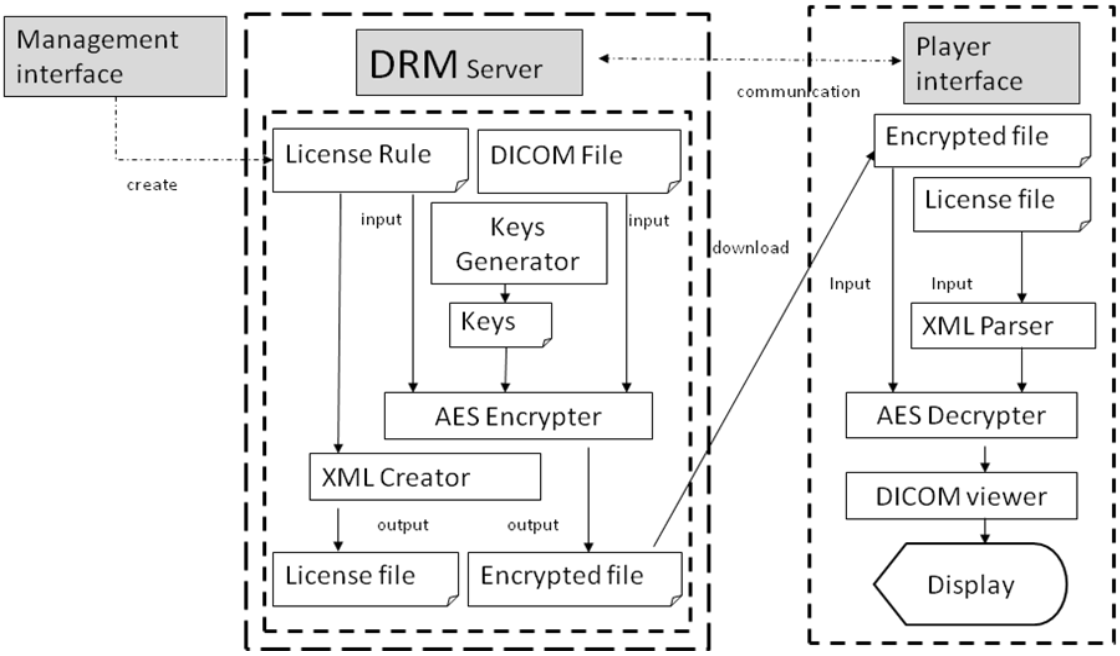

圖 17　各模組的關係

3.5　DICOM 的解析及資料結構

在這一小節中，我們將說明在進行 DICOM 資料處理時，程式內部所使用的資料結構。

程式在進行 DICOM 解析時，會將 DICOM 的 Data Element 轉換成以下結構，以方便進行管理及加密處理。

Structure of Data Element

wGroup 2Bytes	wElement 2Bytes	bExplicit 1Bytes	bStateIndex 1Bytes	bVRLen 1Bytes	bVLLen 1Bytes
VR 4Bytes	VL 4Bytes	e_len 4Bytes	VF 4Bytes	sInfo 4Bytes	Next 4Bytes

圖 18　加密資料結構圖

底下以程式碼的內容進行說明:

表 5　資料結構程式碼

Structure of Data Element

```
PDicomElement = ^TDicomElement;
TDicomElement = record
wGroup          : Word;
wElement        : Word;
bExplicit       : Byte;
bStateIndex : Byte;
bVRLen          : Byte; //value = 2 or 4
bVLLen          : Byte; //value = 2 or 4
VR              : array [0..3] of Byte;
VL              : array [0..3] of Byte;
e_len           : DWord;
VF              : pChar;
sInfo           : string;
Next            : PDicomElement;
end;
```

各欄位說明:

wGroup　：存放 Group 資訊。

wElement　：存放 Element 資訊。

bExplicit　：判斷是否為 Explicit。

bStateIndex：此欄位記錄是否需進行加密。

bVRLen　：此欄位記錄 VR 為 2Bytes 或 4Bytes

bVLLen　：此欄位記錄 VL 為 2Bytes 或 4Bytes

VR　：此欄位記錄 VR 的值。

VL　：此欄位記錄 VL 的值。

e_len　：此欄位記錄 VF 的長度。

VF　：此欄位為一個指向 VF 的指標。

sInfo　：此欄位記錄此 Data Element 的相關資訊及描述。

Next　：此欄位指向下一個 Data Element 節點。

其中在 bExplicit 的部份，如果為 True，則此 Data Element 的格式為{Tag ,VR ,VL ,VF}，若為 False，則代表為 Implicit，則此 Data Element 的格式為{Tag ,VL ,VF}。

3.5.1 加密流程與資料結構的說明

這一小節將說明如何利用我們提出的資料結構，對一個 Data Element 進行加密。首先，由授權管理視窗對某一個要加密的項目進行勾選，此時，在資料結構中的相對應的節點，其中的 bStateIndex 會記錄成需加密的 State，當管理者進行加密確認後，系統會掃瞄所有的 Data Element 節點，判斷其 bStateIndex 並進行加密，在加密時，由於 VF 的長度受到加密而改變，因為，VL 也要跟著修改，而這個加密過的 Data Element，已經無法由其他的播放軟體所識別，所以，我們會連 Tag 也一併修改，最後再將所有修改過後的資料，儲存進入檔案中。完成加密程序。

3.5.2 解密流程與資料結構的說明

依據上述的資料結構圖，解密時，程式會將 DICOM 檔案中的每個 Data Element 進行擷取並存放在資料結構中，並識別每個 Tag 是否為我們加密欄位，如果是，則依據上一小節的解密流程進行解密，解密完成後，還原回原來的 Tag、VL 及 VF，並進行正常 DICOM 的解讀程式。

3.6 DICOM 加解密的限制

在這一小節中，我們將說明 DICOM 在加密時的特性及限制，主要區分成不加密、不單獨加密及需加密等欄位，說明如下：

3.6.1 不加密的項目

由於考慮到相容性問題，如何使加密後的檔案，除了加密的部份，仍能提供給一般播放軟體進行播放，我們的處理方式為某些欄位不進行加密，如 UID 的部份，是為了要關聯 DICOM 之間的檔案，下表列舉了常見的 UID 類型:

表 6　常見的 UID 類型

UIDs
(0002,0002) UI Media Storage SOP Class UID
(0002,0003) UI Media Storage SOP Inst UID
(0002,0010) UI Transfer Syntax UID
(0002,0012) UI Implementation Class UID
(0008,0016) UI SOP Class UID
(0008,0018) UI SOP Instance UID
(0020,000D) UI Study Instance UID
(0020,000E) UI Series Instance UID
(0020,0052) UI Frame of Reference UID

3.6.2 不單獨加密的項目

在描述影像的 Information 部分，屬於不單獨加密的，亦即若影像加密，則這些項目可一併進行加密，若影像不加密，則這些項目不進行加密，如下表所示:

表 7　描述影像的 Data Element

Data Element
(0028,0002) US Samples Per Pixel
(0028,0004) CS Photometric Interpretation
(0028,0010) US Rows
(0028,0011) US Columns
(0028,0030) DS Pixel Spacing
(0028,0100) US Bits Allocated
(0028,0101) US Bits Stored
(0028,0102) US High Bit
(0028,0103) US Pixel Representation
(0028,0120) SS Pixel Padding Value

3.6.3 需加密的項目

如隱私資料及某些可依據 Frame 的 ID 追蹤到病人相關資料的項目等等。

3.7　Key 的設定策略

在進行加密時，會動態的產生 AES 的 Key，但由於 Key 的策略不同，所產生的應用也不同，底下分別說明 Key 的不同應用策略。

1. 使用相同的 AES Key，對所有欄位進行加密:

   此種作法較為簡單，意即使用者只要擁有其 Private Key，就可以解開所有的欄位，適用於 DICOM 檔案不再進行轉移的情況。

2. 使用不同的 AES Key，分別對各欄位進行加密:

   此種作法為每加密一個欄位，即使用不同的 AES Key，這樣做的好處是可以讓使用者再行將檔案轉移給其他人，因為使用了不同的 AES Key，所以只要將特定欄位的 AES Key 一併進行轉移即可，因為每個加密的欄位所使用的 AES Key 不同，所以受轉移者也無法開啟其他加密的欄位。

3.8 加密流程

在這一小節中，更加詳細的說明在授權管理視窗中，進行加密的步驟。

1. 系統隨機產生一組 128bit 的 AES Key。
2. 此時系統將 DICOM 及 Key 送進 AES Encrypter 中，進行加密。
3. AES Encrypter 將會產生一個被加密後的 DICOM 檔。
4. 在步驟 1 所產生的 128 bit AES Key，也同時送進了 RSA Encrypter 中。
5. 系統此時會取得被授權者的 Public Key。
6. RSA Encrypter 利用 Public Key，將 128 bit 的 AES Key 進行加密，並將加密後的資料，記載在授權檔中。

步驟如下圖所示：

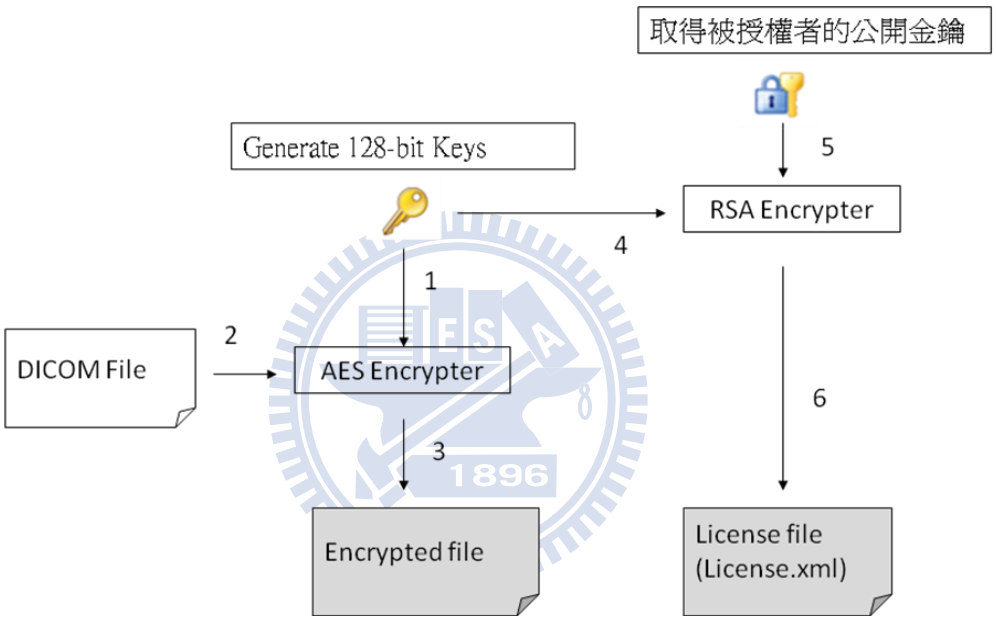

圖 19 加密流程

3.9 解密流程

在這一小節中，詳細的說明解密的步驟。

1. 系統取得被授權者的 Private Key。
2. 此時系統將 License 檔及 Private Key 送進 RSA decrypter 中，進行解密。
3. 解密完成後，RSA decrypter 將會取得授權 Rule 及 128 bit 的 AES Key。
4. 接著系統將 AES Key 送進 AES decrypter 中。
5. 同時也將被加密過的 DICOM 檔案送進 AES decrypter 中，進行解密。
6. 最後解密完成，得到明文的 DICOM 檔案。

步驟如下圖所示：

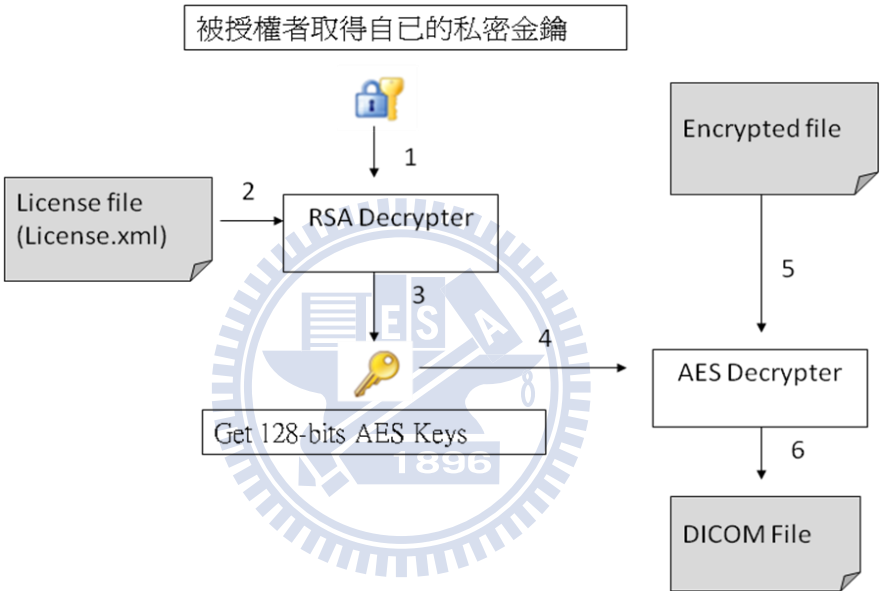

圖 20 解密流程

3.10 授權檔(License.xml)

授權檔是依據 World Wide Web Consortium (W3C)的格式制作，內容中說明了加密方式及 Key Info 等資料，意即此授權檔不僅可供我們制作的播放器能夠播放，只要是能夠解讀 W3C 的格式的播放器，即可以共通的語言來取得 Key 及對所保護的 DICOM 進行解密。這功能使程式在未來更有相容性及擴充性。

在 Key 的使用上，我們採用了 AES Keys 對 DICOM 內容進行加密，並使用 RSA 加密方法再將 AES Keys 進行加密。在 AES Key 的使用上，因為 Key 的運用策略的不同，可以使用一組 AES Key，也可以使用多組 AES Keys；一組 Key 以下面方式表示:

<CipherData>

<CipherValue>sr4f4dbv7KSvibb…</CipherValue>

</CipherData>

下圖為一個授權檔的簡略內容，可以看出多組 AES Keys 使用 RSA 的加密情形。

```
<?xml version="1.0" standalone="no"?>
<article>
<EncryptedData Type= "http://www.w3.org/2001/04/xmlenc#Element"
        xmlns= "http://www.w3.org/2001/04/xmlenc#" >
<EncryptionMethod Algorithm= "http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
<KeyInfo xmlns= "http://www.w3.org/2000/09/xmldsig#" >
 <EncryptedKey xmlns= "http://www.w3.org/2001/04/xmlenc#" >
   <EncryptionMethod Algorithm= "http://www.w3.org/2001/04/xmlenc#rsa-1_5" />
   <KeyInfo xmlns= "http://www.w3.org/2000/09/xmldsig#" >
        <KeyName>sessionkey</KeyName>
   </KeyInfo>
   <CipherData>
        <CipherValue>sr4f4dbv7KSvibb...</CipherValue>
   </CipherData>
   <CipherData>
        <CipherValue>sKcimeshf7dkxk...</CipherValue>
   </CipherData>
   </EncryptedKey>
   </KeyInfo>
   <CipherData>
        <CipherValue>2g5sGNhKqMRFd...</CipherValue>
   </CipherData>
</EncryptedData>
</article>
```

圖 21　授權檔格式

3.11 授權管理視窗流程圖

下圖為授權管理視窗的流程圖:

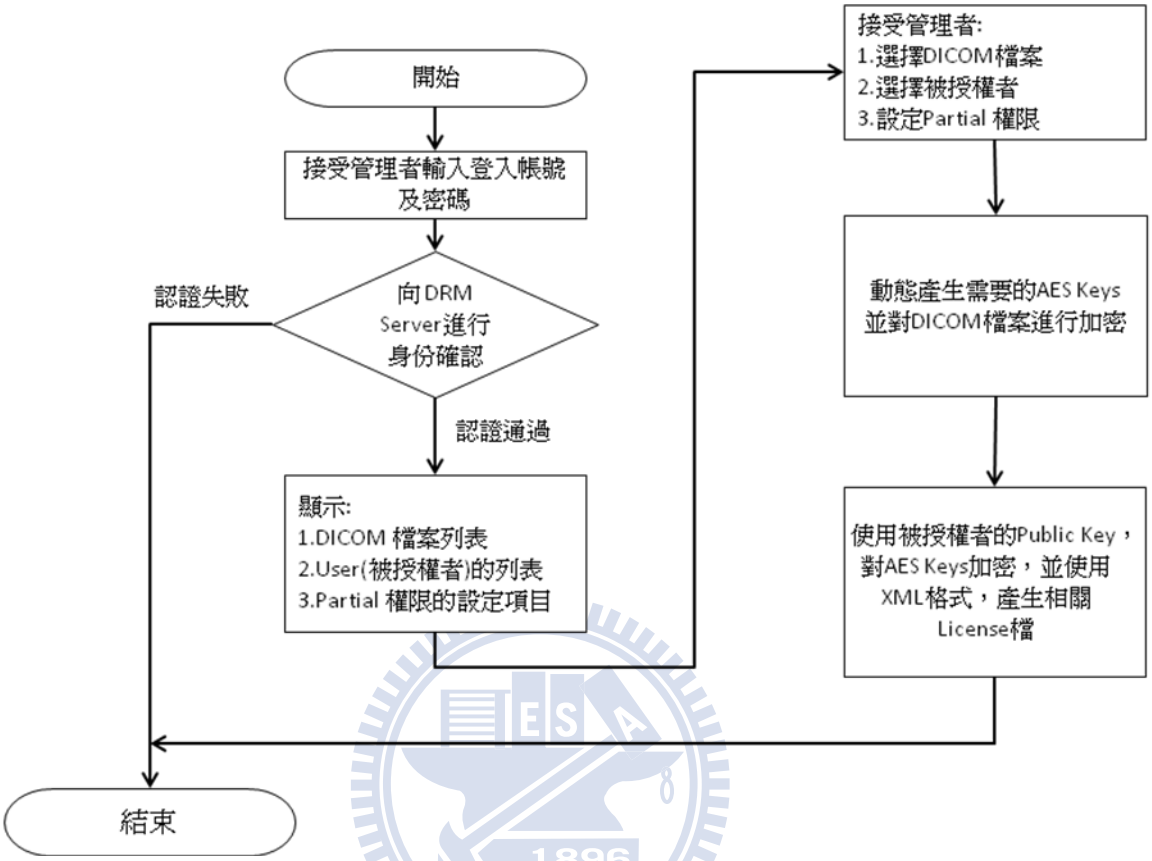

圖 22 授權管理視窗流程圖

3.12 播放視窗流程圖

下圖為播放視窗的流程圖:

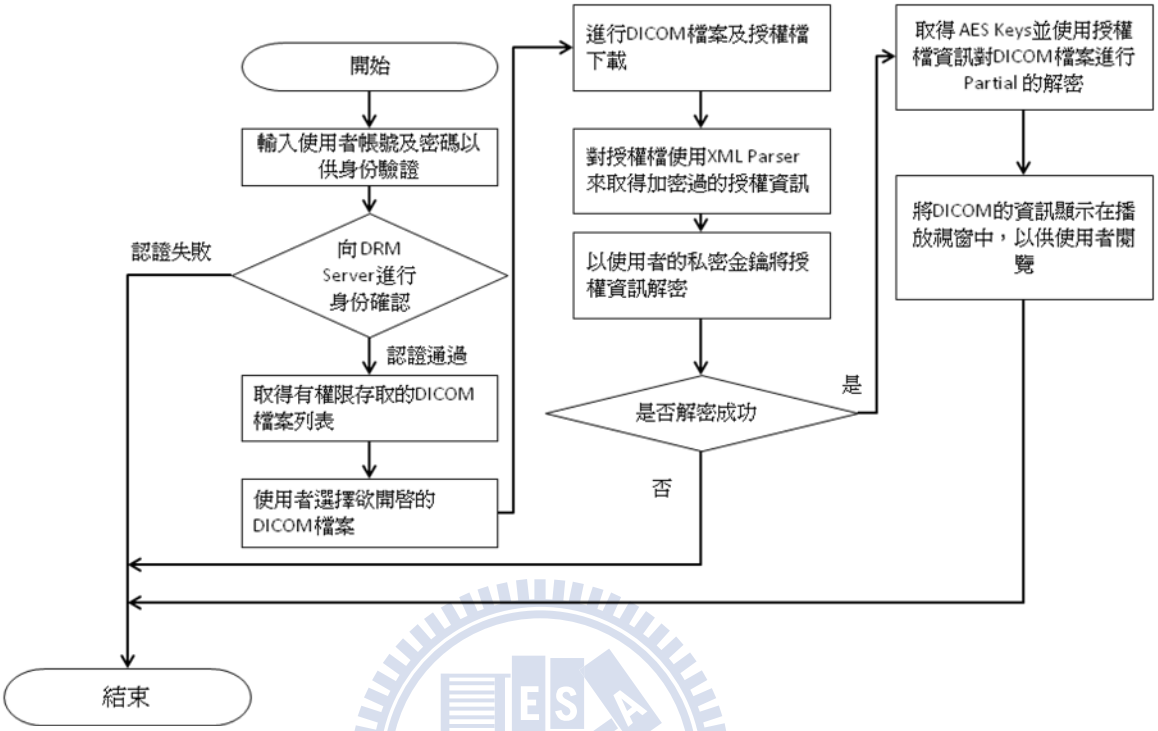

圖 23　播放視窗流程圖

3.13 Sequence Diagram

下圖為 Sequence Diagram，說明如下:

1.管理者進入授權管理視窗

2.管理者輸入帳號密碼，此時授權管理視窗會向 DRM Server 進行身份驗證。

3.DRM Server 確認身份後，回報給授權管理視窗。

4.授權管理視窗允許管理者登入。

5.管理者設定完 DRM 或 Partial DRM 的權限後，授權管理視窗會將授權設定及加密過的檔案存放在 DRM Server 上。

6.使用者從播放視窗中，輸入帳號密碼。

7.此時播放視窗會向 DRM Server 進行身份驗證。

8.DRM Server 確認身份後，回報給播放視窗。

9.使用者登入後，向播放視窗要求播放某個 DICOM 檔案。

10.播放視窗向 DRM Server 提出要求，並同時下載 DICOM 檔案及授權檔。

11.播放視窗對 DICOM 進行解密及播放。

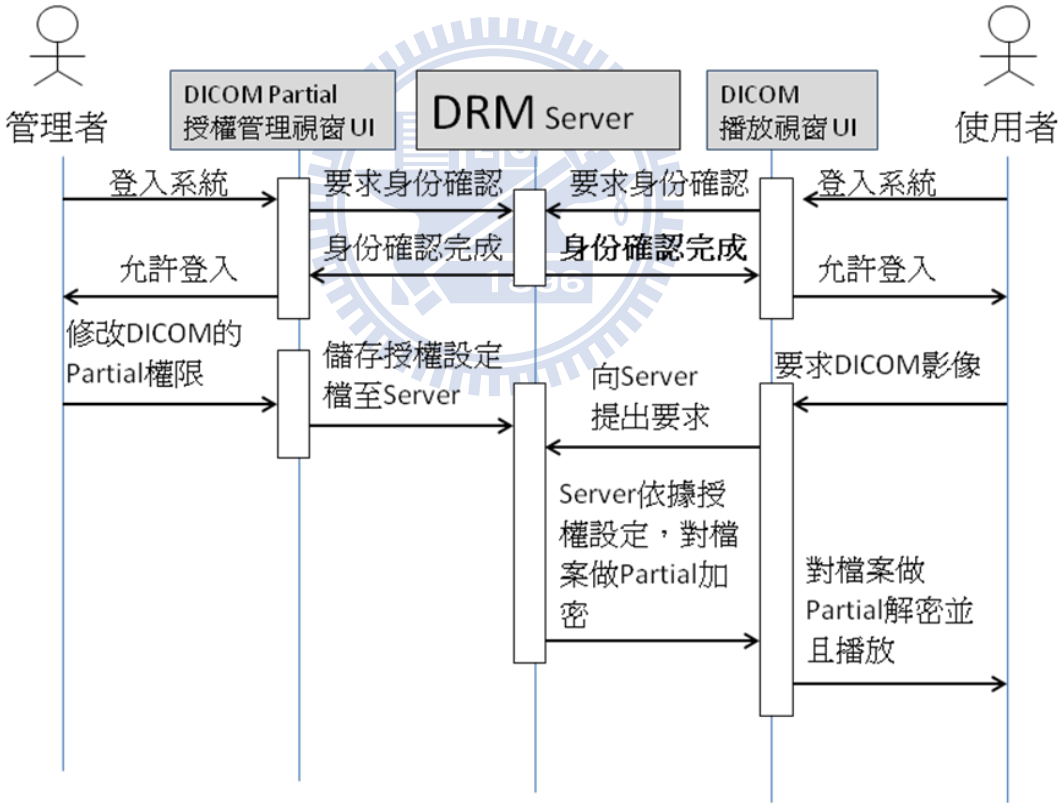

圖 24 Sequence Diagram

以上就完成了整個系統的設計。

四、討論

4.1 相容性問題探討

由於對 DICOM 進行 Partial 加密之後，為了使未被加密的部份，依然可以被一般 DICOM 播放軟體進行播放，我們將系統做了底下的設計:

1.我們將加密的部份，採用自訂欄位的方式(可參照 3.5.1 節說明)，讓一般播放軟體能夠正常取得，並視之為其他二進制資料，進而繼續 Parsing 其餘資料，不會造成解讀的困擾。

2. 我們將 DICOM 的 Data Element 轉換成 3.5.1 節所描述的結構，加密時，由於被加密的資料長度會改變(變成 128 bit 的倍數，因為我們使用 AES 128bits 加密的關係，若使用 AES 256bits，則為 256bit 的倍數，其他加密方法同理)，因此，在 Data Element 內部的長度欄位，也需跟著修正，進行相關欄位的調整，轉換成另一個加密後仍符合 Data Element 定義的結構，因此最終被 Partial DRM 加密過後的整個 DICOM 檔案，依然可以相容於其他軟體。

4.2 Key 的設定探討

我們使用 AES Key 進行 DICOM 檔案的 Partial 加密，然而，是否需對不同的欄位，使用不同的 Key 進行加密，應視其應用上的需要，當被授權的檔案有再轉移他人的需求時，使用不同的 Key 進行加密是較好的作法(可參照 3.7 節說明)。

使用多組 Key 時，適合的運用環境如應用於 E-learning, E-library，病歷移轉等等具轉移性的應用，因此，多 Key 的使用策略提供了多層次和多種應用的環境。

五、實作展示

5.1 展示說明

在我們的展示中，我們會說明我們提供的三種保護方式，以及它們的不同:

1. DRM:這種保護模式與傳統的 DRM 保護模式相同。
2. Partial DRM:這種保護模式就是我們所提出來的方法，我們可依不同的應用需求，來對特定項目做保護，在展示中有列出的項目，只是為了展示用途所列出的項目，並非只能對這些項目做保護，實際應用時，可增刪其中的項目來符合實際需求。
3. No Protection:這個模式即為完全不保護的方式。

上面所述可對照底下的圖片，將會更清楚了解我們要展示的內容。

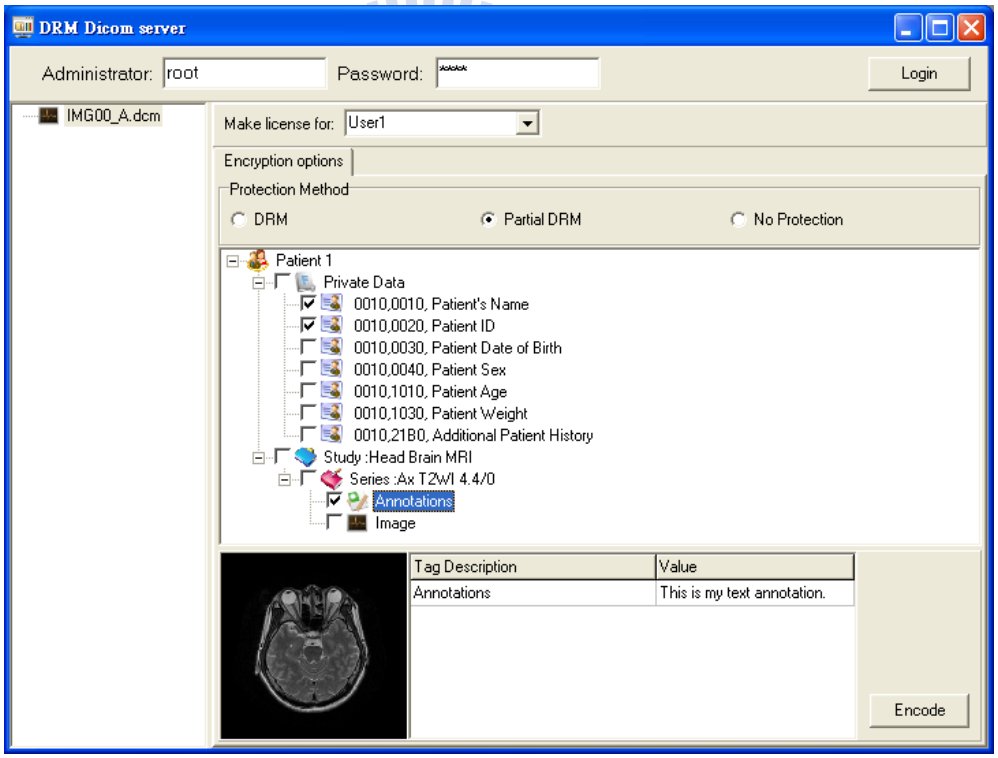

圖 25 展示說明

5.2 授權管理畫面操作說明

在這一節裡，我們主要介紹管理者如何在系統中設定 DICOM 檔案的授權方式、授權對象及 Partial DRM 對個別項目的授權選擇方式。

5.2.1 登入授權管理程式

1.輸入管理者帳號密碼。

2.點選 Login 進行登入。此時，系統會進行管理者的身份確認。

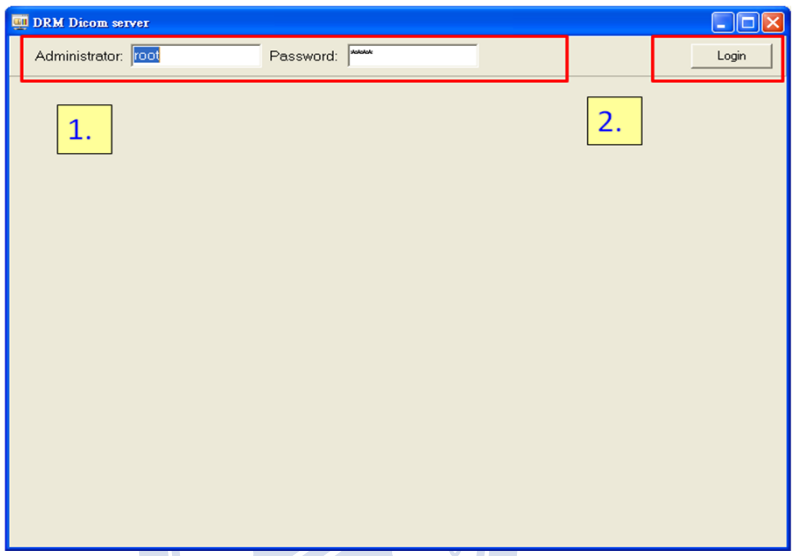

圖 26 登入授權管理程式

5.2.2 完成登入

1.身份確認完成後，系統顯示登入成功訊息。

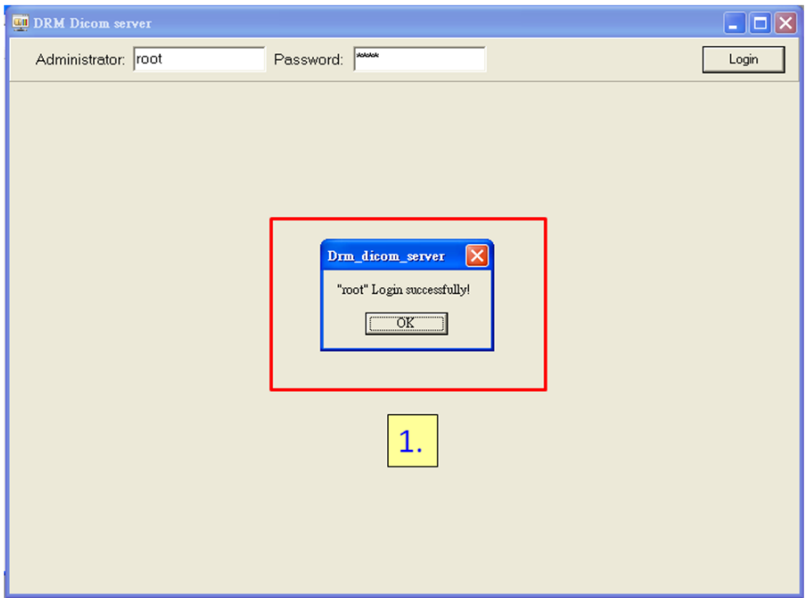

圖 27 顯示登入成功訊息

5.2.3 顯示 DICOM 列表

1.系統顯示出可供使用的 DICOM 列表。

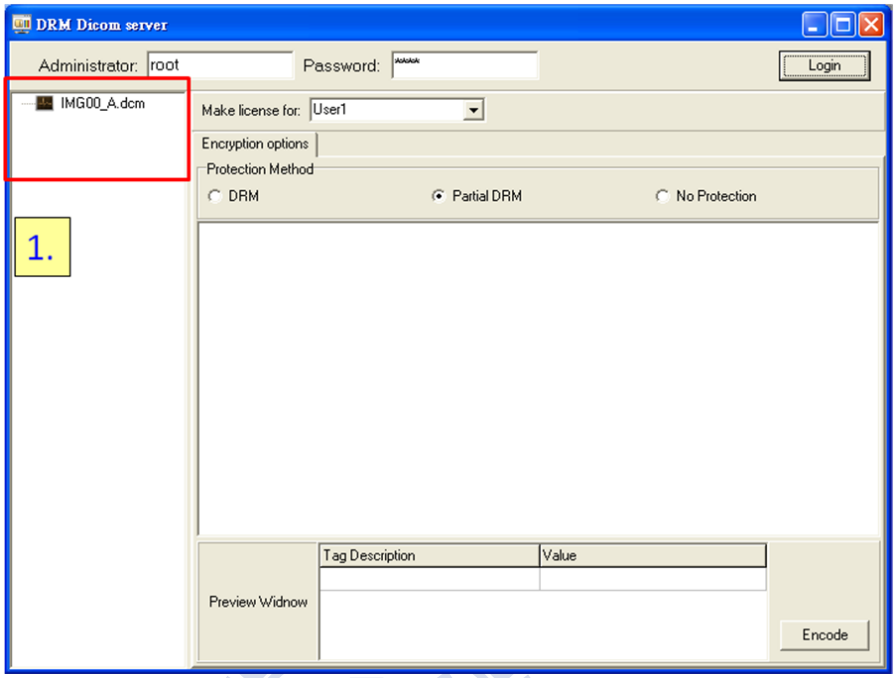

圖 28　顯示 DICOM 檔案列表

5.2.4 選擇要授權的 DI COM 檔案

1. 選擇要進行設定的 DICOM 檔案。
2. 選擇後，中央的視窗會列出 DICOM 的內部資訊。

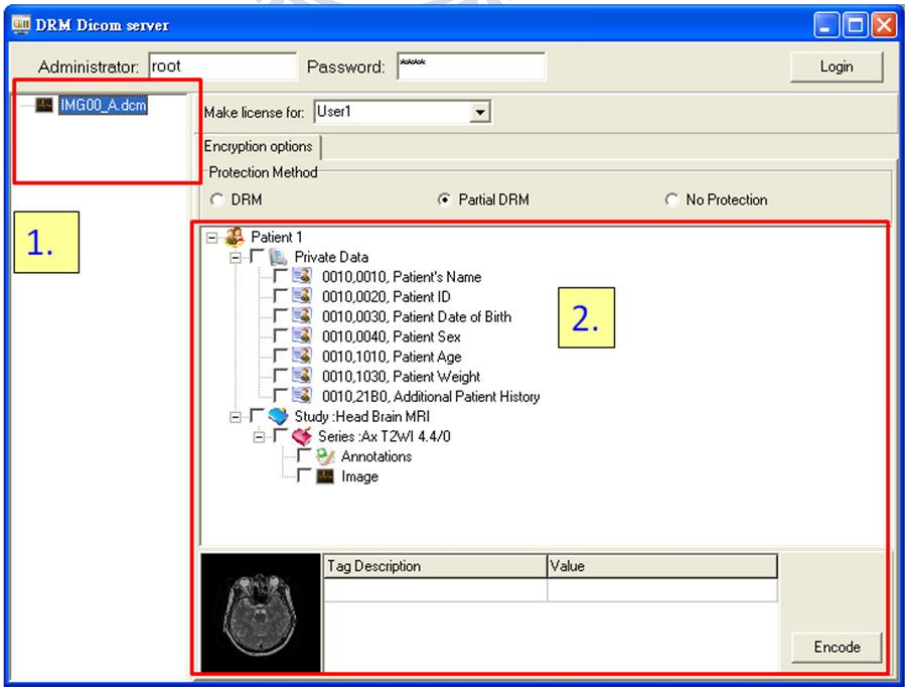

圖 29　顯示 DICOM 內部資訊

5.2.5 選擇要授權的 DI COM 檔案

1. 選擇要將此所選擇的 DICOM，授權給哪個使用者。

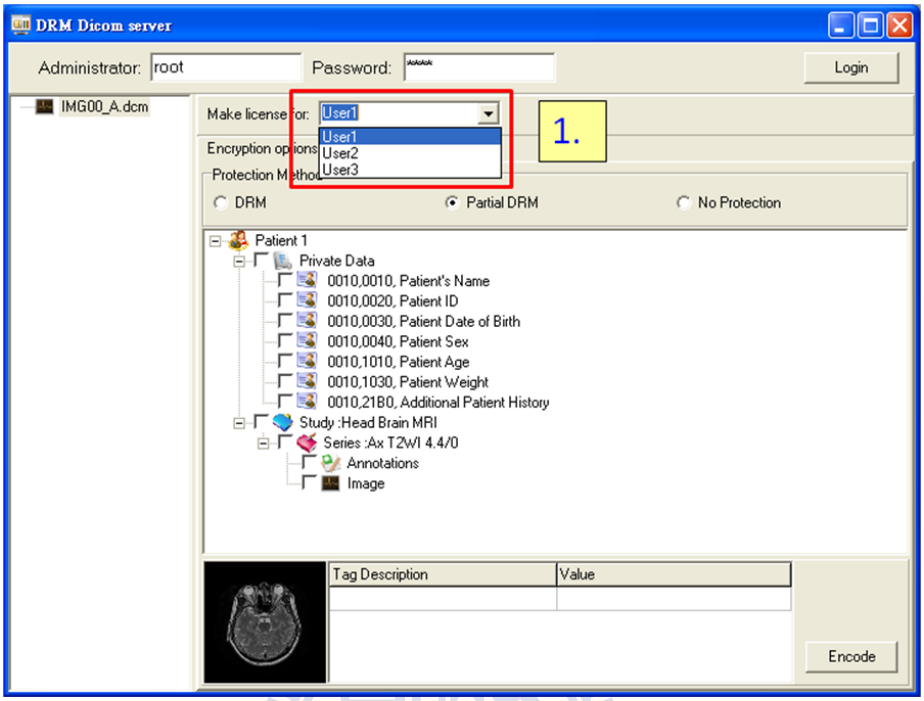

圖 30　選擇被授權者

5.2.6 選擇要保護的模式 1

1. 當選擇 DRM 保護時，所有項目都將加密保護。
2. 項目前方的 ICON 都變成了”上鎖”的圖示。

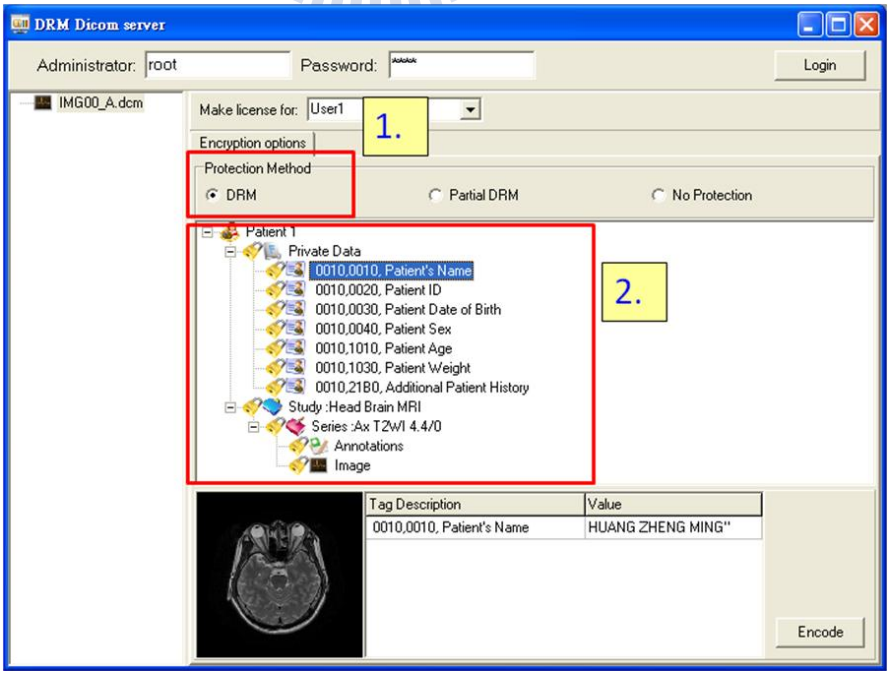

圖 31　保護模式 - DRM

5.2.7 選擇要保護的模式 2

1. 選擇 Partial DRM 的保護模式
2. 此時可針對要保護的項目，個別進行選擇
3. 選定項目的預覽窗格

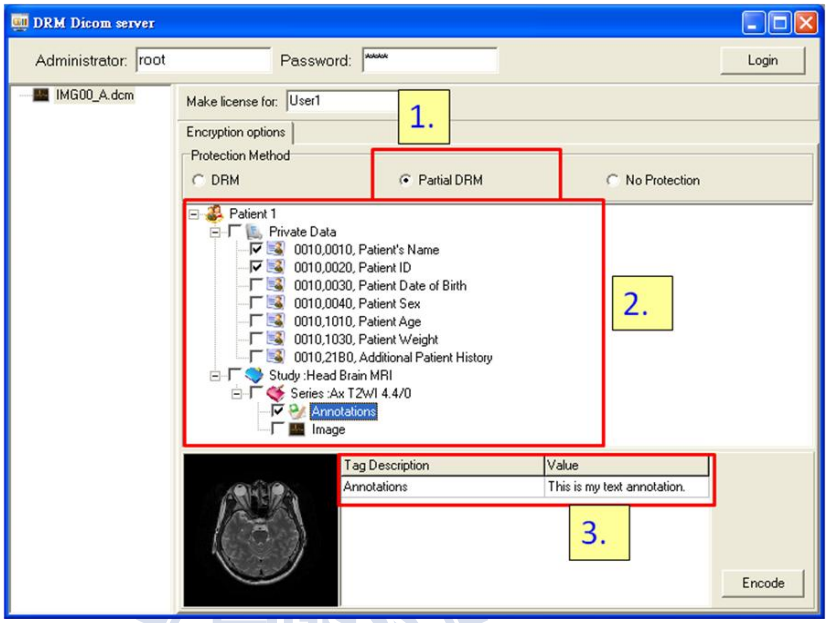

圖 32　保護模式 - Partial DRM

5.2.8 選擇要保護的模式 3

1. 選擇不進行保護的模式
2. 項目前方的 ICON 都變成了”開鎖”的圖示

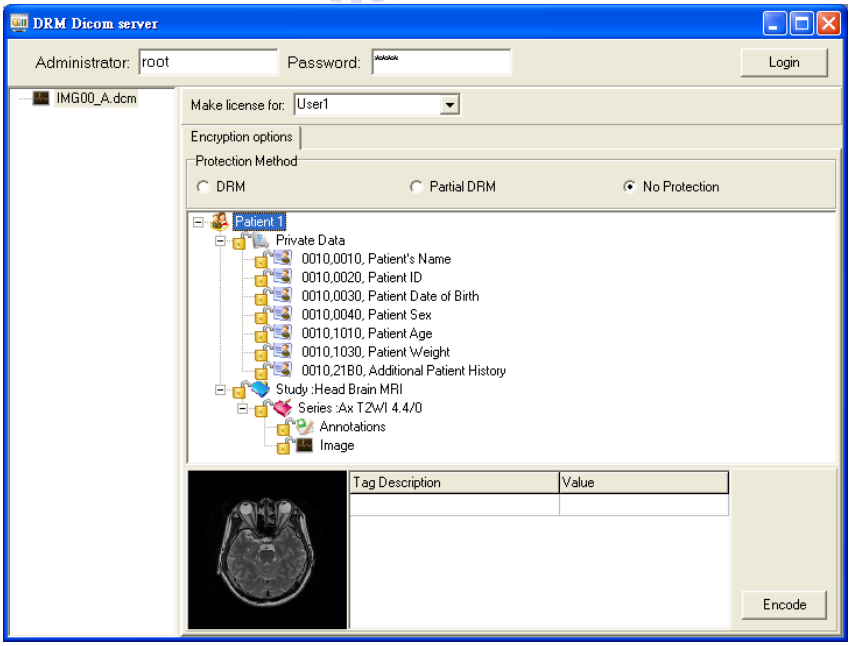

圖 33　保護模式 - 不進行保護

5.2.9 進行加密編碼

1. 選擇完畢後，進行加密編碼

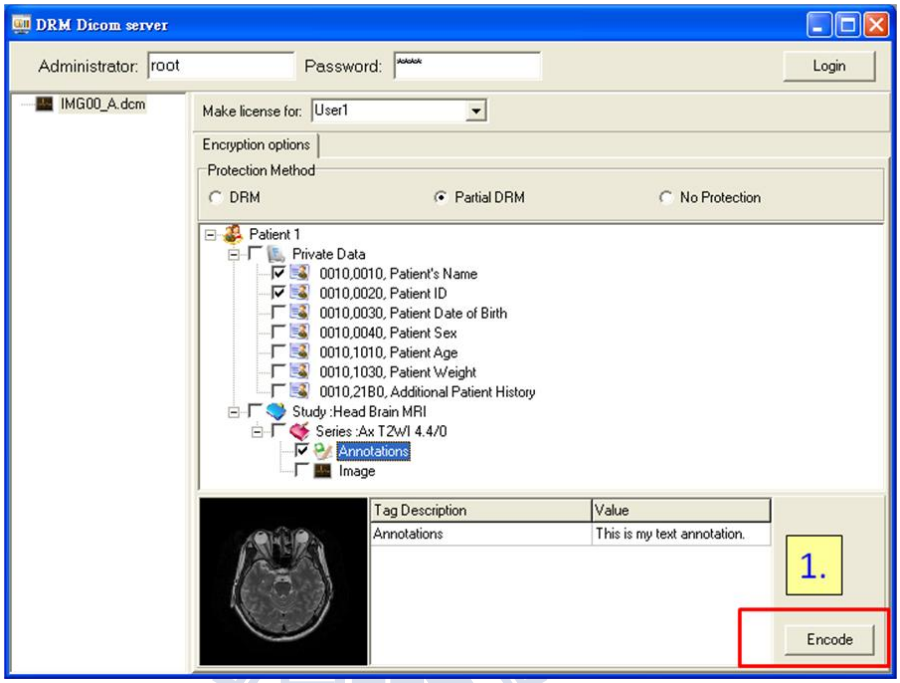

圖 34　執行加密編碼

5.2.10 完成加密編碼

1. 顯示加密編碼完成訊息

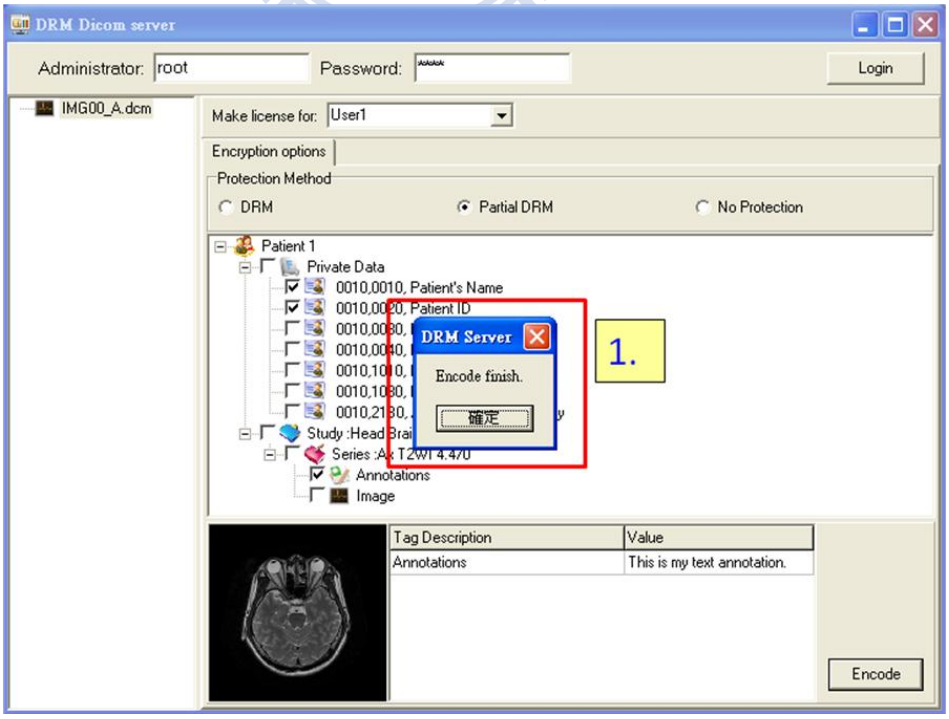

圖 35　加密編碼完成訊息

5.3 播放畫面操作說明

在這一節裡，我們將以使用者的身份，瀏覽被授權的檔案內容。

5.3.1 連線至 DRM Server

1. 設定欲連線的 DRM Server。

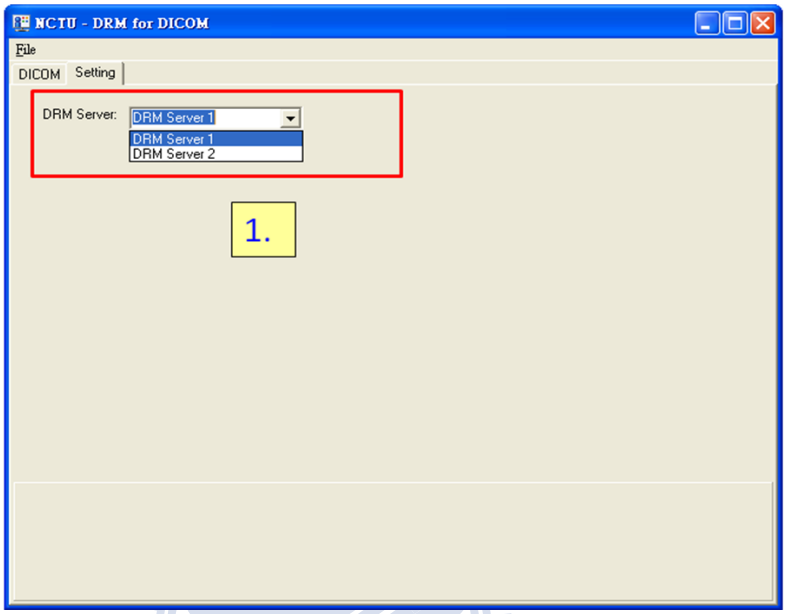

圖 36 選擇 DRM Server

5.3.2 選擇使用者帳號

1. 輸入使用者帳號及密碼以供身份驗證。
2. 向 DRM Server 取得被授權的 DICOM 清單

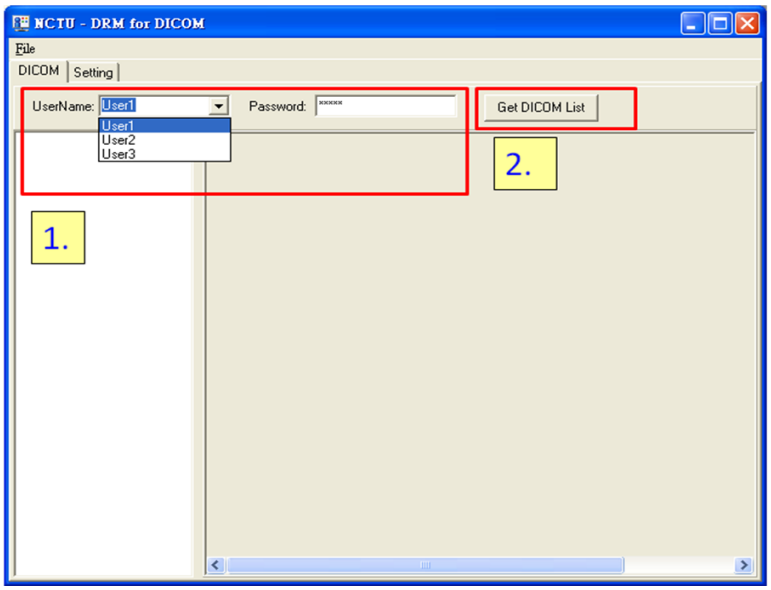

圖 37 使用者登入

5.3.3 選擇 DICOM 檔案

1. 選擇要下載的 DICOM 檔案，進行下載。

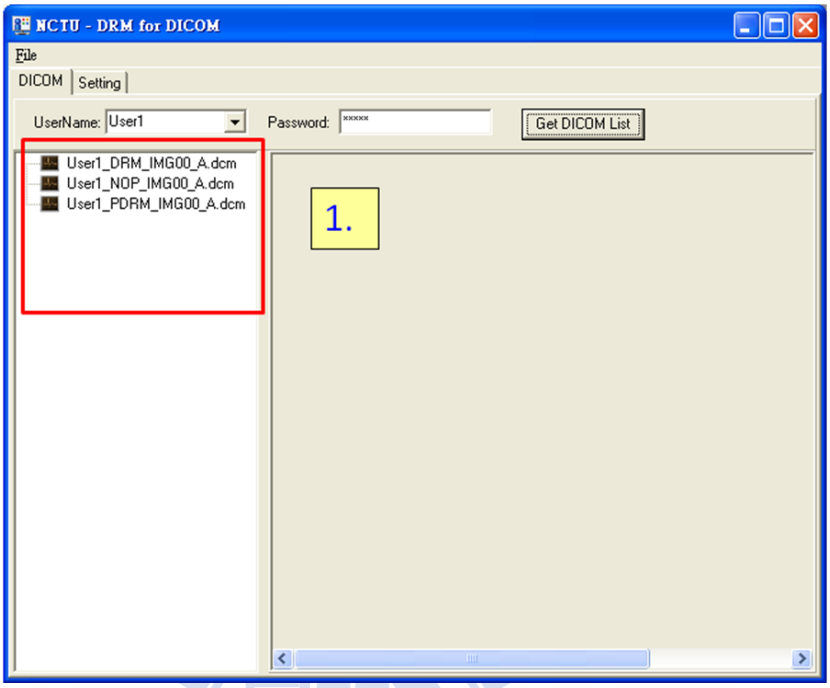

圖 38　選擇 DICOM 檔案

5.3.4 進行檔案下載

1. 下載完成後，系統提示下載成功。

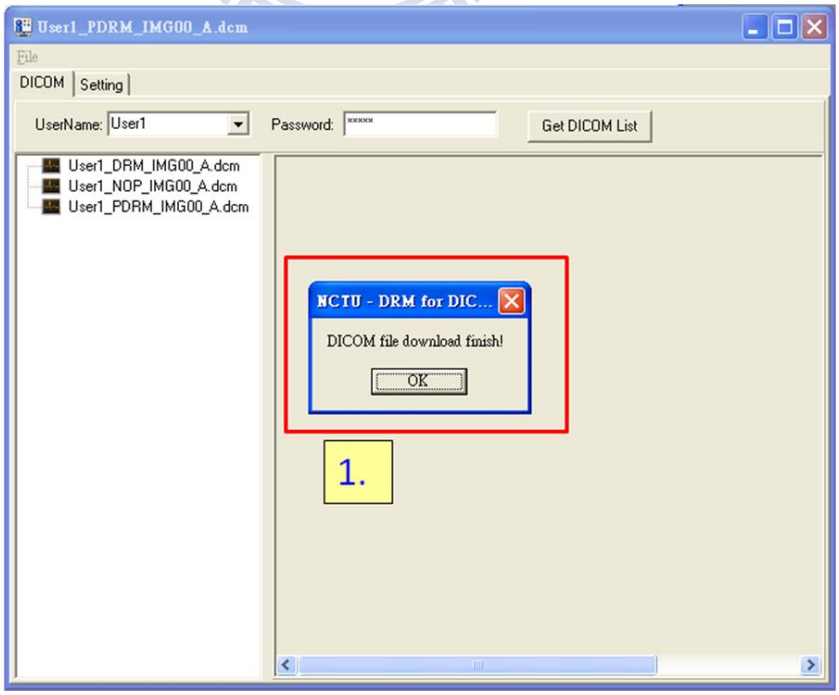

圖 39　下載完成訊息

5.3.5 進行授權檔下載

1. 系統詢問是否下載 License 授權檔。

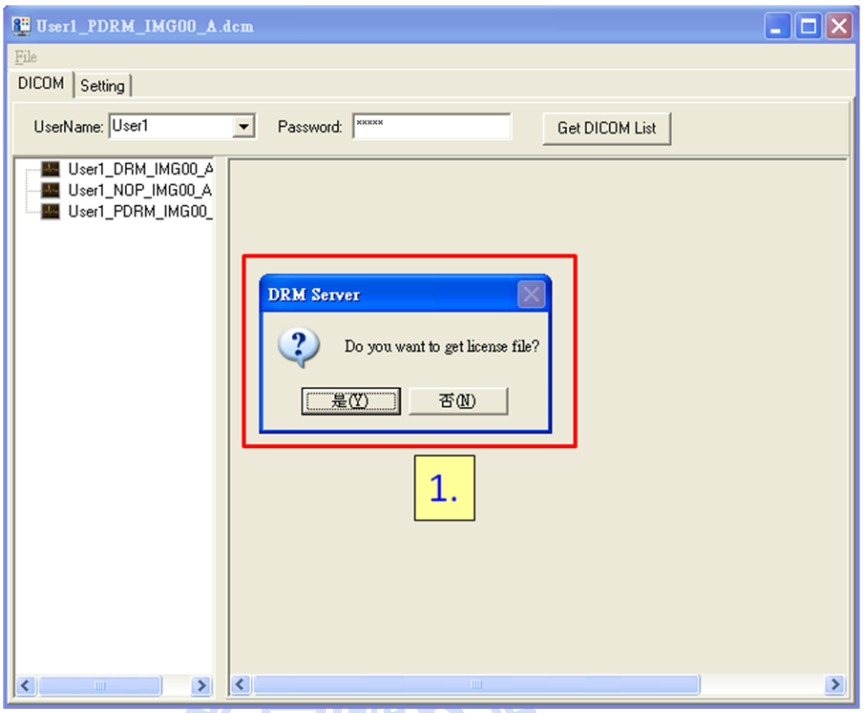

圖 40　下載授權檔

5.3.6 未取得授權畫面

1. 如果 step 4 選擇不取得授權檔，則被保護的項目將無法解密(以 Encrypted 顯示)。

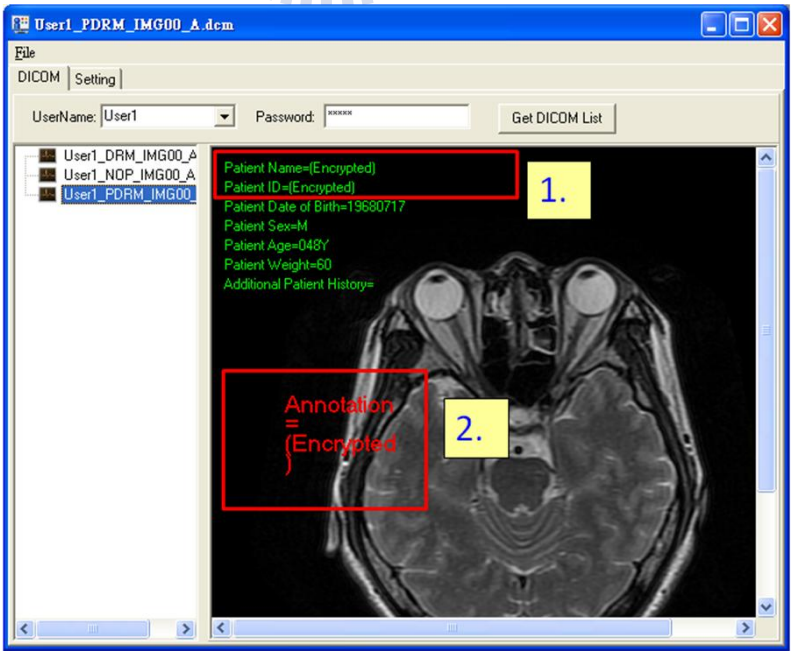

圖 41　瀏覽時以 Partial 的方式顯示

5.3.7 取得授權畫面

1. 如果 step 4 選擇下載授權檔，則系統會以 Private Key 將授權資訊解密並取得 AES Key。

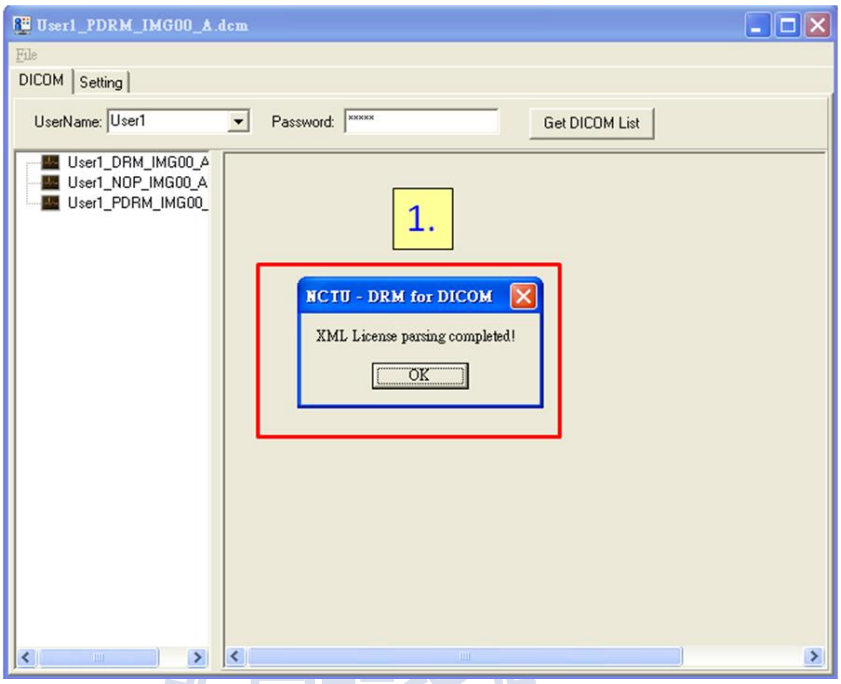

圖 42 授權檔取得成功訊息

5.3.8 進行解密

1. 系統取得 AES Key 後，對受保護的部份，進行解密。

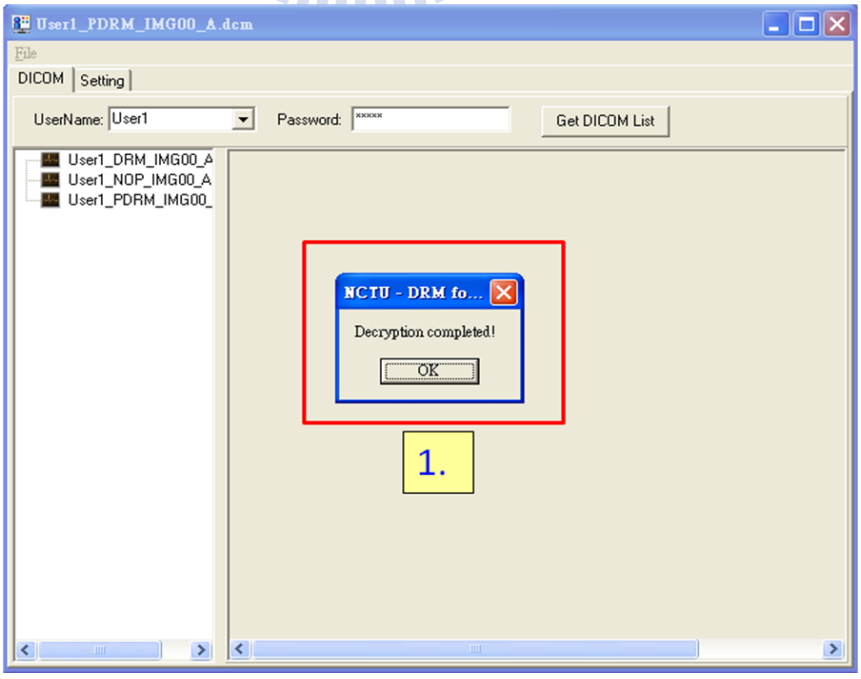

圖 43 解密完成訊息

5.3.9 顯示畫面

1. 解密完成之後，系統依照授權資訊，顯示出被授權觀看的內容。

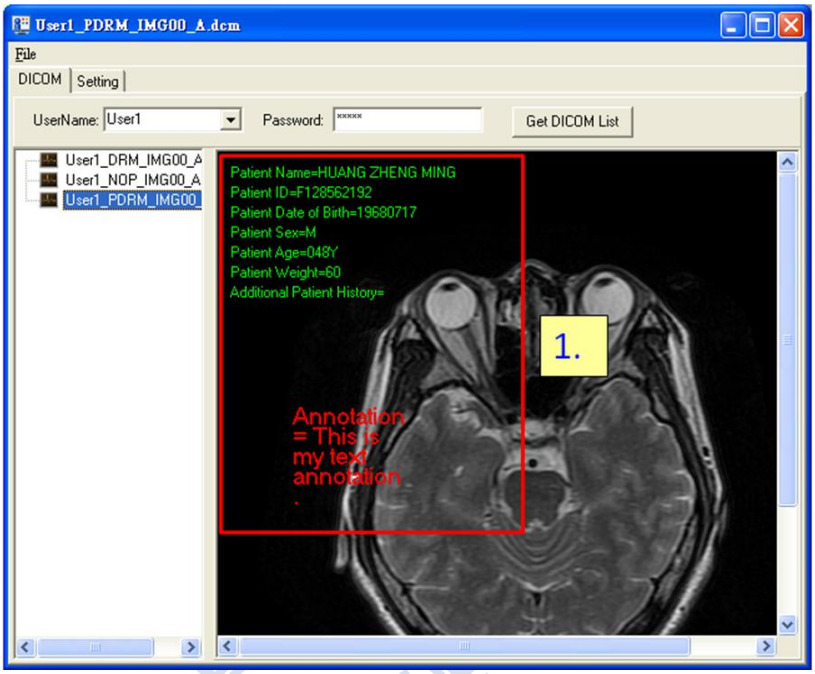

圖 44 顯示所有授權內容

六、結論

6.1 總結

傳統的 DRM 機制對數位內容的保護是在全有與全無間的管理，而 Partial DRM 機制提供了更多的彈性使能夠分別對各模組進行版權保護。

將 DICOM 做了局部性保護機制後，可提供更多的應用，如：

1. 醫療教學平台(Medical E-Learning):

2. 病歷資料可攜帶/移轉性(Transferring)

6.2 未來發展方向

Partial DRM 的機制不僅能夠運用在 DICOM 的保護上,也能夠應用在其他不同的領域中，使版權保護的運用更加的靈活，來符合真實世界的需求，我們提出以下可以繼續發展的方向，如:

表 8 未來發展方向

名稱	**希望達到的保護方式(例子)**
數位試題	開放題目閱覽，加密保護解題的答案
電子書	只對某些特定的章節保護。
數位報紙	只開放體育版或是綜藝版。
數位多媒體內容	開放部份功能試用。
其他…	

REFERENCES

[1] Digital Imaging and Communications in Medicine (DICOM), NEMA Publications," DICOM strategic document," Ver. 8.0, April 2008, available at: http://medical.nema.org/dicom/geninfo/Strategy.pdf

[2] Peter Mildenberger, Marco Eichelberg, Eric Martin "Introduction to the DICOM standard," European Radiology, Vol. 12, No. 4, April 2002, pp. 920-927

[3] W. Dean Bidgood, Jr., MD, MS, Steven C. Horii, MD, Fred W. Prior, PhD, and Donald E. Van Syckle, "Understanding and Using DICOM, the Dana Interchange Standard for Biomedical Imaging", Journal of the American Medical Informatics Association, Vol. 4, No. 3, May 1997, pp. 199-212

[4] Steven C. Horiil, Fred W. Prior, W. Dean Bidgood, Jr., Charles Parisot, Geert Claeys, "DICOM: An Introduction to the Standard", 1994, available at: http://www.csd.uoc.gr/~hy544/mini_projects/Project8/DICOM%20(Paper_Parisot).doc

[5] Kelly Welch, "Digital Imaging and Communications in Medicine: DICOM", April 2004,available at: http://www.engineering.uiowa.edu/~bme_285/Misc/Project1/WelchDICOM2.doc

[6] Digital Imaging and Communications in Medicine (DICOM), NEMA Publications,"WORKING GROUPS of the DICOM Standards Committee", 2002, available at: ftp://medical.nema.org/medical/dicom/Geninfo

[7] Digital Imaging and Communications in Medicine (DICOM), NEMA Publications, "DICOM Standard", 2008, available at: ftp://medical.nema.org/medical/dicom/2008

[8] R.N.J. Graham, R.W. Perriss, A.F. Scarsbrook,"DICOM demystified: A review of digital file formats and their use in radiological practice",Clinical Radiology, Vol. 60, June 2005, pp.1133-1140

[9] U. S. 104th Congress, Health Insurance Portability and Accountability Act, Public Law 104-191, Aug. 21, 1996

[10] Julien Kunzi; M. Petkovic; Paul Koster, “Data-centric protection in DICOM”, Proc. Of Medical Imaging 2009: Advanced PACS-based Imaging Informatics and Therapeutic Applications, SPIE, 2009.

[11] Bogdan C. Popescu,Frank L.A.J. Kamperman,Bruno Crispo,Andrew S. Tanenbaum, “A DRM Security Architecture for Home Networks”, The 4th ACM Workshop On Digital Rights Management, pp.1 - 10, 2004.

[12] Bill Rosenblatt, Gail Dykstra, “Integrating Content Management with Digital Rights Management – Imperatives and Opportunities for Digital Content Lifecycles”, GiantSteps Media Technology Strategies and Dykstra Research, May 2003.

[13] Srijith K. Nair, Bogdan C. Popescu, Chandana Gamage, Bruno Crispo and Andrew S.Tanenbaum, ”Enabling DRM-preserving Digital Content Redistribution”, Proceedings of the Seventh IEEE International Conference on E-Commerce Technology, pp.151–158,

July 19-22 2005.

[14] Sam Michiels, Kristof Verslype, Wouter Joosen, Bart De Decker, “Towards a Software Architecture for DRM”, In Proceedings of the 14th ACM Workshop on Digital Rights Management, pp. 65–74, 2005.

[15] L. J. Camp, “First Principles of Copyright for DRM Design”, IEEE Internet Computing, vol.7, pp.59-65, May-June 2003.

[16] Gyorgy Kalman and J. Noll, “Right management infrastructure for home content”, in Proceedings of the 16th IST Mobile and Wireless Summit, pp.1–5, July 1-5 2007

[17] G. Hanaoka, K. Ogawa, I. Murota, G. Ohtake, K. Majima, S.Gohshi, K. Oyamada, S. Namba, and H. Imai, “Managing Encryption and Key Publication Independently in Digital Rights Management Systems”, IEICE Trans. On Fundamentals of Electronics, Communications, and Computer Sciences, vol.E87-A, no.1, January 2004.

[18] Deirdre K. Mulligan,John Han,Aaron J. Burstein,, “How DRM Based Content Delivery Systems Disrupt Expectations of Personal Use”, Proc. 2003 ACM Works. Digital Rights Management, pp.77-88, October 2003.