# 壹、簡介

隨著網際網路的快速發展與普及，愈來愈多人習慣將資料儲存在網際網路上，包含個人私密資料與商業重要資訊等。爲了提供使用者安全的資訊傳送管道，機密檔案的保護議題受到的廣泛討論與研究。一般常用的機密資料保護機制爲加密技術（encryption）與隱藏技術（steganography），加密技術主要運作方式是利用一個加密演算法，將所要保護的重要資料轉換成一串看似亂七八糟無意義的密文，讓一般使用者無法從密文中看到其包含的資訊內容，而預期接收者可利用密鑰與解密演算法還原資訊內容；隱藏技術主要運作的方式爲將所要保護的資料嵌入遮蔽媒體物件（cover object）中，如文字、聲音、圖像、動畫等，形成一個僞裝媒體物件（stego-object），這個僞裝媒體片段就如同一般媒體片段一樣被傳送儲存與使用，一般人看到它就如同平常使用的媒體物件沒什麼差異；然而，預期接收者得到僞裝媒體物件後，則可利用資料取出演算法將重要資料從僞裝物中取出。藉由遮蔽媒體物件的掩護讓人察覺不出重要資料的存在性，來達到保護這些重要資料的目的。

在網際網路上存放資料，一般使用者爲了貪圖方便或擔心忘記資料存放位置，常會習慣將資料儲存在同一空間，利用集中式來保管資料。然而一旦這些資料因某些原因遭到破壞或遺失，資料就會無法還原而導致永久遺失。一般來說，上述情況可藉由將機密資料複製多份並分別存放在不同的位置，來降低資料遺失風險，但這也易造成資料因分存多處導致不連續性，同時讓機密資料遭到破解的可能性也會增加。機密分享（secret sharing）技術（Naor & Shamir, 1995; Shamir, 1979）爲解決上述問題的一項機制，在一個 $(t, n)$ 門檻式機密分享方法上，係利用一個分享演算法將資料編碼成爲 $n$ 份分存資料（share data），每份分存資料可分別傳輸或儲存。當使用者取得少於 $t$ 份分存資料時，是無法得到關於原機密資料的任何資訊，而在取得其中 $t(2 \le t \le n)$ 份或更多分存資料時，即可回復原始的機密資料（Asmuth & Bloom, 1983; Blakley, 1979）。在這樣的機制下，當某些分存資料被竊取或複製，也不會造成機密資料的洩密或破壞。且在 $n - t$ 份分存資料遺失的狀況下，使用者仍可利用剩餘的 $t$ 份分存資料來還原出原機密資料。這項技術解決機密資料集中儲存容易損毀的缺點，也提高了機密資訊保護的容錯性與安全性。

在早期文獻中的機密分享技術，以探討數值資料的保護爲主（Asmuth & Bloom, 1983; Beimel & Chor, 1998; Blakley, 1979; Shamir, 1979; Wang, Zhang, Ma, & Li, 2007; Wang & Wong, 2008），其大部分在探討加密系統中密鑰的保

護機制，研究方向著重在設計出更安全的分享機制與彈性化的存取結構。而在近年來，隨著網際網路的普及與數位多媒體資料的廣泛被使用與傳播，許多專家學者也投入多媒體資料的分享研究，其大都以二維影像的研究爲主，且已有不錯的研究成果（Asmuth & Bloom, 1983; Beimel & Chor, 1998; Blakley, 1979; Chang, Hsieh, & Lin, 2008; Lin & Tsai, 2004; Lin & Chan, 2010; Lin, Lee, & Chang, 2009; Shamir, 1979; Thien & Lin, 2002; Wang et al., 2007; Wang & Wong, 2008; Wang, Chien, & Lin, 2010; Wang & Shyu, 2007; Wang & Su, 2006; Yang, Chen, Yu, & Wang, 2007）。這些研究除了維持基本的安全性設計外，主要方向爲設計小分存圖像的分享方法與各種不同解密效果的分享技術，讓分享機制更有效率且應用性更廣。

另一方面，隨著近年來電腦硬體的進步，三維模型的技術使用上日漸普及，從電腦動畫到電腦遊戲，甚至 3D 電影產業，皆採用大量的三維模型來建構動畫中的場景物件。一般來說，三維模型主要由頂點（vertex）及多邊形（polygon）所構成，而一個多邊形即爲多個三維點所圍成的區域。一些研究（Benedens, 1999; Cayre & Macq, 2007; Chou & Tseng, 2006; Cotting, Weyrich, Pauly, & Gross, 2004; Lin, Liao, Lu, & Lin, 2005; Ohbuchi, Masuda, & Aono, 1997; Ohbuchi, Mukaiyama, Takahashi, 2004; Yeo & Yeung, 1999）設計三維模型浮水印技術，作爲 3D 模型所有權人的版權證明；另外一些研究（Chao, Lin, Yu, & Lee, 2009; Cheng & Wang, 2006; Wang & Cheng, 2005; Wang et al., 2007）設計以 3D 模型資料爲遮蔽物件的隱藏技術，利用三維模型資料的掩護來儲存與傳輸重要資料。

本研究中首先提出了一個基於 IEEE-754 標準浮點數（IEEE-754 Floating Point Standard）點資訊的漸進式 $n$ 階層三維模型分享技術，將三維模型經由分享演算法編碼成 $n + 1$ 份分存模型，並達到漸進式還原的效果。在所設計的 $n$ 階層分享方法上，若使用者只取得單份分存模型，是無法得到原模型的任何資訊；而當取得 $q(2 \le q \le n + 1)$ 份分存做還原時，會依據 $q$ 的大小來顯示出不一樣解析度的原始機密模型資料，當取得的分存模型愈多（意即 $q$ 值愈大）時，使用者可還原的原始機密模型資訊就愈完整，當取得 $n + 1$ 份分存模型即可無失真的還原出原始的機密模型資料。

## 貳、相關技術

本章介紹與本研究所使用的相關技術。首先在第一節將會先說明本研究中所