植基於空間切割之三維模型秘密分享技術之介紹

蔡淵裕 [1, 2]
[1] 亞洲大學行動商務與多媒體應用學系
[2] 中國醫藥大學附設醫院醫學研究部
yytsai@asia.edu.tw

摘要

在本文中，我們介紹 Tsai 學者所提出的三維模型秘密分享技術。秘密分享是個高度受到重視的研究領域，已有許多相關研究應用至二維影像上。然而，秘密分享演算法並未隨著三維模型多媒體技術的快速發展而逐步增長，因此將秘密分享的應用延伸到三維模型就顯得十分重要。Tsai 學者提出一套植基於空間切割技術之可回復式點雲模型秘密分享技術，欲分享的點雲模型中的每個頂點會先被編碼成一連串落在$[0, p-1]$的整數值，其中p是一個預設的質數。接著，將編碼後的整數值取代分享多項式的係數取得分享值，並透過表面重建技術和取樣概念的整合，提供每位參與者一個具有足夠模型複雜度的掩護模型。最後，將分享值嵌入至每位參與者的掩護模型中，便可得到帶有分享值的偽裝模型。實驗結果證實，Tsai 學者所提出的技術支援可回復式資訊隱藏，分享值能有更高層次的隱私性與強韌性，是第一篇整合秘密分享與資訊隱藏的三維模型秘密分享的文獻。

關鍵詞：三維模型、可回復式資訊隱藏、秘密分享、取樣、空間切割、表面重建

Introduction to a Secret 3D Model Sharing Scheme Based on Spatial Subdivision

Yuan-Yu Tsai[1, 2]
[1]Department of M-Commerce and Multimedia Applications,
Asia University, Taichung, Taiwan
[2]Department of Medical Research, China Medical University Hospital,
China Medical University, Taichung, Taiwan
yytsai@asia.edu.tw

Abstract

This paper introduces Tsai's secret 3D model sharing algorithm. The proposed algorithm is the first secret sharing scheme to include reversible data hiding for 3D point geometries. Each point is first encoded into a series of integer values within 0 and $p-1$ based on space subdivision, where p is a predefined prime number. The integer values then substitute all

coefficients of the sharing polynomial to obtain the share values. A cover model with sufficient model complexity is generated by integrating the surface reconstruction and the sampling concepts. Finally, each participant has a separate 3D stego model with embedded share values. Experimental results show that Tsai's proposed technique supports reversible data hiding and the share values have higher levels of privacy and improved robustness.

Keywords: 3D Models, Reversible Data Hiding, Secret 3D Model Sharing, Sampling, Space Subdivision, Surface Reconstruction

壹、前言

資訊科技的發展和網際網路的便利巧妙地改變人類的行為，即時通訊、電子郵件、Facebook 和 Skype 已經取代傳統的信件成為人與人之間主要的溝通橋樑。但是，網際網路是每個人都能存取的開放式網路，傳送的訊息很容易被攔截或篡改，因此發展一套能防止訊息遭受攔截或竄改的技術是有必要的。

解決這項問題最直接方法就是使用加密演算法，透過秘密金鑰的協助對發送的訊息進行加密，使訊息變成無法閱讀的字元，再經由網際網路發送加密後的訊息。只有知道秘密金鑰的接收者才能進行解密的操作，重建出原始的訊息，而非法的攔截者無法取得訊息中的任何資料。秘密金鑰在密碼系統中扮演著重要的角色，一旦秘密金鑰被竊取或遺失，秘密訊息的安全性將受到損害，因此為秘密金鑰開發一種安全且方便的保護機制便顯得非常重要。

秘密分享將秘密的分享值分給特定的參與者[2][20][26] [28][29]，秘密只能透過結合足夠數量的分享值後才能重建出來，如果只有單個或數量不足的分享值就無法獲得關於秘密的任何資訊。傳統(t,n)門檻值秘密分享演算法包含了 Shamir 學者[20]所提出的多項式內插技術與 Blakley 學者[2]所提出的超平面交點技術，(t,n)門檻值秘密分享演算法意旨在n個的分享值中，任t個以上分享值的結合都能重建出完整的秘密，少於t個分享值則無法獲取任何有關秘密的任何資訊。

先進的科技使得傳統媒體得以數位化並經由網際網路快速的散佈到全世界。因此，傳統的秘密金鑰分享的概念已經擴展到秘密影像分享[3][11][12][15][21][25]和秘密三維模型分享[8][9][10][18]。然而，秘密影像分享已經成為一個被大量研究的議題，秘密三維模型分享卻僅有部分學者提出。Elsheh 和 Hamza 兩學者採用 Blakley[2]、Thien 和 Lin[21]所提出的秘密分享概念延伸至三維多邊形模型。使用 Blakley 機制的演算法中，作者將三維模型中的每個頂點和面分配到n個子機密超平面$z = ax + by + c$中。在訊息重建時，透過各個超平面間的交點取回頂點座標和面的原始值。在使用 Thien 和 Lin 機制的演算法中，則是先將三維模型做無失真的壓縮，然後再用壓縮碼取代多項式的係數

產生n個分享值。Martín del Rey 學者[18]則是提出了一套植基於可逆儲存三維細胞自動機之三維實體模型多重秘密分享演算法。然而，上述演算法的各個分享值都是毫無意義的，容易遭到有意人士的截取或竄改。Tsai 學者[28]則結合秘密分享和資訊隱藏的技術[4][7][13][14]開發一個更有效的三維模型秘密分享演算法。首先，作者將一個欲分享的點雲模型利用空間分割技術編碼成一連串的整數序列，並將這些整數值取代分享多項式的係數得到分享值，每個分享值再嵌入至各個參與者的掩護模型中得到偽裝模型。該技術有五個重要的特性：第一，每個分享值的私密性在掩護模型的掩護下有相當大的提升。第二，各個分享值透過主成分分析技術[19]來抵抗相似轉換攻擊。第三，該技術在執行秘密分享前會先進行編碼的動作，降低資料處理的複雜度。第四，藉由表面重建技術和取樣概念的整合，掩護模型的模型複雜度能有效的提升。最後，該技術支援可回復式資訊隱藏[6][16][17][27]，意旨在擷取出分享值後，偽裝模型能回復至未帶有分享值的掩護模型。

本文其餘部分安排如下：第貳章節提供了秘密分享相關概念及在秘密影像分享的文獻回顧；第參章節詳述 Tsai 學者所提技術；第肆章展示其實驗結果及討論；最後，第伍章提出結論和未來的研究方向。

貳、文獻探討

Shamir 提出的(t,n)門檻機制是一種有效的秘密分享方法。這個機制利用多項式內插技術，將欲分享的秘密訊息分配給n位參與者。秘密訊息只有在n位參與者中的任t位以上的參與才能重建出，少於t位則無法取得任何有關秘密訊息的資訊。在秘密分享階段時，給定一個欲分享的秘密s，在質數p的模數運算下決定出一個$(t-1)$次的多項式，其中方程式的每一個係數$a_1, a_2, \dots, a_{t-1}$為介於$[0, p-1]$之間的隨機整數(參見方程式(1))。而欲分享的秘密被編碼成$f(0)$的值，每個參與者i可以得到其分享值$y_i = f(i)$。在秘密重建階段時，只要有n位中的t位參與，便可透過 Lagrange 內插技術(參見方程式(2))將方程式重建出來，並在$f(0)$中取得機密s。

$$f(x) = (s + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}) \ \ mod \ \ p \tag{1}$$

$$f(x) = \sum_{i=1}^{t} \left(\prod_{j=1, i \neq j}^{t} \frac{x - x_j}{x_i - x_j} \right) f(x_i) \tag{2}$$

當秘密分享的原理延伸到影像時，最常用的方式便是將秘密影像中各個像素值代入方程式(1)中的係數s，再隨機選定$a_1, a_2, \dots, a_{t-1}$等係數後產生分享值給各個參與者，便能完成秘密影像的分享。之後許多學者提出改進的技術。首先，因為像素的灰階值介於 0 到 255，所以 251 是最常被選擇的質數，但也使得秘密影像的數值在計算分享值前必須被截斷至 250，這個缺失可以透過採用伽羅瓦體(Galois Field) $GF(2^8)$[26]達到無失真的秘密影像分享。接著，每個分享值影像的大小和秘密影像是相等的，Thien 和 Lin[21]

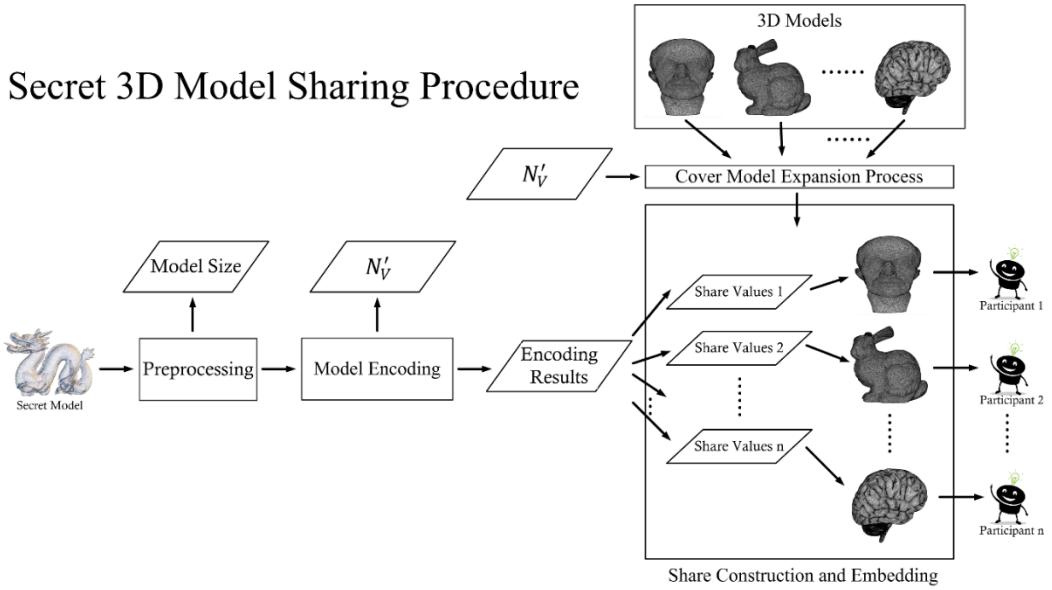
將秘密影像中的像素值取代分享多項式中所有的係數，這樣每個參與者僅會拿到$1/t$秘密影像大小的分享值影像。最後，部分技術使用資訊隱藏機制[3][11][12][15][25]，將分享值嵌入至有意義的掩護影像以增加其私密性。

參、Tsai 學者所提之秘密分享技術

本章節將詳細介紹 Tsai 學者所提出的三維點雲模型秘密分享演算法，主要概念是利用空間切割的技術將秘密點雲模型的頂點編碼成一連串的整數值，使得資料處理的複雜度從實數運算簡化至整數運算。之後，將所有整數值取代$t-1$次分享多項式的所有係數，以取得每位參與者的分享值，並整合資訊隱藏演算法提高分享值的隱密性。然而，掩護模型的複雜度可能不足以承載分享值，因此 Tsai 學者使用表面重建演算法與取樣概念，有效增加掩護模型的頂點個數以加強其複雜度。最後，將分享值嵌入至每個參與者各自擁有的掩護模型中，得到其偽裝模型。在秘密三維模型的重建過程中，只要n個偽裝模型中的任意t個，便可以透過反向流程重建出無失真的秘密三維模型。

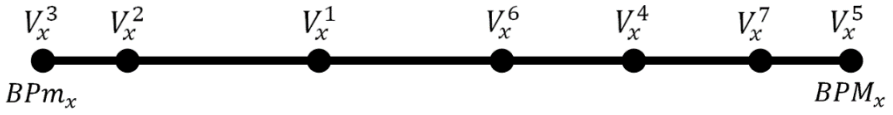
3.1 三維模型秘密分享的流程

圖一為 Tsai 學者所提出的三維模型秘密分享技術的流程圖。在前處理步驟中，透過讀取欲處理的秘密點雲模型建立其界線容積。接著，在模型編碼步驟中將秘密模型編碼成一連串的整數值，並計算出掩護模型所需的頂點數目。在分享值的建立步驟中，則是將上述的整數值，取代$(t-1)$次多項式中的每一個係數，以取得每個參與者的分享值。在掩護模型的擴增步驟中，則是透過表面重建和取樣概念進行掩護模型擴增的動作，使得掩護模型能有足夠的複雜度嵌入分享值。最後，將分享值嵌入至每位參與者所對應的掩護模型中，便可得到其偽裝模型。



圖一：三維模型秘密分享技術的流程圖

前處理步驟：在此步驟中，首先讀入欲分享之秘密點雲模型(SPG)以得到模型相關資訊，假設點雲模型由N_V個頂點所組成。接著，尋找各個頂點在笛卡兒座標系統中各個座標軸上的最大值與最小值(最少兩個最多六個)，透過對角的兩個頂點座標BPM和BPm來建立界線容積，界線容積的長、寬、高可以透過BPM_d和BPm_d兩頂點之間的差值求得$(d = x, y, z)$。圖二為一個擁有七個頂點的點雲模型，皆位於x軸上，而頂點V_x^3和V_x^5因為位於x軸上的最小值與最大值，因此被用來建立界線容積。



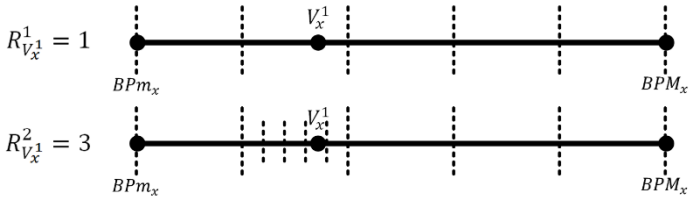
圖二：建立界線容積的例子

模型編碼步驟：此步驟利用一個質數p將秘密點雲模型編碼成一連串落在$[0, p-1]$內的整數值，每個頂點將被轉換成p進位的表示方式，而頂點的編碼長度r可以在模型尺寸$\overline{BPM_d BPm_d}$、質數p及輸入模型檔案中點座標數值的最大顯示精度(NP)的幫助下估算出來(參見方程式(3))。透過將每一回合編碼的轉換數字$R_{V_d^k}$蒐集起來便可以得到該頂點的編碼結果$EL_{V_d^k}$ (參見方程式(4))，而原來的座標V_d^k可以利用方程式(5)無失真的回復出來。以圖三為例，質數p設為 5，並且要對座標V_x^1進行編碼，在第一回合的編碼中，$\overline{BPM_x BPm_x}$區間被分割為 5 個子區間，而座標V_x^1落在區間$R_{V_x^1}^1 = 1$。在第二回合編碼中，區間$R_{V_x^1}^1 = 1$又被分割為 5 個子區間，且座標V_x^1落在區間$R_{V_x^1}^2 = 3$。經過若干回合後，座標V_x^1的編碼結果$EL_{V_x^1}$變成$(1, 3, \ldots)_5$。值得注意的是，方程式(3)計算出的編碼長度只是一個估算值，為了避免在復原分享模型時出現失真，使用者應適時的調整方程式(3)所產生的編碼長度。

$$r = \left\lceil log_p\left(max\left(\overline{BPM_xBPm_x}, \overline{BPM_yBPm_y}, \overline{BPM_zBPm_z}\right) \times 10^{NP}\right)\right\rceil \quad (3)$$

$$EL_{V_d^k} = \left(R_{V_d^k}^1, R_{V_d^k}^2, R_{V_d^k}^3, \ldots, R_{V_d^k}^r\right)_p \quad (4)$$

$$V_d^k = \sum_{m=1}^{r} \frac{\overline{BPM_dBPm_d}}{p^m} \times R_{V_d^k}^m + BPm_d \quad (5)$$



圖三：座標V_x^1進行編碼處理的例子

掩護模型擴增步驟：在每個頂點都進行編碼之後，最後點雲模型的編碼結果EL_d^{SPG}會是由$N_V \times r$個介於$[0, p-1]$之間的整數值所組成(參見方程式(6)，$k = 1, 2, \ldots, N_V \times r$)。接著，將得到的整數值取代所有在方程式(1)中的分享多項式的係數$s, a_1, a_2, \ldots, a_{t-1}$以求得分享值，由於$(t, n)$門檻值機制的分享多項式中共有$t$個係數，因此會得到$\lceil (N_V \times r)/t \rceil$個分享值。接著，便可使用資訊隱藏演算法增加上述分享值的隱密性。而掩護模型擴增步驟的目的，就是產生一個具有足夠頂點數量的掩護模型來嵌入分享值。因為 Tsai 學者所提技術的每個頂點僅能承載一個分享值，所以在擴增掩護模型中的頂點數量N'_V，會與分享值的數量相同，共有$\lceil (N_V \times r)/t \rceil$個頂點。

$$\begin{aligned} EL_d^{SPG} &= EL_{V_d^1} || EL_{V_d^2} || \ldots || EL_{V_d^{N_V}} \\ &= \left(R_{V_d^1}^1, R_{V_d^1}^2, \ldots, R_{V_d^1}^r\right) || \left(R_{V_d^2}^1, R_{V_d^2}^2, \ldots, R_{V_d^2}^r\right) || \ldots || \left(R_{V_d^{N_V}}^1, R_{V_d^{N_V}}^2, \ldots, R_{V_d^{N_V}}^r\right) \\ &= \left(R_{V_d^1}^1, R_{V_d^1}^2, \ldots, R_{V_d^1}^r, R_{V_d^2}^1, R_{V_d^2}^2, \ldots, R_{V_d^2}^r, R_{V_d^{N_V}}^1, R_{V_d^{N_V}}^2, \ldots, R_{V_d^{N_V}}^r\right) = R_{V_d}^k \end{aligned} \quad (6)$$

在此步驟中，Tsai 學者採用 Ball Pivoting 表面重建演算法[1]，將每個參與者的點雲掩護模型PG^i轉換為多邊形掩護模型PM^i，接著使用方程式(7)計算數量不足的頂點數量$n_{inp}^{PG^i}$，其中n^{PG^i}是在模型PG^i上頂點的數量，$n_{BP}^{PG^i}$則是模型PG^i用來建立界線容積所使用的頂點數量。為了確保界線容積在嵌入分享值之前與之後的一致性，用於建立掩護模型界線容積的頂點是不會被修改的。接著，Tsai 學者依據各多邊形的表面積將$n_{inp}^{PG^i}$個頂點分配給模型PM^i內的各個多邊形，擁有最大面積的多邊形將含有最多數量的頂點。方程式(8)為頂點分布在每個多邊形P_k的方式，其中$SA_{P_k}^{PM^i}$和SA^{PM^i}分別是每個多邊形P_k和多邊形模型PM^i的表面積。經過上述步驟頂點分配後，若頂點仍有不足之處，則隨機從多邊形模型中選擇一個多邊形，然後在選定的多邊形中增加一個點。重複上述的步驟，直到所需頂點數量足夠為止。最後，Tsai 學者使用質心座標技術[24]以得到每個多邊形$n_{P_k}^{PM^i}$個頂點，替每位參與者i產生擴增後的掩護模型CPG^i。在方程式(9)中，P為位於多邊形V_{P_k}上的頂點；$V_{P_k}^j$是位於多邊形V_{P_k}的第j個頂點；α_j是 0 和 1 之間的隨機數，且$\sum_{j=1}^{|V_{P_k}|} \alpha_j =$

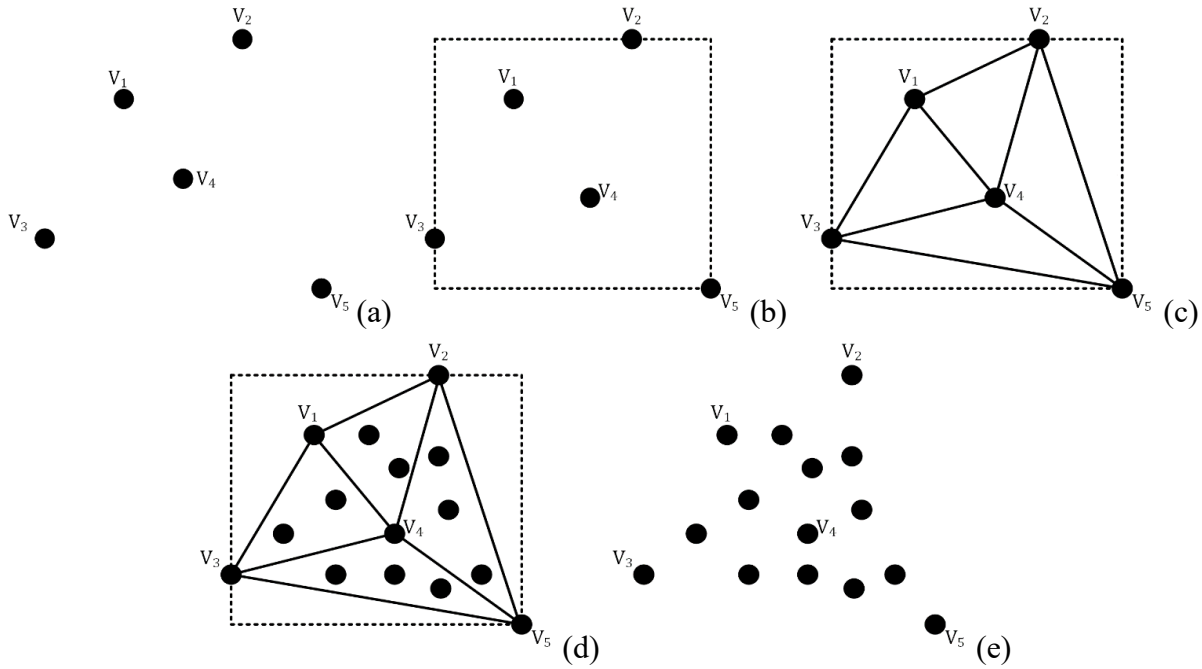
1，其中$\left|V_{P_k}\right|$是多邊形V_{P_k}的頂點數量，每個掩護模型的最終擴增比例可以從$\lceil(N_V \times r)/t\rceil/n^{PG^i}$取得。

$$n_{inp}^{PG^i} = \lceil(N_V \times r)/t\rceil - \left(n^{PG^i} - n_{BP}^{PG^i}\right) \tag{7}$$

$$n_{P_k}^{PM^i} = \left\lfloor n_{inp}^{PG^i} \times \left(SA_{P_k}^{PM^i}/SA^{PM^i}\right)\right\rfloor \tag{8}$$

$$P = \sum_{j=1}^{\left|V_{P_k}\right|}\left(\alpha_j \times V_{P_k}^j\right) \tag{9}$$

以圖四為例，假設一位參與者擁有如圖四(a)所示 5 個頂點的掩護模型。首先需產生此掩護模型的界線容積，由於頂點V_2、V_3和V_5在x和y軸上有著最大值與最小值，因此被用來建立界線容積(如圖四(b)虛線所示)。假設秘密分享模型經過編碼處理後，掩護模型需要的頂點個數N'_V為 12，顯然原來的掩護模型是需要被擴增的。因此利用方程式(7)計算出不足的頂點數量$n_{inp}^{PG^i}(n_{inp}^{PG^i} = 12 - (5-3) = 10)$。換句話說，為了進行分享值的嵌入，還需要額外的 10 個頂點。因此使用表面重建技術得到重建後的多邊型模型(如圖四(c)所示)，重建的模型共有五個頂點和四個面積相同的多邊形。接著，依據方程式(8)將 10 個頂點分配至各個三角形，由於各個三角形擁有相同的表面積，因此每個三角形能擁有相同的頂點數量$n_{P_k}^{PM^i} = \lfloor 10 \times (1/4)\rfloor = 2$。但因為仍缺少兩個點，便隨機從建立起來的多邊形模型中選擇一個多邊形並增加一個點，直到達到所須的頂點數量。圖四(d)假設多邊形$V_2V_4V_5$和多邊形$V_3V_4V_5$各增加一個點。最後，此步驟使用方程式(9)中的質心座標系統來取得每一三角形內的頂點，圖四(e)為此步驟掩護模型模型擴增的例子。



圖四：模型擴增步驟的例子

分享值的生成與嵌入步驟：當掩護模型中的頂點數目足夠時，此步驟便開始執行。除了用來建立界線容積的頂點外，擴增後掩護模型中的每個頂點V^k的座標值v_d^k會利用模型

編碼步驟中所提的技術進行編碼，每個頂點的編碼結果可參見方程式(10)中。接著從EL_d^{SPG}中取出t個整數值，取代分享多項式中所有的係數$s, a_1, a_2, \dots, a_{t-1}$，便可得到每個參與者$i$的分享值$SV_d^i$，並將每個頂點編碼結果的最後一位數字替換成$SV_d^i$，即完成嵌入的步驟(請參見方程式(11))。最終一回合分享多項式中不足整數值的係數則被置換成 0。完成分享值的嵌入後，偽裝模型中的頂點座標值v'^k_d便可使用方程式(12)獲得。一旦每個頂點都被處理過，每個參與者i就能得到帶有分享值嵌入的偽裝模型SPG^i。為了確保能抵抗相似轉換的攻擊，我們在偽裝模型上採用主成分分析技術，產生一個座標系統PCA，並計算求得一個從PCA座標系統轉換成至笛卡兒座標系統的轉換矩陣TM^{SPG^i}，以有效在秘密模型重建步驟中進行模型校正。

$$EL_{v_d^k} = \left(R_v^1, R_{v_d^k}^2, R_{v_d^k}^3, \dots, R_{v_d^k}^r\right)_p \tag{10}$$

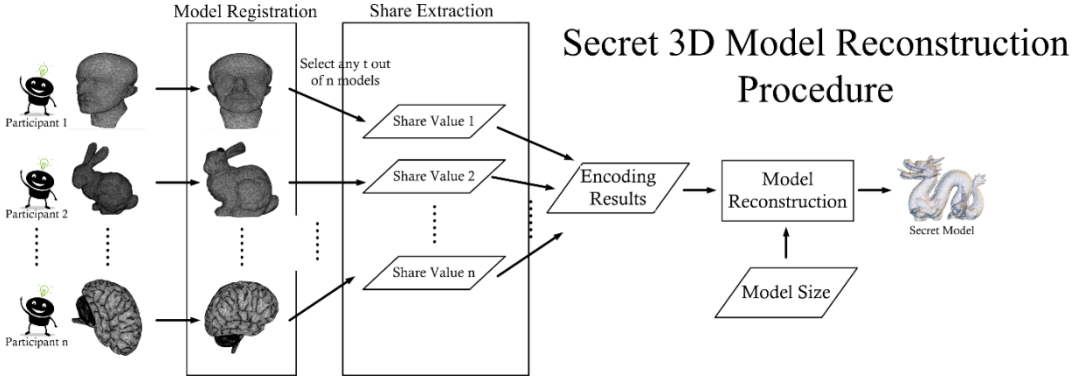
$$EL'_{v_d^k} = \left(R_v^1, R_{v_d^k}^2, R_{v_d^k}^3, \dots, SV_d^i\right)_p \tag{11}$$

$$v'^k_d = \sum_{m=1}^{r-1} \frac{\overline{BPM_d^{CPG^i} BPm_d^{CPG^i}}}{p^m} \times R_{V_d^i}^m + \frac{\overline{BPM_d^{CPG^i} BPm_d^{CPG^i}}}{p^r} \times SV_d^i + BPm_d^{CPG^i} \tag{12}$$

3.2 三維模型重建的流程

給予n個參與者中的任t個偽裝模型和額外的資訊，便可啟動秘密三維模型重建的流程以取回秘密點雲模型。圖五為秘密三維模型重建的流程圖，共包含三個步驟。

首先，每個參與者i透過主成分分析技術和轉換矩陣TM^{SPG^i}，校正可能經過相似轉換攻擊的偽裝模型SPG'^i，並建立其界線容積$BV^{SPG'^i}$。除了用來建立界線容積的邊界頂點，偽裝模型的每一個頂點都會在r個回合的編碼步驟中編碼成一連串的整數值，透過蒐集每個頂點在第r個回合的編碼結果，便可重建出分享多項式$f(x)$，得到$(N_V \times r)$個整數值。最後，每個秘密點雲模型頂點的原始值可使用方程式(5)來取回。

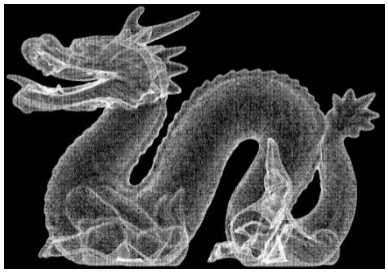


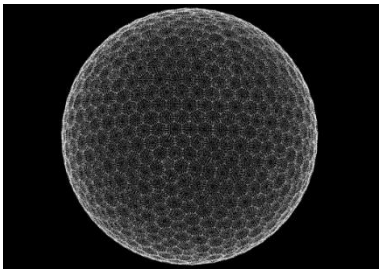
圖五：秘密三維模型重建流程圖

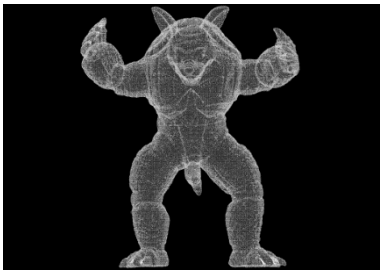
3.3 延伸至可回復式資訊隱藏

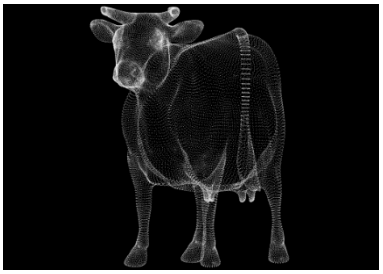
本章節說明 Tsai 學者所提技術如何支援可回復式資訊隱藏。可回復式資訊隱藏技術能使得偽裝模型在擷取訊息後，還能準確地恢復成原本的掩護模型。回想掩護模型中的每一個頂點v_d^k，會在r個回合的編碼過程中產生一連串的整數值$EL_{v_d^k}$，表示成如方程式(10)所示，而最後一回合的編碼結果$R_{v_d^k}^r$會被修改成分享值SV_d^i。因此，若$EL'_{v_d^k}$無法恢復到$EL_{v_d^k}$，我們的演算法將無法實現可回復式資訊隱藏。換句話說，整數值$R_{v_d^k}^r$必須先預先儲存，否則掩護模型將被永久破壞，無法恢復成原來的值。

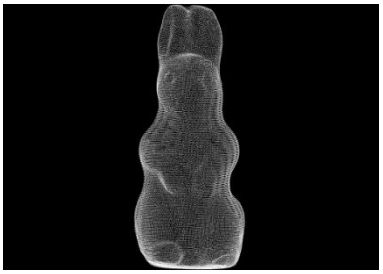
在秘密分享機制的幫助下，Tsai 學者保留分享多項式中的係數s用以儲存回復資訊$R_{v_d^k}^r$，而剩餘的$t-1$個係數$a_1, a_2, \ldots, a_{t-1}$，則用$EL_d^{SPG}$內的每一個整數值取代。因此，在擴增掩護模型所需的頂點數量將變成$\lceil (N_V \times r)/(t-1) \rceil$。此外，在分享值建立的過程中，每個參與者所拿到的分享多項式是相同的，也就是說每位參與者分享方程式的係數s是相同的。因為係數s被擴增掩護模型中每個點的最後一回合的編碼結果取代，代表每個參與者擴增掩護模型中的頂點，在最後一輪的編碼結果需要相同，而最好的解決辦法便是限制每位參與者使用相同的掩護模型。


秘密模型 - Dragon


秘密模型 - Golf Ball


掩護模型 – Armadillo


掩護模型 - Cow


掩護模型 - Rabbit

圖六：秘密模型和掩護模型的視覺效果

肆、研究結果與討論

本章節將介紹 Tsai 學者所提技術之實驗結果以評估該方法的可行性。Tsai 學者採用(2, 3)門檻值秘密分享機制來探討其實驗結果。表一為該實驗所採用秘密模型及掩護模型的相關資訊，包括頂點的數量N_V和其模型大小(由界線容積的對角線長度DL_{BV}表示)。圖

六為每一模型的視覺效果。該技術在搭載 Intel Core i7 2.67 GHz 處理器和 3 GB 記憶體的個人電腦上使用 Microsoft Visual C++程式語言進行實作，並使用均方根誤差來測量掩護模型與偽裝模型之間的失真度，其定義詳見方程式(13)，C_i和S_i分別代表著位於第i次讀取順序的原始模型與修改的模型的頂點。

$$RMSE = \sqrt{\frac{\sum_{i=1}^{N_V'} \|C_i - S_i\|^2}{N_V'}} \tag{13}$$

表一：Tsai 學者所採用秘密模型及掩護模型的相關資訊

模型名稱		N_V	DL_{BV}
秘密模型	Dragon	437645	26.69
	Golf Ball	122882	1.73
掩護模型	Armadillo	172974	228.80
	Cow	46433	30.49
	Rabbit	67038	33.91

本節首先展示 Tsai 學者所提技術在各種質數p之下的秘密模型的編碼結果，並透過編碼結果回復每個點的座標來計算模型失真度以評估方程式(3)編碼長度的準確度。本章節也會展示重建出的多邊形模型和擴增掩護模型的視覺效果。接著，透過對偽裝模型進行相似轉換攻擊，以展現偽裝模型的強韌性。此外，本章節將比較掩護模型和偽裝模型在使用(2, 3)門檻值秘密分享演算法後的失真度比較，並透過與其他演算法的效能比較，證明 Tsai 學者所提技術的可行性。

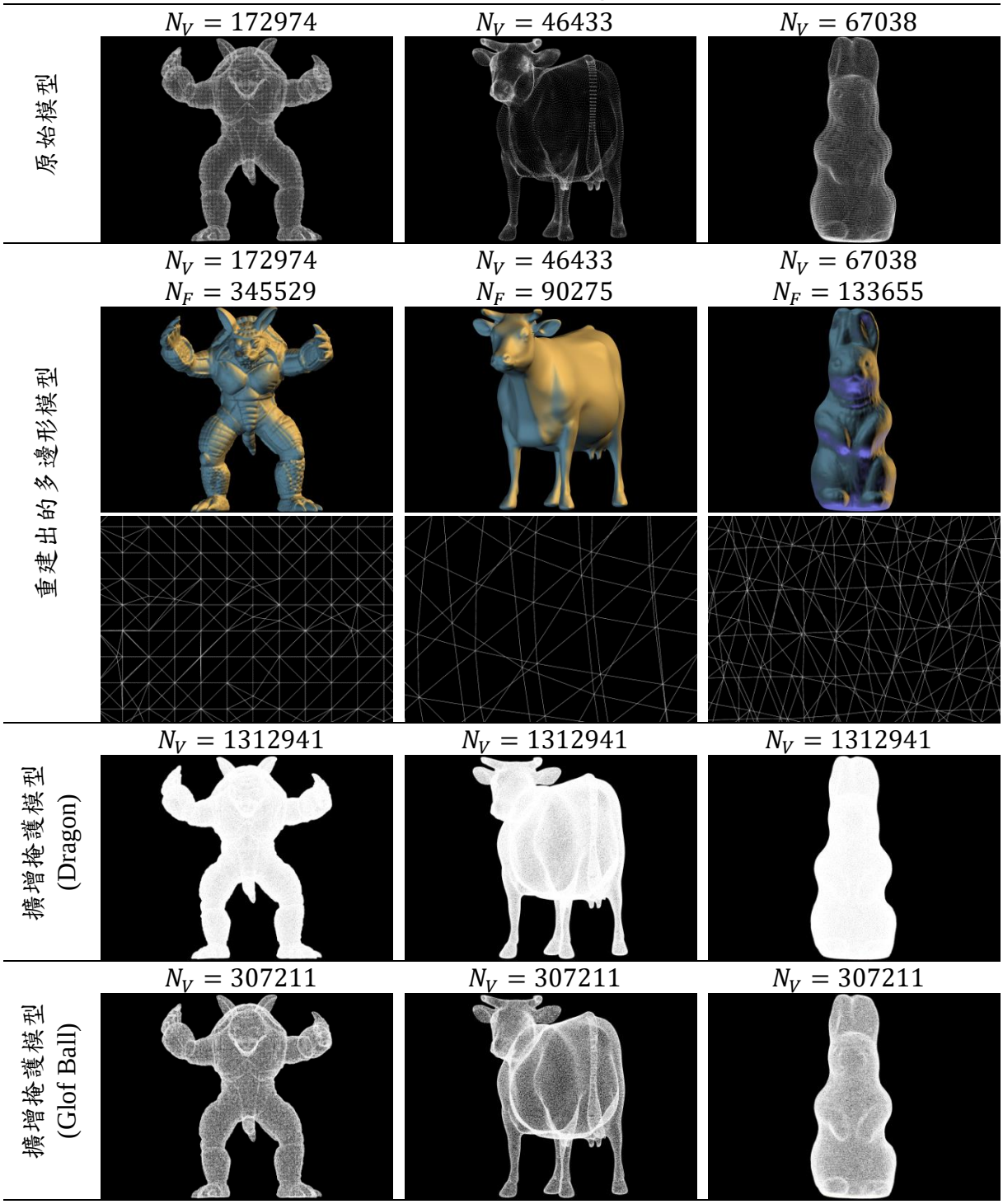
表二展示了 Tsai 學者所提技術中每個三維模型在各種質數p下計算出的編碼長度，這個編碼長度是使用方程式(3)計算得出，並利用模型的失真度估算其精準度。如表二所示，實驗結果證實該三維模型可以在使用計算出的編碼長度下進行編碼動作，且在恢復時沒有任何的錯誤。

表二：不同質數計算出來的編碼長度 r

Model Name	$p = 5$	$p = 11$	$p = 17$
Dragon	11	8	6
Golf Ball	9	6	5
Armadillo	12	8	7
Cow	11	8	6
Rabbit	12	8	7

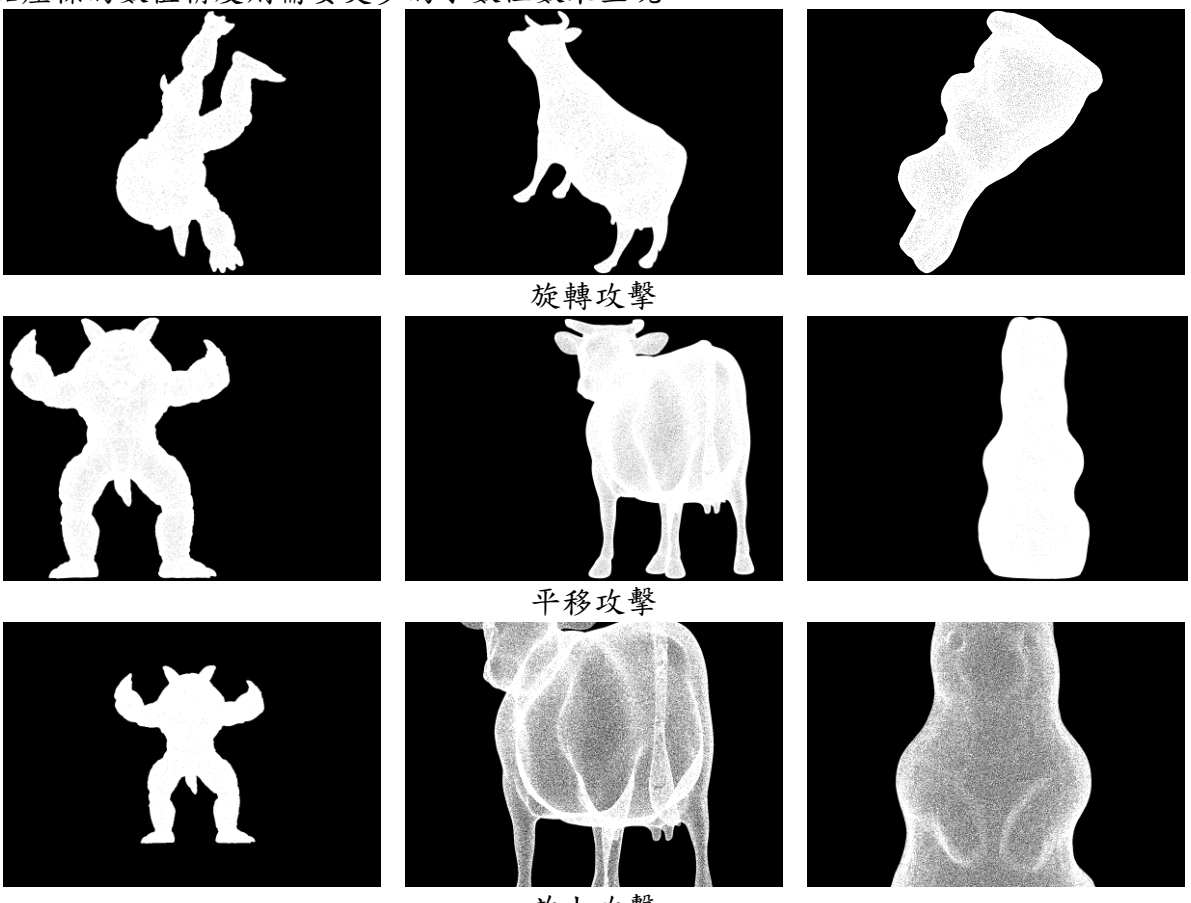
接著，我們展示 Tsai 學者所提技術重建出的多邊形模型和擴增掩護模型的視覺效果。如上節 3.1 提到，表面重建演算法是用於根據輸入的點模型計算出多邊形模型，圖七中

的第一列與第二列分別顯示原始的掩護模型和被計算出來的多邊形模型，其中N_F是計算出來的多邊形模型中的多邊形數目，而欲嵌入 Dragon 和 Golf Ball 兩模型的擴增掩護模型則呈現在圖七的第三行與第四行。Tsai 學者也提供計算出的多邊型模型的特寫圖以便於進行比較。實驗結果證實，表面重建演算法可以有效的解決分享值嵌入點的數量不足問題，並能使得擴增過的掩護模型與原始模型的視覺效果相似。



圖七：原始模型和擴增後的掩護模型之間的比較

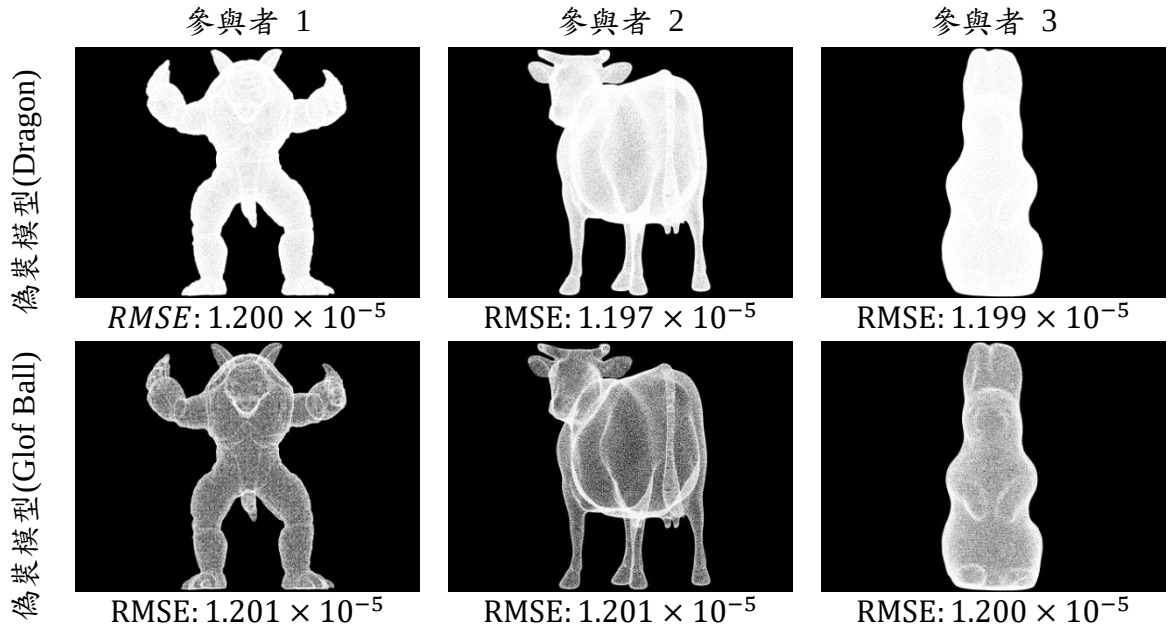
本章節接下來介紹評估 Tsai 學者所提技術的強韌性。對三維模型來說，平移、旋轉與縮放等相似的轉換攻擊被視為普通的操作，三維模型在受到這些攻擊後，其外觀是不受影響的，因此，大多數的三維模型資訊隱藏演算法均有能力可以抵抗相似轉換攻擊，Tsai 學者所提出的演算法也不例外。由於編碼結果是來自於編碼頂點與邊界頂點之間的距離，此距離在平移攻擊下是不會改變的。而在遭受旋轉攻擊後，可以透過轉換矩陣和主成分分析來校正點雲模型。然而，當偽裝模型遭受到縮放攻擊，從模型大小產生出來的編碼長度r變成是一個需要額外記錄的資訊。為了測試該演算法的強韌性，Tsai 學者隨機旋轉、平移和縮放每個三維偽裝模型，圖八為三個偽裝模型在受到相似轉換攻擊後的視覺效果。實驗結果顯示，擷取出的分享值沒有發生任何錯誤。不過值得一提的是，偽裝模型在經過相似轉換攻擊後，因截斷和捨去的數值運算會影響分享值擷取的正確性，因此部分偽裝模型的數值精準度必須至第 7 位小數，而當偽裝模型遭到縮小攻擊，其頂點座標的數值精度則需要更多的小數位數來呈現。



圖八：相似轉換攻擊之後的偽裝模型視覺效果

接著圖九展示(2, 3)門檻值的秘密分享演算法，在嵌入分享值後偽裝模型的視覺效果。實驗結果顯示重建出的三維模型與原來的秘密分享模型毫無失真。就圖七與圖九兩圖之模型外觀也無法分辨其差異，代表該技術所造成的失真度很小。嵌入 Dragon 模型的偽裝模型失真度為1.199×10^{-5}，而嵌入 Golf Ball 模型的偽裝模型失真度也約略在$1.201 \times$

10^{-5}。



圖九：嵌入分享值後的偽裝模型

最後，表三為 Tsai 學者所提技術與相關機制間的功能性比較。根據秘密分享技術所使用分享媒體的不同可分為兩類：二維影像與三維模型。從資訊隱藏的角度來看，方法[11][12][15][25]可以恢復掩護影像且不需要像素擴張，但在[3]的演算法中無法支援可回復式資訊隱藏。Tsai 學者所提出的演算法是第一個能同時兼具三維模型秘密分享與可回復式的資訊隱藏演算法，但由於三維模型數值範圍的變化使得需要進行頂點擴增的動作。從嵌入的訊息量來看，Hu 等學者所提出的技術[11][12]能提供最大的嵌入量，每張影像都可以有$(t-1)/2$個像素嵌入。Tsai 學者提出的演算法中，掩護模型的頂點數量可以根據分享模型的大小進行擴增的動作，可以固定嵌入N_V個頂點的秘密分享模型。最後，從強韌性的角度來看，只有 Martín del Rey 與 Tsai 學者所提出的演算法可以抵抗相關攻擊，以上各特性說明 Tsai 學者的演算法在三維模型秘密分享領域中是可行的。

伍、結論與建議

本文介紹 Tsai 學者所提出的三維模型秘密分享技術。該演算法降低了資料處理的複雜性，將含有小數運算的操作利用空間分割技術轉換至整數運算，並利用表面重建技術搭配取樣概念，擴增掩護模型以得到足夠的頂點數量。該演算法簡單，秘密模型的失真度很小，且分享值具有較高的隱密性與強韌性。此外，該技術支援可回復式資訊隱藏，這些優勢證明了該技術的可行性。

雖然這種技術的結果令人感到滿意，但仍有部分地方需要探究。首先，希望能拓展此

技術的適用性，應用至擁有拓樸資訊的多邊形模型與擁有小數數值的高動態範圍影像。此外，如何使 Tsai 學者所提出的演算法預防詐欺[5][22]也是一個有趣的研究課題。最後，有效減少掩護模型中多餘的點使其複雜度降低，以嵌入複雜度較低的秘密分享模型，也是值得探討的議題。

表三：Tsai 學者所提技術與秘密分享相關機制間的比較

方法	分享媒體	有意義的分享值	無失真的秘密媒體	無失真的掩護媒體	像素/頂點擴張	強韌性	嵌入量 (像素/頂點)
[21]	2D Images	No	Yes	–	Yes	No	–
[3]		Yes	Yes	No	Yes	No	$\frac{H \times W}{4}$
[15]		Yes	Yes	Yes	No	No	$\frac{(t-3) \times H \times W}{\lceil log_m 255 \rceil}$
[11]		Yes	Yes	Yes	No	No	$\frac{(t-1) \times H \times W}{2}$
[25]		Yes	Yes	Yes	No	No	$\frac{(t-2) \times H \times W}{4}$
[12]		Yes	Yes	Yes	No	No	$\frac{(t-1) \times H \times W}{2}$
[9]	3D Models	No	Yes	–	No	No	–
[18]		No	Yes	–	No	Differential Attack	–
[28]		Yes	Yes	Yes	Yes	Similarity Transformation	N_V

參考文獻

[1] F. Bernardini, J. Mittleman, H. Rushmeier, C. Silva, and G. Taubin, “The ball-pivoting algorithm for surface reconstruction,” *IEEE Transactions on Visualization and Computer Graphics*, vol. 5, no. 4, pp. 349–359, 1999.

[2] G. R. Blakley, “Safeguarding cryptographic keys,” *Proceedings of AFIPS National Computer Conference*, pp. 313–317, 1979.

[3] C. C. Chang, Y. P. Hsieh, and C. H. Lin, “Sharing secrets in stego images with authentication,” *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008.

[4] M. W. Chao, C. H. Lin, C. W. Yu, and T. Y. Lee, “A high capacity 3D steganography algorithm,” *IEEE Transactions on Visualization and Computer Graphics*, vol. 15, no. 2, pp. 274–284, 2009.

[5] Y. C. Chen, D. S. Tsai, and G. Horng, “Visual secret sharing with cheating prevention revisited,” *Digital Signal Processing*, vol. 23, no. 5, pp. 1496–1504, 2013.

[6] I. L. Chung, C. M. Chou, and D. C. Tseng, "Multi-layer reversible data-hiding scheme on 3D mesh models," *Journal of Internet Technology*, vol. 11, no. 5, pp. 609–618, 2010.

[7] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital watermarking and steganography*, Second Edition, Morgan Kaufmann, Burlington, 2008.

[8] E. Elsheh and A. B. Hamza, "Robust approaches to 3D object secret sharing," *Proceedings of 7th International Conference of Image Analysis and Recognition*, pp. 326–335, 2010.

[9] E. Elsheh and A. B. Hamza, "Secret sharing approaches for 3D object encryption," *Expert Systems with Applications*, vol. 38, no. 11, pp. 13906–13911, 2011.

[10] E. Elsheh and A. B. Hamza, "Secret sharing of 3D models using blakely scheme," *Proceedings of 25th Biennial Symposium on Communications*, pp. 92–95, 2010.

[11] W. T. Hu, M. C. Li, C. Guo, and Y. Z. Ren, "Reversible secret image sharing with steganography and dynamic embedding," *Security and Communication Networks*, vol. 5, no. 11, pp. 1267–1276, 2012.

[12] W. T. Hu, M. C. Li, C. Guo, and L. F. Yuan, "A reversible steganography scheme of secret image sharing based on cellular automata and least significant bits construction," *Mathematical Problems in Engineering*, vol. 2015, Article: 849768, pp. 1–11, 2015.

[13] Y. H. Huang and Y. Y. Tsai, "A reversible data hiding scheme for 3D polygonal models based on histogram shifting with high embedding capacity," *3D Research*, vol. 6, no. 20, Article: 20, pp. 1–12, 2015.

[14] M. T. Li, N. C. Huang, and C. M. Wang, "A novel high capacity 3D steganographic algorithm," *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 3, pp. 1055–1074, 2011.

[15] P. Y. Lin, J. S. Lee, and C. C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognition*, vol. 42, no. 5, pp. 886–895, 2009.

[16] C. C. Lo and Y. C. Hu, "A novel reversible image authentication scheme for digital images," *Signal Processing*, vol. 98, pp. 174–185, 2014.

[17] T. C. Lu, C. Y. Tseng, K. M. Deng, "Reversible data hiding using local edge sensing prediction methods and adaptive thresholds," Signal Processing, vol. 104, pp. 152–166, 2014.

[18] Á. Martín del Rey, "A multi-secret sharing scheme for 3D solid objects," *Expert Systems with Applications*, vol. 42, no. 4, pp. 2114–2120, 2015.

[19] A. C. Rencher, *Methods of multivariate analysis*, Second Edition, Wiley, New York, 2002.

[20] A. Shamir, "How to share a secret," *Communication of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[21] C. C. Thien and J. C. Lin, "Secret image sharing," *Computer & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[22] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 3, pp. 133–138, 1989.

[23] Y. Y. Tsai, "A secret 3D model sharing scheme with reversible data hiding based on space subdivision," *3D Research*, vol. 7, no. 1, Article: 1, pp. 1–14, 2016.

[24] G. Turk, "Generating random points in triangles," *Graphics Gems*, pp. 24–28, Academic Press Inc, San Diego, 1990.

[25] M. Ulutas, G. Ulutas, and V. V. Nabiyev, "Invertible secret image sharing for gray level and dithered cover images," *Journal of Systems and Software*, vol. 86, no. 2, pp. 485–500, 2013.

[26] R. Z. Wang and C. H. Su, "Secret image sharing with smaller shadow images," *Pattern Recognition Letters*, vol. 27, no. 6, pp. 551–555, 2006.

[27] P. C. Wang and C. M. Wang, "Reversible data hiding for point-sampled geometry," *Journal of Information Science and Engineering*, vol. 23, no. 6, pp. 1865–1887, 2007.

[28] Y. S. Wu, C. C. Thien, and J. C. Lin, "Sharing and hiding secret images with size constraint," *Pattern Recognition*, vol. 37, no. 7, pp. 1377–1385, 2004.

[29] D. Zhao, H. Peng, C. Wang, and Y. Yang, "A secret sharing scheme with a short share realizing the (t, n) threshold and the adversary structure," *Computers & Mathematics with Applications*, vol. 64, no. 4, pp. 611–615, 2012.