

科技部

110年度大專學生研究計畫申請書

一、綜合資料：

申請條碼：110CFA1200032



申請人 【學生】	姓 名	林育如	身分證號碼	S22492****
	就 讀 學 校、 科 系 及 年 級	國立暨南國際大學資訊工程學系 (所) 3 年級	電 話	0903015634
	學 生 研 究 計 畫 名 稱	A Study on Random Grid-based Threshold Visual Secret Sharing Scheme		
	研 究 期 間	自110年7月1日至111年2月底止，計8個月		
	計 畫 歸 屬 司 別	工程司		
	研究學門代碼及名稱	E4004 -- 計算機理論與演算法		
	上年度曾執行本部大專學生研究計畫	否		
指導教授	姓 名	阮夙姿	身分證號碼	F22009****
	服 務 機 構 及 科 系(所)	國立暨南國際大學資訊工程學系 (所)		
	職 稱	教授	電 話	049-2910960-4875
補助經費	每位學生每月6,000元研究助學金，研究期間為8個月，共計48,000元			

表C801

(一) 摘要

Visual Cryptography Scheme，縮寫為 VCS 最早被 Naor 和 Shamir 正式定義(1995)[1]。視覺密碼是一種秘密共享的方法，將秘密影像加密成 n 張加密影像(share)，經過堆疊後可還原出原來的影像。本計劃預計設計將一張黑白或彩色的秘密影像分享為 n 張加密影像，使得集合至少 k 張可以還原回秘密影像的新演算法，並且於理論及實驗證明我們的演算法將優於目前所知的研究成果。

(二) 研究動機與研究問題

Kafri 和 Keren 定義隨機網格中的每一個像素只有分為透明或是不透明[2]。且每一個像素是由亂數產生，所以透明像素量會約等於不透明像素量。因此隨機網格的平均光透率(L)為 $\frac{1}{2}$ ，其中光透率的定義為全部的像素量分之透明的像素量。他們並提出三種不同的演算法來加密一張黑白的秘密影像，輸出得到兩張隨機網格 B_1 、 B_2 ，或稱為加密影像，在疊合 B_1 與 B_2 後將可以以人類視覺看出秘密影像 A 。

在 2011 年 Chen 和 Tso 改進了上述的演算法，使得原來是加密成兩張加密影像的方法變成可以加密成 n 張[3]。並使用有門檻(Threshold) k 的方式來還原，也就是疊合至少 k 張可以被人類視覺識別，而此時每張隨機網格的光透率仍為 $\frac{1}{2}$ 。此方法必須產生一個二維

陣列，依據每次新產生的隨機網格對此陣列值做修改，這是為了第 k 張加密影像而作準備。也就是說，前面的 $k - 1$ 張加密影像皆是由亂數所產生，只有第 k 張是根據前面的二維陣列及原圖所產生的，而後面的 $k + 1$ 到 n 張也是由亂數產生的。任何集合少於 k 張加密影像都無法看出秘密影像為何，一定要 k 張或是 k 張以上的加密影像疊起來才能看出個秘密影像。但是此種演算法只要分出來的加密影像越多就會越看不清楚，疊合 t 張後的與秘密影像的對比度會越來越接近 0 ($(\frac{1}{2})^t, k \leq t \leq n$)。還原影像 S 與秘密影像 A 的對比度定義為：

$$\frac{L[S[A_{(0)}]] - L[S[A_{(1)}]]}{1 + L[S[A_{(1)}]]}, \text{ 其中 } L[S[A_{(0)}]] \text{ 為秘密影像 } A \text{ 為白色部分，還原影像 } S \text{ 也為白色的機率；}$$

$$L[S[A_{(1)}]] \text{ 為秘密影像 } A \text{ 為黑色部分，還原影像 } S \text{ 為白色的機率。}$$

因此，本研究的目的就是設計出一種新的演算法，希望選定 k 張或 k 張以上的加密影像疊起來後與原圖秘密影像的對比度可以提升，使得多張疊合後的影像仍舊清晰可辨識。除此之外，再進一步增加以 XOR 運算為解密方式[4]，並加入以彩色影像為秘密影像的研究對象使得我們的新方法能夠更有彈性的被多方應用。

(三) 文獻回顧與探討

首先定義兩像素所疊合的所有結果，其中 1 代表黑色，0 代表白色的像素，其中 \otimes 代表疊合運算，也就是 OR 運算。

B_1	B_2	$B_1 \otimes B_2$
0	0	0
0	1	1
1	0	1
1	1	1

1987 年 Kafri 和 Keren 提出了能產生兩張隨機網格的演算法[2]，其中一個如下：

演算法 1:

```

Generate a random grid  $B_1$ ,  $L(B_1) = \frac{1}{2}$ 
for (  $i = 0 ; i < w ; i++$  )
    for (  $j = 0 ; j < h ; j++$  )
        if (  $A[i][j] == 0$  )  $B_2[i][j] = B_1[i][j]$  ;
        else  $B_2[i][j] = B_1[i][j]$  ;
output (  $B_1, B_2$  )

```

下表為演算法 1 疊合後的光透率，其中 A 代表原始秘密影像的像素值， B 代表加密影像的像素值：

	A	B_1	B_2	$B_1 \otimes B_2$	光透率
演算法 1	□	□ ■	□ ■	□ ■	$\frac{1}{2}$
	■	□ ■	■ □	■ ■	0

在 2011 年 Chen 和 Tso 將此演算法延伸出可以產生多張片段的 $(k, n) - VCS$ [3]如下。

演算法 2:

```

 $k$ -out-of- $n$ _RandomGrids() {
     $B_1$  create by random
    if (  $A == 0$  )  $\widetilde{B_2} = B_1$  ;
    else  $\widetilde{B_2} = \overline{B_1}$  ;

    for (  $x = 2 ; x < k ; x++$  ) {
         $B_x$  create by random
        if (  $\widetilde{B_x} == 0$  )  $\widetilde{B_{x+1}} = B_x$  ;
    }
}

```

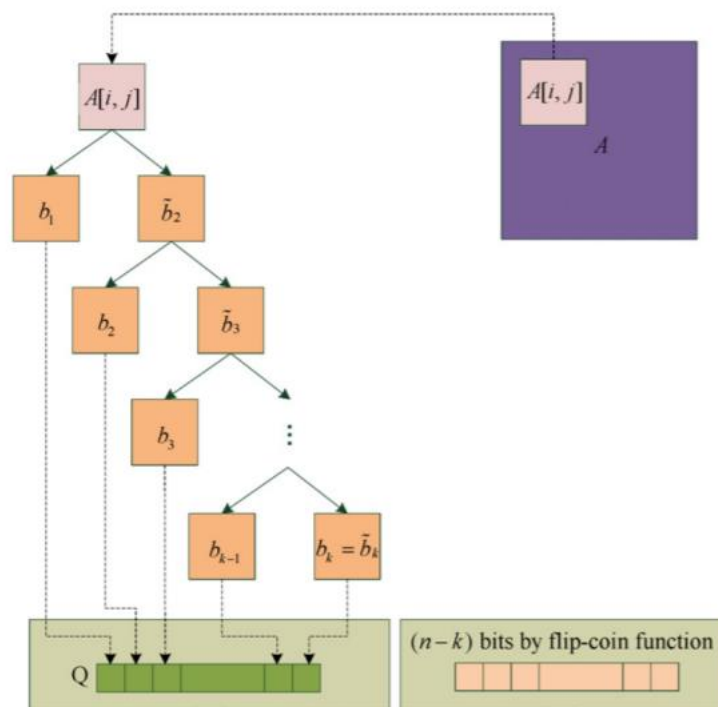
```

    else  $\widetilde{B_{x+1}} = \overline{B_x}$ ;
  }
   $B_k = \widetilde{B_k}$ ;
  for ( $x = k + 1$ ;  $x < n + 1$ ;  $x++$ ) {
     $B_x$  create by random
  }
  Randomly arrangement  $B_1, B_2, \dots, B_n$ ;
}

```

此法所產生的多重隨機網格樹狀圖如下所示：

T.-H. Chen, K.-H. Tsao / The Journal of Systems and Software 84 (2011) 1197–1208



2013 年 Guo、Liu 和 Wu 針對[3]其還原之後的對比度進行改良

[5]，使得其還原之後能夠看得更加清楚。演算法如下：

演算法 3:

```

k-out-of-n_RandomGrids(){
   $B_1$  create by random
  if ( $A == 0$ )  $\widetilde{B_2} = B_1$ ;
  else  $\widetilde{B_2} = \overline{B_1}$ ;
  for ( $x = 2$ ;  $x < k$ ;  $x++$ ) {

```

```

     $B_x$  create by random
    if (  $\widetilde{B_x} == 0$  )  $\widetilde{B_{x+1}} = B_x$  ;
    else  $\widetilde{B_{x+1}} = \overline{B_x}$ ;
}
 $B_k = \widetilde{B_k}$ ;

 $B_{k+1}$  create by random;
if (  $A == 0$  )  $\widetilde{B_{k+2}} = B_{k+1}$  ;
else  $\widetilde{B_{k+2}} = \overline{B_{k+1}}$ ;
for (  $x = k + 2$ ;  $x < n$ ;  $x++$  ) {
     $B_x$  create by random
    if (  $\widetilde{B_x} == 0$  )  $\widetilde{B_{x+1}} = B_x$  ;
    else  $\widetilde{B_{x+1}} = \overline{B_x}$ ;
}
 $B_n = \widetilde{B_n}$ ;

Randomly arrangement  $B_1, B_2 \cdots B_n$ ;
}

```

Yan 等人在 2015 年發表的論文[4]中，改良了[3]中的演算法，在
 原來的功能上加上 XOR 的功能，使得其演算法可擁有多種的解法，
 增加其使用空間。 \oplus 代表 XOR 運算，演算法如下：

演算法 4:

```

k-out-of-n_RandomGrids(){
     $B_1$  create by random
    if (  $A == 0$  )  $\widetilde{B_2} = B_1$  ;
    else  $\widetilde{B_2} = \overline{B_1}$ ;
    for (  $x = 2$ ;  $x < k$ ;  $x++$  ) {
         $B_x$  create by random
        if (  $\widetilde{B_x} == 0$  )  $\widetilde{B_{x+1}} = B_x$  ;
        else  $\widetilde{B_{x+1}} = \overline{B_x}$ ;
    }
     $B_k = \widetilde{B_k}$ ;
    for (  $x = k + 1$ ;  $x < n + 1$ ;  $x++$  ) {
         $B_x$  create by random
    }
    if (  $A != B_1 \oplus B_2 \cdots B_n$  ) {
         $p$  selected from 1 to  $n$  by random
    }
}

```

$$\begin{aligned}
 & B_p = \overline{B_p}; \\
 & \} \\
 & \text{Randomly arrangement } B_1, B_2 \cdots \cdots B_n; \\
 & \}
 \end{aligned}$$

(四) 研究方法及步驟

我們預計進行的研究方法及步驟如下：

步驟一：

實作[3]中的演算法，前 $k - 1$ 張片段由亂數產生，第 k 張則經由計算產生，後面 $k + 1$ 張到 n 張也是由亂數產生的。舉例如下：

當加密影像的張數為 3， $k = 2$ 時：

A	B_1	B_2	B_3	$B_1 \otimes B_2$	$B_1 \otimes B_3$	$B_2 \otimes B_3$	$B_1 \otimes B_2 \otimes B_3$
□	□	□	□ ■	□ □	□ ■	□ ■	□ ■
	■	■	■ □	■ ■	■ ■	■ ■	■ ■
■	□	■	■ □	■ ■	■ □	■ ■	■ ■
	■	□	□ ■	■ ■	■ ■	□ ■	■ ■

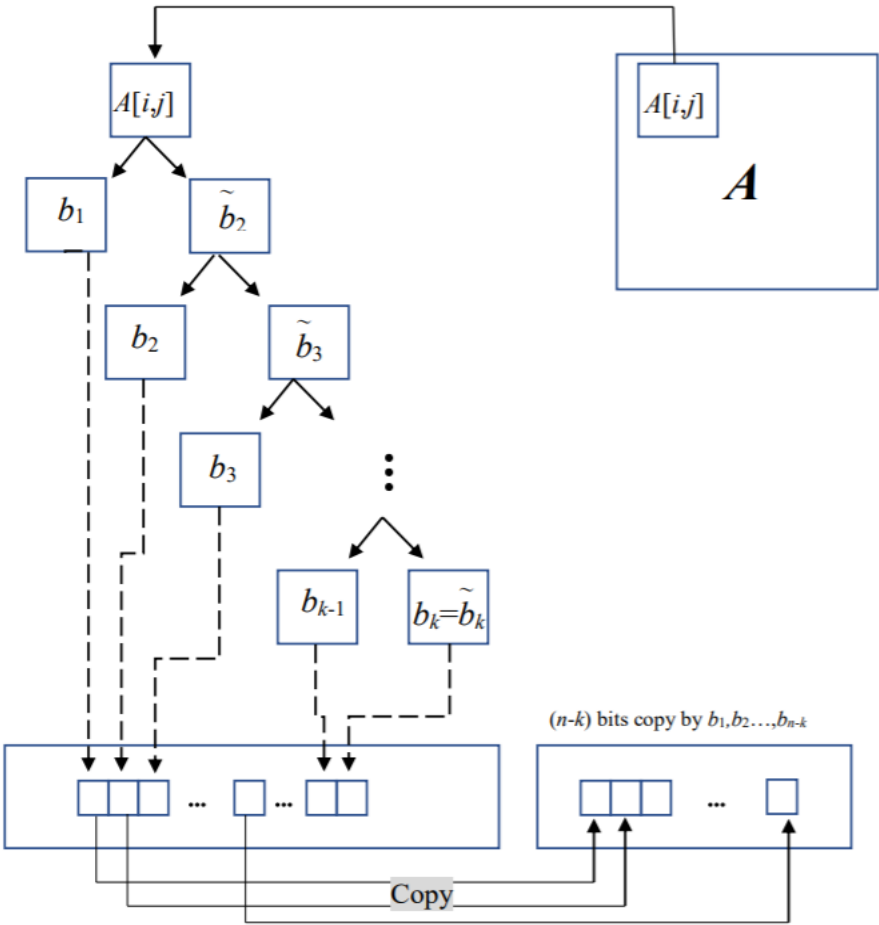
由上表可看出疊合兩張後白色部分的光透率 $= \frac{4}{12} = \frac{1}{3}$ ，黑色部分的光透率 $= \frac{2}{12} = \frac{1}{6}$ ，經過計算與秘密影像的對比度為 $\frac{\frac{1}{3} - \frac{1}{6}}{1 + \frac{1}{6}} = \frac{1}{7}$ 。疊合三張後白色部分的光透率 $= \frac{1}{4}$ ，黑色部分的光透率 $= 0$ ，經過計算與秘密影像的對比度為 $\frac{\frac{1}{4} - 0}{1 + 0} = \frac{1}{4}$ 。因此可以看出原秘密圖形。下表為[3]中，不同 k 、 n 、 t 情況下實驗作出的對比度。

(k, n)				
	$t = 2$	$t = 3$	$t = 4$	$t = 5$
(2, 2)	0.501165			
(2, 3)	0.142115	0.248105		
(3, 3)		0.250455		
(2, 4)	0.06793	0.116515	0.12393	
(3, 4)		0.057075	0.124555	
(4, 4)			0.123935	
(2, 5)	0.04091	0.06905	0.073195	0.062645
(3, 5)		0.022485	0.04839	0.063065
(4, 5)			0.023985	0.062515
(5, 5)				0.06297

由此可以看出，當每張加密影像的光透率為 $\frac{1}{2}$ ，而共分為 n 張加密影像時，疊合 n 張後白色的光透率會降為 $\frac{1}{2^{n-1}}$ ，而黑色部分仍維持為 0。同理當 n 越大即使疊合全 n 張也將不易看清楚原圖為何，與原圖的對比度如上表所示越來越接近 0。

步驟二：

改良[3]中演算法，在產生 $k+1$ 到 n 張加密影像的過程中加入自己的想法。修改成： $k+1$ 複製第一張， $k+2$ 複製第二張，以此類推至第 n 張。想法如下圖所示：



舉例如下：

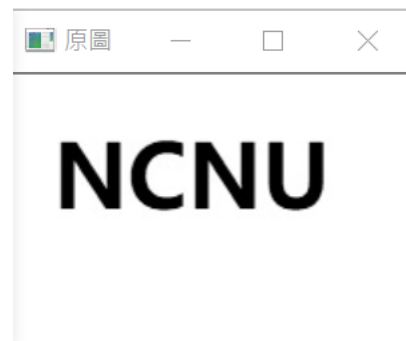
1. 加密影像張數為 3 時， $k=2$ ：

A	B_1	B_2	B_3	$B_1 \otimes B_2$	$B_1 \otimes B_3$	$B_2 \otimes B_3$	$B_1 \otimes B_2 \otimes B_3$
□	□	□	□	□	□	□	□
	■	■	■	■	■	■	■
■	□	■	□	■	□	■	■
	■	□	■	■	■	■	■

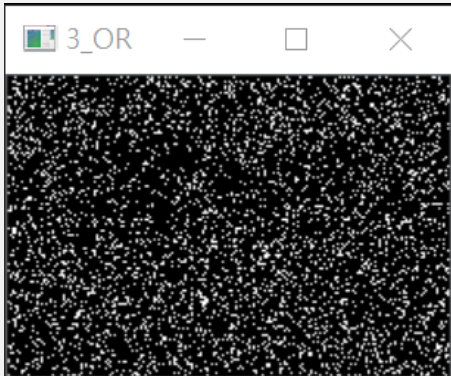
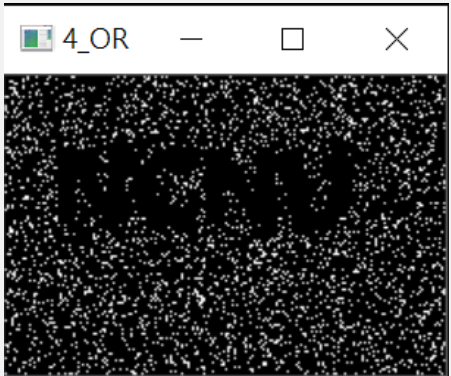
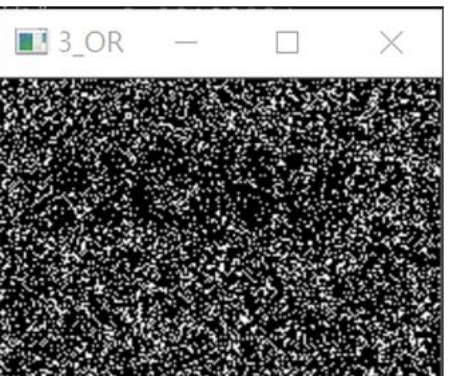

從上表可知，由上表可看出疊合兩張後白色部分的光透率 $= \frac{3}{6} = \frac{1}{2}$ ，黑色部分的光透率 $= \frac{1}{6}$ ，經過計算與秘密影像的對比度為 $\frac{\frac{1}{2} - \frac{1}{6}}{1 + \frac{1}{6}} = \frac{2}{7}$ 。疊合三張後白色部分的光透率 $= \frac{1}{2}$ ，黑色部分的光透率 $= 0$ ，經過計算與秘密影像的對比度為 $\frac{\frac{1}{2} - 0}{1 + 0} = \frac{1}{2}$ 。由此可看出，與[3]中演算法對比與秘密影像的對比度得到很高的提升。

實驗結果如下：

原圖



$n = 3$ $k = 2$	共分三張，疊合其中兩張後	共分三張，疊合其中三張後
[3]中 演算法		
改良後 演算法		

$n = 4$ $k = 3$	共分四張，疊合其中三張後	共分四張，疊合其中四張後
[3]中演算法		
改良後演算法		

由上面實驗結果可以看出，此法可以將疊合後的結果會變的不清楚的問題改善，讓圖像更明顯的可辨識。

步驟三：

在上一步驟中可看出經由我們改良之後的演算法在解密後的可辨識度有所提升，在此步驟我們將進行分析計算出對比度的理論值公式，以證明演算法的正確與改進。

步驟四：

當改良[3]中的演算法有了成果之後，下一步將針對增加多種解密功能議題做研究。根據 2015 年 Yan 等人發表的論文[4]進行改良。預期可設計出運用隨機網格加密並且擁有多種解密方式(OR 運算及 XOR 運算並存)之演算法。

步驟五：

根據上述的結果,我們將延伸至彩色圖片的加密與解密,使其也可以做到多種方式解密和有高對比度。

步驟六：

最後的結果，我們將其與論文[3]、[4]、[5]進行比較，探討其可以繼續改良的地方。

(五) 預期結果

首先預計將能夠改良[3]中的演算法，使得每張加密影像依舊是隨機網格且不能看出秘密影像，疊合之後與秘密影像的對比度能夠提高，也就是說可以更加清晰地辨識出秘密影像。其次增加一種解密方法，期望近一步提升還原影像的對比度。最後增加在彩色圖片上的研究，使得此演算法的運用範圍可以更加廣泛。

(六) 參考文獻

- [1] Naor, M., & Shamir, A. (1994, May). Visual cryptography. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 1-12). Springer, Berlin, Heidelberg.
- [2] Kafri, O., & Keren, E. (1987). Encryption of pictures and shapes by random grids. Optics letters, 12(6), 377-379.
- [3] Chen, T. H., & Tsao, K. H. (2011). Threshold visual secret sharing by random grids. Journal of Systems and Software, 84(7), 1197-1208.
- [4] Yan, X., Wang, S., Niu, X., & Yang, C. N. (2015). Random grid-based visual secret sharing with multiple decryptions. Journal of Visual Communication and Image Representation, 26, 94-104.
- [5] Guo, T., Liu, F., & Wu, C. (2013). Threshold visual secret sharing by random grids with improved contrast. Journal of Systems and Software, 86(8), 2094-2109.

(七) 需要指導教授指導內容

在研究論文時遇到許多困難，對於在視覺密碼領域中的專有名稱似懂非懂，在看演算法分析的時候也有許多困惑，也需要指導教授的指點。在改良演算法時遇到瓶頸不知道從何下手，演算法的理論值分析開始打結的時候，亦需要指導教授的指點與從旁輔導。

大專學生研究計畫指導教授初評意見表

一、學生潛力評估：

林育如同學於學校的在校成績並不是特別頂尖的，但也一直維持中上程度。她的學習態度一直很好，修課至今未曾有過不及格的科目，她對於各方面的課程都很有興趣，廣泛的學習在各個領域的課程，是位有想法主動又好問的學生。育如此次跟隨我作視覺密碼方面的專題研究，表現得很積極主動且投入；在指點她方向後，在很短的時間之內即有研究成果；對於有錯漏的地方，也能認真思考修正；對於問題，也能舉一反三的自行推論。比較印象深刻的是，在我尚未要求她將論文上的演算法實做出來時，她已經在很短的時間內自己完成了，速度比同時期的碩士研究生快多了！而在我提點了一個新的想法之後，育如能夠很快抓到重點地將其完整呈現，並實作出結果。相信這樣有想法、負責任，且對研究俱主動及熱情的學生，若給予相當時間的鼓勵與協助，必能有很好的研究成果。

二、對學生所提研究計畫內容之評述：

視覺密碼問題(Visual Cryptography)是資訊安全問題的一個分支，國內外皆有許多學者廣泛的研究這方面的問題。將視覺密碼的概念結合 (k, n) -門檻機密分享機制，是一個實用的主題；同時可以使用 OR 及 XOR 運算方式解密，則為最近幾年研究者專注的方向；擴展研究成果到彩色圖片則是未來發展的趨勢。因此育如提出的研究問題是相當具有研究價值的。從她初步的實驗結果可以看出，計畫中所提出的演算法確實安全可行，並且大幅改進了前人的研究成果。而接下來預計將進行理論上的證明、及後續以 XOR 運算解密及對彩色圖片的研究，將可使這個問題的研究面更完整。預計本計畫的研究成果將可順利地發表於國際會議或期刊中。

三、指導方式：

控制研究進度及方向，並且給予適時的幫助與教導。首先預計將先指導他一些關於視覺密碼及資訊安全的基本概念。其次對於論文研讀與研究方向給予幫助：針對 (k, n) -門檻機密分享機制、同時可以使用 OR 及 XOR 運算方式解密的演算法之特性予以深入探討，透過學習一些已發表的演算法及證明做為參考，指導她從中獲得一些做研究的方法。而針對育如所提出的想法，撰寫出的程式結果，指出其缺失或可以改進之處。對於理論證明的方法給予指導、以及說明如何與前人研究成果進行比較。最後助其整理並且驗證其研究成果使其順利於國際會議或期刊中發表。

四、本人同意指導學生瞭解並遵照學術倫理規範；本計畫無違反學術倫理。

指導教授簽名：



110 年 2 月 25 日

國立暨南國際大學學生歷年成績表

系組別：資訊工程學系

姓名：林育如

學號：107321048

第一學年 107年9月至108年6月					第二學年 108年9月至109年6月					第三學年 109年9月至110年6月													
科	目	第一學期		第二學期		科	目	第一學期		第二學期		科	目	第一學期		第二學期		科	目	第一學期		第二學期	
		學分	成績	學分	成績			學分	成績	學分	成績			學分	成績	學分	成績			學分	成績	學分	成績
通	Excel 原理與進階應用	2	91			選	UNIX使用入門	3	75			選	Python語言程式設計	3	75								
通	永續能源、資源暨碳管理	3	86			選	工程數學	3	77			選	系統程式	3	82								
通	生態旅遊與城鄉自然資源規劃	3	77			通	世界城市和台灣地方	3	89			選	計算機組織與結構	3	85								
通	在地實踐自主學習	2	95			通	資工系英文二	2	89			選	專題(一)	2	90								
通	科技學院國文I(上)	2	88			選	資料結構與演算法(一)	3	71			選	資料壓縮	3	86								
必	計算機概論	3	79			選	電腦圖學	3	91			選	電腦與資訊安全	3	90								
必	微積分(上)	3	72			選	邏輯設計與實驗(二)	3	93			選	語言學習與科技(全英語授課)	3	80								
通	資工系大一體育(上)	0	86			選	LISP程式設計			3	60	選	VR/AR應用實作			3	缺						
通	資工系服務學習(上)	0.5	92			通	台股投資法則			2	99	選	作業系統			3	缺						
通	資工系英文(上)	2	91			通	全球化現象導論			2	89	選	專題(二)			2	缺						
通	離散數學	3	66			通	資料結構與演算法(二)			3	93	選	組合數學			3	缺						
通	大一體育(下：運動與體重控制)			0	88	選	數位電子學			3	85	選	智慧型行動裝置軟體設計			3	缺						
通	政治哲學概論	2	77			必	線性代數			3	73	選	微算機實驗			1	缺						
通	科技學院國文I(下)	2	86			共	機率			3	79												
通	從經濟學看世界	3	84				體育:高爾夫球			0.5	90		以下空白										
必	程式設計	3	78				體育:游泳			0.5	90												
必	微積分(下)	3	72																				
通	資工系服務學習(下)			0.5	90																		
通	資工系英文(下)	2	98																				
通	戲劇欣賞	2	82																				
必	邏輯設計與實驗(一)	3	83																				
學 期 平 均 成 績		81.53		82.05		學 期 平 均 成 績		83.3		81.8		學 期 平 均 成 績		83.7		0		學 期 平 均 成 績					
修 習 學 分 數		23.5		20.5		修 習 學 分 數		20		20		修 習 學 分 數		20		15		修 習 學 分 數					
實 得 學 分 數		23.5		20.5		實 得 學 分 數		20		20		實 得 學 分 數		20		0		實 得 學 分 數					
學 分 累 計		23.5		44		學 分 累 計		64		84		學 分 累 計		104		104		學 分 累 計					
操 行 成 績		85		85		操 行 成 績		85		85		操 行 成 績		85				操 行 成 績					
附	通識講座:IoT Applications on Smart City: The IoTalk Approach(林一平)					附	通識講座:一開口撩人又聊心~助你脫單的有效策略(諮商中心主辦)(瑪那					附						附					
註	通識講座:島嶼DNA：由台灣人疾病人類學看臺灣人祖先的多元及親海性格(陳耀昌)					註	熊-諮商心理師)					註						註					
	通識講座:因應新冠肺炎的實與虛(楊志良)						通識講座:生命重生大力量(蘇蕙鈺)																
	通識講座:推石頭的薛西佛斯(諮商中心主辦)(徐嘉凱)																						



目前總學分： 104

目前總成績： 82.44

目前班總排名： 18/55 32.73%

目前系總排名： 18/55 32.73%

一百一十年二月二十三日

第1頁共1頁