科技部補助

大專學生研究計畫研究成果報告

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

＊計畫 ＊

＊ ： 立體聲的資料隱藏 ＊

＊名稱 ＊

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

執行計畫學生：李東岳

學生計畫編號：103-2815-C-260-024-E

研究期間：103年7 月1 日至104年2 月底止，計8 個月

指導教授：吳坤熹

處理方式(請勾選)：□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：

中華民國104年2月28日

**摘要**

由於資訊科技的發展以及網際網路的便利性，使得資料得以快速傳輸。為了避免機密資料輕易被竊取，資料加密及資訊隱藏的技術成為了重要的研究課題。傳統的資訊隱藏使用最低位元替換藏密法（LSB），優點是很難被人類視覺系統察覺，但是藏密量不多。像素值差異藏密法（PVD）將機密訊息透過更改兩兩相鄰之像素值差異，按規則藏入影像中，大幅增加藏密量。矩陣嵌入(matrix embedding)是透過漢明碼的特性來隱藏資料，本文將會改良matrix embedding隱藏法，並與PVD做結合。

關鍵字：PVD，Matrix embedding，Hamming code，LSB，資訊隱藏。

1. **前言**

在這資訊爆炸的時代，我們能在網路上傳遞任何媒體資料。在傳送資料前，為了不讓有心人士容易竊取我們的資料，可以將資料進行加密的動作，接收者接收時再進行解密。但若有心人士發現此資料是密碼，就會曉得這是有價值的資料，更提高他進行破解密碼的動機，這樣就會造成反效果。因此現今有了資料隱藏這項技術，它能夠將機密資訊隱藏在媒體檔案裡面，這樣一來只需要傳送一個看似正常的媒體檔案，就能夠將機密資訊傳送出去。

Bender等學者於1996年所提出的最低位元替換藏密法（Least Significant Bit, LSB）[1]，優點是藏密後很難被人類視覺系統察覺異狀，缺點是藏密量最多僅1bpp（bit per pixel）。此外，此LSB藏密技術容易被 Regular-Singular（RS）[2]偵密技術所察覺。Wu與Tsai學者於2003年提出的像素值差異演算法(Pixel Value Differencing, PVD)[3]，將祕密訊息透過更改兩兩相鄰之像素值差異，按規則藏入影像中，此方法不但增加藏密量，並且可避免被RS偵密技術所察覺。由於PVD在相鄰像素值差異小的時候，藏密量不高，在2005年，Hwang等學者[4]結合了改良後的LSB與PVD，將兩種演算法的優點結合在一起，提升了1.5倍的藏密量。

在矩陣嵌入(matrix embedding)裡，漢明碼(hamming code)資料隱藏是透過錯誤更正碼計算徵狀值(syndrome)的概念進行資料隱藏，其優點是掩護序列所更動的位元數會小於所藏入的位元數，藏密量相當驚人，固本篇論文嘗試將PVD與matrix embedding結合。在結合過程中發現漢明碼隱藏的演算法套用在影像中效果不佳，所以在文中也提出將漢明碼資料隱藏進行改良之法。

1. **研究目的**

之前閱讀了一篇IEEE上發表的論文，它是將資料經由Pixel Value Differencing(PVD) 的方式隱藏在兩個audio檔案裡面，為了讓資料都固定藏在最後兩個bit，它還特地將每個區間值設為固定，這麼一來會有兩個缺點：第一，每次要藏資料必須要有兩個audio檔案；第二，可以藏的資料量就會被壓縮。如果將兩個單聲道的audio檔案改成一個雙聲道檔案，這樣只需要一個stereo audio檔案就能夠進行PVD做資料隱藏；而區間值如果能按照原本PVD的精神，依照不同的差值來藏不同的資料量，capacity就能增加。

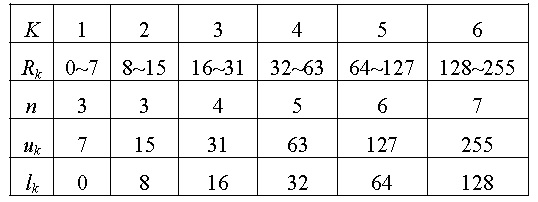
基於上述的研究動機，本研究問題為：

1. 在stereo audio裡進行PVD隱藏資料。
2. PVD的區間大小修改為依據差值做調整。
3. **文獻探討**

**1. 像素值差異藏密法**

在2003年Wu學者與Tsai學者所提出的像素值差異藏密法(PVD)[3]中，機密訊息是藏在影像中相鄰像素的差值裡。如果將機密訊息直接替換成差值，那麼圖像隱藏前後的差異用肉眼即可辨識。因此我們需要將像素差值做分類，讓差值只在該特定區間內做替換，如下表所示：

表一 依照差值大小分為六個區間



表一中Rk為相鄰像素差值，uk與lk為該區間的最大值與最小值，n = log2(uk - lk + 1) ，為可藏入的位元數，以下為PVD演算法：

步驟一：經由式子(1)計算出影像中相鄰像素Pi與Pi+1差值d。

d = | Pi - Pi+1 | (1)

步驟二：判斷d屬於哪個區間，向機密訊息取n個位元後，將二進位的值轉為十進位計算出b。

步驟三：依照式子(2)計算出d’：

d’ = (2)

步驟四：[4]依照式子(3)計算出新的像素值P’i與P’i+1，m = |d’ – (Pi - Pi+1)|。

(P’i,P’i+1 ) =

(3)

要擷取訊息時，依照式子(4)計算出d’後，判斷d’屬於哪個區間，計算出d’ – lk便可得到訊息。

d' = | P'i - P'i+1 | (4)

例子：假設Pi = 50，Pi+1 = 30，d = 20 R3，機密訊息4個位元假設為(1010)2，b = 10，d’ = 26，P’i = 50 +3 = 53，P'i+1 = 30 - 3 = 27，隱藏完成。擷取訊息時，計算出d’ = 53 – 27 = 26，26 – 16 = (10)10 = (1010)2 得到訊息。

**2. Amplitude Differencing**

2010年Shafi等學者將PVD演算法應用在聲音上，掩護資料為兩個大小相近的音訊檔案，而機密訊息藏於兩個檔案相對應位置chunk data的差值，做法如下：

步驟一：計算出兩個檔案A、D相對應位置Ai、Di的差值d = |Ai - Di|。

步驟二：將PVD的區間值改為固定16，向機密訊息取4個位元，把取出來二進位的值轉為十進位。

步驟三與步驟四跟PVD演算法相同，將像素值Pi、Pi+1改為Ai、Di，P’i、P’i+1改為A’i、D’i。

例子：假設Ai = 50，Di = 30，d = 20 ，為16~31區間，機密訊息4個位元假設為(1010)2，b = 10，d’ = 26，A’i = 50 +3 = 53，D’i = 30 - 3 = 27，隱藏完成。擷取訊息時，計算出d’ = 53 – 27 = 26，26 – 16 = (10)10 = (1010)2 得到訊息。

**3. Interaural Phase Difference and Minimnm Audible Angle**

在1958年Mills提出了Minmum Audible Angle(MAA)，關於人耳對於聲音的方位辨識。實驗如圖一，以測試者為中心，將聲源A、B分別放在測試者左右兩側，讓A、B兩點的中點與測試者所形成的直線與直線AB垂直。實驗時讓聲源AB隨機發出聲音，讓測試者分辨是在左邊或是右邊，θ為變數，測試發現θ在1˚以內時測試者無法分辨聲音來源為左邊或是右邊。



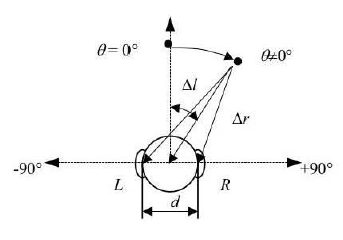
圖一 MAA實驗

利用MAA概念，可以計算出interaural phase difference(IPD)最大值，IPD的意義為聲源到左右耳的相位角差值，也就是計算差了多少個波長。首先計算出聲源到左耳與到右耳的距離差值Δd，圖二為聲源到兩耳的示意圖，Δl為聲源到左耳的距離，Δr為聲源到右耳的距離，Δd為兩者的距離差，d為左耳到右耳的距離，r為聲音來源到中心點位置。假設目前方位角為θ，則：

∆r = (5)

∆l = (6)

∆d = | ∆r - ∆l | (7)



圖二 azimuth plane

接下來計算IPD，IPD(Φ)可表示為頻率f的函式：

Φ = ∆d × × 2π or ∆d × × 360˚ (8)

其中c為聲音在空氣中的傳送速率，約344m/s，由於 v = f × λ，故Δd × 可視為 ，也就是聲源到兩耳的波程差，最後乘上2π或360˚變成相位角。

利用MAA概念，當θ ≤ 1˚時，Φ計算出的最大值Φmax為

-3.104 × 10-3 × f，也就是說，左右耳所接收到特定頻率的波的相位角差值小於Φmax的話，人耳分辨不出聲音來自左方或右方，此時更改資料不易被發現，便能夠嵌入資料。 透過傅立葉轉換能夠計算得到某頻率的相位角，經由psychoacoustical phase threshold式子(9)可以得知該頻率能否進行資料隱藏：

cos{phase[XR(fi)] – phase[XL(fi)]} < cos(-3.104 × 10-3 × fi) (9)

phase[XR(fi)]為右聲道在頻率為fi的相位角，傅立葉轉換會得到頻率為fi的複數a + bi，式子(10)的φ即為此頻率的相位角：

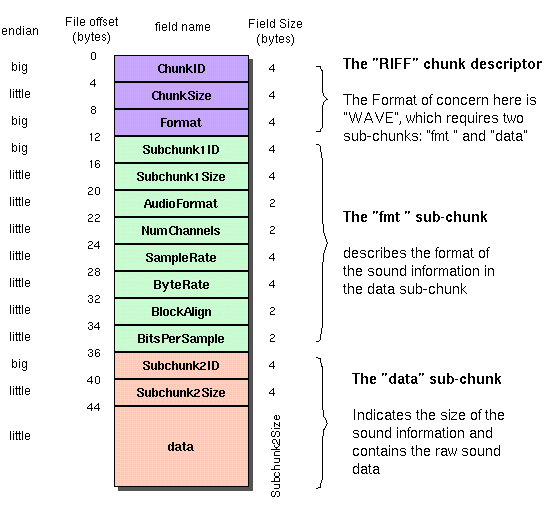
φ = tan-1() (10)

1. **研究方法**

本研究實做環境如下：

* 作業系統：Ubuntu 12.04
* 語言：C++
* 編譯器： gcc 4.6.3
* 引用library：libsndfile

要在雙聲道進行資料隱藏，首先要先了解支援雙聲道格式的檔案，本研究採用WAV檔，他的chunk data是沒有被壓縮的，處理起來較方便，圖二為WAV格式，雙聲道儲存格式為每兩個byte為一組，第一個byte為左聲道振幅，第二個byte為右聲道振幅。



圖二 WAV格式

接下來為本研究的資料隱藏方法：

步驟一：將左聲道的資料每8個一組經過離散傅立葉轉換，右聲道的資料每8個一組經過傅立葉轉換，便能得到左右聲道相對應頻率的複數。



1. **結果與討論**
2. **參考文獻**