行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　　　※
※　　　　　　　資訊隱藏於聲音之研究　　　　　　　　※
※　　　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：■個別型計畫　　□整合型計畫
計畫編號：NSC　90－2213－E－009－127－
執行期間：90 年 08 月 01 日至 91 年 07 月 31 日

計畫主持人：陳玲慧 教授
共同主持人：
計畫參與人員：

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

執行單位：國立交通大學資訊科學學系

中　華　民　國　91 年　8　月　　　日

行政院國家科學委員會專題研究計畫成果報告

資訊隱藏於聲音之研究

A Study on Data Hiding in Audio Signals

計畫編號：NSC 90-2213-E-009-127

執行期限：90 年 8 月 1 日至 91 年 7 月 31 日

主持人：陳玲慧　國立交通大學　資訊科學系

一、中文摘要

資訊隱藏是將資訊藏入數位媒體中以達到掩護機密資訊的目的。現今的資訊社會，大量的資訊如：文件、影像、聲音等均藉由公開的網路來進行傳遞，如何保護機密資訊在傳遞的過程中不被嫖竊者以非法手段竊取就成為一個重要的問題。一般傳統的方法是將機密資訊在傳遞前先使用密碼學方法將機密資訊加密，經過加密後的機密資訊成為一些看起來像是亂碼的雜訊，最後再進行傳遞。可是這種方法將導致一種後果，那就是更激發了攻擊者的攻擊心態，因此，資料隱藏的技巧提供了一個好的解決方法，使機密資訊能逃過攻擊者的攻擊而安全地送達目的地。

目前已有一些嵌入機密資訊於聲音中的方法被提出，然而這些方法所能藏入的資料量太小只能應用於 Watermarking，若要隱藏大量資訊將有困難，這對於擁有大量多餘資訊的聲音而言是一種相當大的浪費。另一方面，無法抵擋壓縮也是另外一個問題，因此實用性就大為減低。

本計劃擬將任何形式的機密資訊隱藏於聲音格式中，且是人類聽覺無法覺察的。隱藏技巧主要將依靠一些聲音的特性，例如：聲音大的會將聲音小的遮蓋掉。利用這些特性，本計劃將提出二個方法，一個是將機密資訊隱藏於時間域之聲音檔中；另一個是將機密資訊隱藏於頻率域之聲音檔，希冀能夠達到抵擋檔案的壓縮與隱藏資訊量的提昇兩大目標，以提昇嵌入機密資訊於聲音中之實用性。

關鍵詞：資訊隱藏、聲音、機密資訊

Abstract

Data hiding is a technique to embed data in a digital media to cover secret information. In today's digital world, a great deal of informations including text, images, audio, and video, etc. are usually distributed through a public network. Thus, how to keep privacy becomes a hot topic. The general method is to use cryptographic techniques, the private information is scrambled using an encryption transformation before it is distributed. Since the scrambled information looks like noise, this will make someone try to attack it. To treat this disadvantage, data hiding provides a solution.

Several techniques for data hiding in audio signals have been developed. But, then do not provide enough capacity to carry a bigger secret data. In this project, we will provide two data hiding methods which will embed secret information in a digital audio media. One will embed data in a audio file expressed in the time domain, it will provide high embedding capacity. The other in the frequency domain, it can resist audio compression under adding the error control

code in the secret information. These two methods will utilize some characteristics of sound, for example, loud sound can mask out quiet sound.

Keywords: data hiding、audio、secret information

二、緣由與目的

隨著電腦與資訊科技的日漸普及，相關的應用與發展也日益成熟。網路世代的興起，使得人們利用網路來傳送重要訊息的頻率逐漸增加。雖然快速卻也顯得並不安全，因此如何在傳送的過程中保護所傳送的資訊而不被非法剽竊亦顯得相當重要。也因此許多大家所熟悉的對稱與非對稱的加密方法如 DES、RSA 相繼地被提出，也提供了部分的安全性。然而，一般的加密方法，卻導致一種後果，那就是更激發攻擊者的攻擊心態。

為了避免上述的缺點，資料隱藏的技巧提供了一個好的解決方法，將機密資料藏入數位媒體中以達到掩護機密資訊的目的，使機密資訊能逃過攻擊者的攻擊而安全地送達目的地。就如同生物界中一些比較弱小的生物利用本身顏色與環境顏色相似來達到欺騙與躲避天敵的攻擊。

由於聲音格式在現今的資訊社會流通非常普遍，因此我們嘗試將我們的機密資訊藏在聲音檔案中。一個聲音檔案可以利用細微的改變來重新改寫每一個聲音訊號而達到隱藏資訊的目的，但如何使所藏入的資訊容量能儘可能的大卻又不會破壞原來聲音的品質是非常重要且須研究的。在所有聲音格式中，WAV File 流通非常普遍，且它提供聲音訊號的所有資訊，因此可供隱藏資訊的容量非常大，故我們將選擇此種格式來隱藏我們的機密資訊。一般來說，資訊隱藏於聲音中必須滿足下列幾點要求：

- 不能被感知：當機密資訊隱藏於聲音中時不能影響原來聲音訊號的品質。
- 不能統計方法察覺：機密資訊不能被統計的方法所察覺。
- 容易取出：機密資訊應當可以不使用原來的聲音訊號就可以很容易地取出。

現今已經有一些隱藏資訊於聲音中的方法被提出，一是將機密資訊藏於時間域中(Time-Domain Coding)，另一種方法是將機密資訊藏於頻率域中(Frequency-Domain Coding)，接下來我們對此兩種方法做一敘述。

在 Time-Domain Coding 的部分，Low Bit Coding 是一項簡單的技術，它的做法是將每一個聲音訊號樣本的最後一個 Bit 替換成機密資訊，此種方法能提供非常大的隱藏資訊容量，一般來說，一個取樣頻率為 44.1 KHz 的聲音檔案擁有一秒鐘可藏 44.1 Kbits 的隱藏容量。但是這樣的隱藏方式會有幾個缺點，第一個缺點就是不夠安全，每一個聲音訊號都是隱藏於固定的容量與位置，這對一個有心的剽竊者而言並不能提供太大的安全性而容易被破解。第二個缺點就是容量還是不夠大，對於一個 CD 品質的聲音檔案而言，16 個位元的解析度只隱藏 1 個位元似乎有點浪費。

在 Frequency-Domain Coding 的部分，Phase Coding 是將相位替換成機密資訊的一種資訊隱藏的作法，

- 首先將聲音訊號分割成一段段的 Segment。
- 利用 Discrete Fourier Transform (DFT) 將每一個 Segment 的聲音訊號轉換到頻率域上。
- 將頻率域上的實部與虛部的直角座標表示法改以長度與角度的極

座標表示法表示。

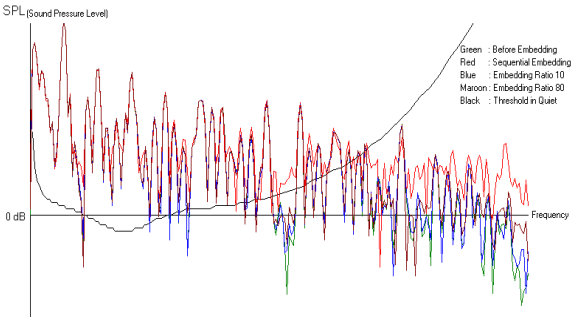
- 將每個 Segment 間相同頻率位置的相位關係紀錄下來。
- 將第一個 Segment 的相位替換成所要隱藏的資訊，若為 0 則為 $-\theta/2$，若為 1 則為 $\theta/2$。
- 依據先前所紀錄的 Segment 間的相位關係重建所有 Segment 的相位。
- 將重建過的相位與原始長度的極座標改回實部與虛部的直角座標表示法。
- 利用 Inverse Discrete Fourier Transform (IDFT)重建聲音訊號。

經過上述步驟就可以將機密資訊藏入聲音中，但是 Phase Coding 的方法所能藏入的資訊容量過小，也就是說當我們將聲音訊號切割成 Segment 時就已經決定了所能藏入資訊的量，若一個 Segment 長度為 512 Samples 則所能藏入的資訊量就只有 512 bits。

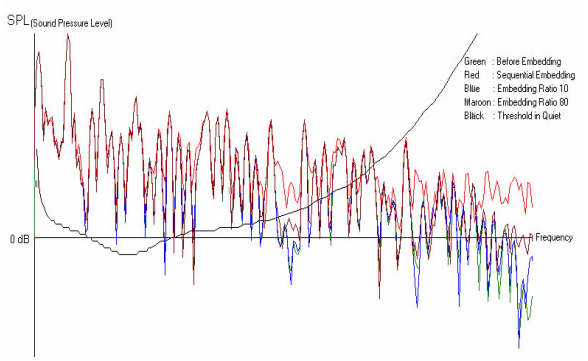
針對上述方法所潛在的幾個缺點，本計劃擬提出兩個方法使我們在藏入機密資訊時，在不影響原始聲音品質的前提下能兼顧到高容量、高安全性的要求，同時能達到容易取出的目的。

三、結論與討論

在這個段落中，我們將介紹利用我們所發展出來的兩個演算法所做的實驗結果。圖一是我們所提出的將機密資訊藏於時間域中(Time-Domain Coding)演算法的實驗結果;圖二是另一個將機密資訊藏於頻率域中(Frequency-Domain Coding)演算法的實驗結果。在圖中，我們以不同的顏色來表示各種曲線的意義。其中，綠色及紅色分別代表機密資訊藏入聲音前、後的聲壓曲線，而黑色曲線則是代表靜音臨界值曲線。

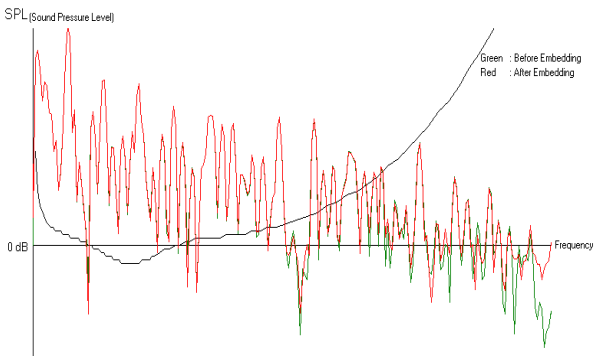


(a) 左聲道

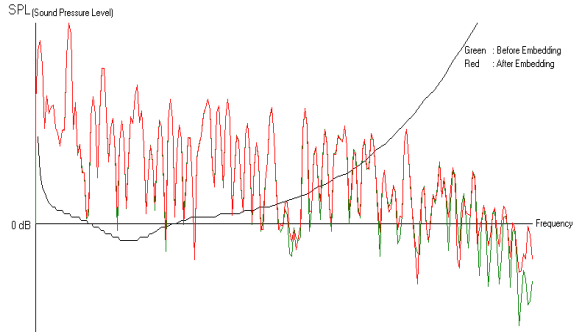


(b) 右聲道

圖一、 將機密資訊藏於時間域中(Time-Domain Coding)演算法的實驗結果



(a) 左聲道



(b) 右聲道

圖二、 將機密資訊藏於頻率域中(Frequency-Domain Coding) 演算法的實驗結果

由圖一與圖二的結果顯示，我們所提出兩個方法使我們在藏入機密資訊時，能達到在不影響原始聲音品質的前提下能兼顧到高容量、高安全性的要求。為了測試我們所提出的方法之抗壓縮容忍度，我們將藏入資訊的聲音資料轉換成壓縮格式 MP3 檔，再將資料取出檢測騎錯誤率。實驗結果如表一。

表一

	MP3 compression bit rate		
	320kbit/s	256kbit/s	128kbit/s
	Error bit rate		
Fashionable Music 1	17.736%	17.767%	19.489%
Fashionable Music 2	1.659%	1.659%	1.832%
Piano Music 1	2.154%	2.154%	2.193%
Piano Music 2	3.097%	3.097%	3.939%

四、計畫成果自評

這一個計畫於執行期間的進度與工作目標與當初所提的計畫內容大致吻合。在本計畫中，實驗結果證明了我們所提出的兩個方法的可行性。讓我們在藏入機密資訊時，在不影響原始聲音品質的前提下能兼顧到高容量、高安全性的要求，同時能達到容易取出的目的。除此之外，我們在本計畫中也建立了一套，簡單且富有彈性的全盤性整合人機介面。

五、參考文獻

[1] W. Bender, D. Gruhl, N. Morimoto, A. Lu, “Techniques for data hiding,” IBM System Journal, Vol. 35, pp. 313-336, 1996.

[2] L. Boney, A. H. Tewfik and K. N. Hamdy, “Digit Watermark for Audio Signals,” IEEE Proceedings of Multimedia, pp. 473-480, 1996.

[3] M. D. Swanson, B. Zhu, A. H. Tewfik, L. Boney, “Robust Audio Watermarking Using Perceptual Masking,” Signal Processing , pp. 337-355, 1998.

[4] A. Lu, W. Bender, D. Gruhl, “Echo Hiding,” Massachusetts Institute of Technology Media Laboratory.

[5] http://nif.www.media.mit.edu/DataHiding/index.html

[6] B. Schneier, “Applied Cryptography, Protocols, Algorithms, and Source Code in C,” pp. 436-441, 1996 by john Wiley & Sons, Inc.

[7] ISO/ICE Standard 11172-3, “Information Technology – Coding of Moving Pictures and Associated Audio for Digital Storage Media at up to about 1.5 Mbit/s – Part 3: Audio.” 1993.

[8] S. Shlien, “Guide to MPEG-1 Audio Standard,” IEEE Transaction On Broadcasting, Vol. 40, No. 4, pp. 206-218, December, 1994.

[9] D. Pan, Motorola, “A Tutorial on MPEG/Audio Compression,” IEEE Multimedia, pp. 60-74, 1995.

[10] P. Noll, “MPEG Digital Audio Coding,” IEEE Signal Processing Magazine, pp. 59-81, SEPTEMBER, 1997.