國 立 交 通 大 學

電信工程學系碩士班
碩士論文

音訊展頻浮水印檢測與解碼之研究

Detection and Decoding of Audio Spread-Spectrum Watermarking

研 究 生：李維晟

指導教授：張文輝 博士

中華民國九十三年六月

音訊展頻浮水印檢測與解碼之研究

Detection and Decoding of Audio Spread-Spectrum Watermarking

研 究 生：李維晟　　**Student: Wei-cheng Lee**

指導教授：張文輝　　**Advisor: Wen-Whei Chang**

國立交通大學

電信工程學系碩士班

碩士論文

A Thesis

Submitted to Institute of Communication Engineering

College of Electrical Engineering and Computer Science

National Chiao Tung University

In Partial Fulfillment of Requirements

for the Degree of

Master of Science

in Electrical Engineering

June 2004

Hsinchu, Taiwan, Republic of China

中華民國 九十三年 六月

音訊展頻浮水印檢測與解碼之研究

學生：李維晟　　指導教授：張文輝 博士

國立交通大學電信工程學系碩士班

中文摘要

由於網際網路的廣泛應用及影音壓縮技術的躍進，使得盜版傳播的問題日益嚴重，為保障原創者之智慧財產，在多媒體檔案中隱藏認證資訊有其必要性。最佳之浮水印設計必須兼顧隱密性、強韌度及可靠度，隱密性使其不被盜版者察覺，強韌度使之能對抗惡意破壞，而可靠度能減少誤警情況的發生。我們採用離散餘弦轉換配合直序展頻技術來建構嵌入浮水印之函數，主要之關鍵在於設定一離散餘弦係數之廣義高斯機率模型，再根據最大相似度理論，設計最佳的檢測與解碼機制。除此之外，我們也探討非特定機率模型的一般情況，並推導出相關之檢測與解碼演算法。

Detection and Decoding of Audio Spread-Spectrum Watermarking

Student：Wei-Cheng Lee　Advisor：Dr. Wen-Whei Chang

Institute of Communication Engineering
National Chiao Tung University

Abstract

In this thesis, we address the problem of the performance analysis of audio watermarking systems that use a spread spectrum technique in the discrete cosine transform (DCT) domain. Two tests are involved in the ownership verification process. First, a watermark detector decides whether the audio under test contains a watermark generated with a certain key. If the audio is watermarked , then authorship by the key holder is proved and extraction of hidden message can be performed by a detector. Most current research concentrate on correlation detectors, despite evidence showing that the underlying Gaussian model assumption does not match the intrinsic natures of DCT coefficients. Recognizing this, we first investigate a statistical approach that uses the generalized Gaussian probability to characterize the DCT coefficients and then use it as a basis for the application of statistical decision theory to the design of efficient detector and decoder structures. We also generalize this approach to the possible nonexistence of a statistical description of the original audio.

誌謝

本篇論文的完成，首先要感謝指導教授張文輝老師的悉心指導與耐心啟蒙，讓我從一個對研究懵懂的新生，進而了解作研究的方法與態度，幫助我逐漸在音訊浮水印的研究領域中建立信心且獲益良多。

感謝實驗室學長若望在研究上的經驗傳承，以及學長姊亨仰、承龍、雅茹在課業上的細心解答與生活上的扶持與關照，世耀、志杰、淑羚在實驗室的朝夕相處，特別感謝玟瑜對我的支持與鼓勵。最後僅以本論文獻給始終在背後默默支持我的父母與所有關心我的人。

目錄

表目錄

圖目錄

第一章　緒論

所謂數位音訊浮水印(digital audio watermarking)，就是將一些智慧財產權的認證訊息，例如原作者、擁有者、出版處、聯絡公司地址、公司商標等，隱藏於音樂軟體產品當中。如果使用中的音樂軟體被懷疑是非法拷貝的，可以檢查其是否嵌入有隱藏的數位浮水印，再依此判斷這個音樂軟體究竟合法或非法拷貝的，以保護創作人之智慧財產。

1.1 研究動機

近幾年來網際網路的廣泛應用，配合商業化的多媒體資料壓縮技術，使得數位音樂與影像可以無失真地複製，非法拷貝和線上傳播已嚴重威脅到原創業者的生存空間。為了有效保障其智慧財產權，數位浮水印技術逐漸被應用於保護數位化的多媒體資訊[1,2,3]。目前大部分的研究都集中在影像和視訊的數位浮水印上，因為一般而言只要視覺上不要有太大的差異，嵌入浮水印的影像及視訊訊號都可以被人眼所接受。但由於人類的聽覺比視覺更加敏銳，訊號稍有失真很容易就被人耳所察覺，所以在音訊訊號上嵌入數位浮水印的技術相對就較為困難。

在音訊浮水印的處理上，嵌入的領域不外乎分為時間領域[4,5]及轉換領域[6,7,8]兩種，亦有合併此兩種領域來嵌入浮水印的技術[9,10]。至於嵌入浮水印的主要方法則有下列幾種：低位元編碼(low-bit coding)、相位編碼(phase coding)、回聲隱藏(echo data hiding)及展頻調變(spread spectrum modulation)等，近年來利用展頻調變技術將可認証用的訊息隱藏嵌入於原始影音訊號頻域的數位浮水印機制最為常見。展頻調變的原理類似展頻通訊，先將一個窄頻訊號轉換成較大的寬頻後再傳送，以期避免鄰近通道間的干擾進而提昇其通訊保密性[9,10,11,12]。因為使用資料應用延展技術相對的復原比率也相對增加，例如我們傳送一個 1，則如果我們接收到的也是一個 1，那我們可以說結果是正確的；但如果將這 1 延展 3 次變成 111，這時如果接收到的資料是 011、101、110、111，則藉由多數決(majority vote)的原理，我們還是可以得到原來正確的資料亦是 1。由於傳送訊息的每個位元被展成較長的擬亂序列，再嵌入於原始音訊當中，因此可嵌入的浮水印資料容量較受限，但展頻調變浮水印最大的優點就是具備有較佳的強韌度與保密安全性。

展頻調變中最多使用的方法就是直序展頻技術(direct sequence spread spectrum)。在嵌入浮水印的過程中，影音訊號扮演著展頻通訊中寬頻雜訊的角色，而認証用的浮水印則代表窄頻訊號，經過處理嵌入浮水印的影音

檔即可放心的傳播流通。本論文選用的加成性展頻浮水印系統，就要是採用離散餘弦域的直序展頻通訊技術，把原始音訊當成通道雜訊，並運用虛擬亂數序列調變生成一組隱藏資訊製成浮水印，再嵌入音訊中以保護其智慧財產權。當著作權的確認有爭議時，即可藉由檢測解碼隱含於音訊訊號中的浮水印來保障原創作者的正當性。

數位浮水印主要有以下幾種應用:(1)廣播監視：我們可透過在廣播內容裡隱藏浮水印的資訊，來判斷廣播電台公司是否正確地播放商品業者的廣告時間，避免真正廣告的時段低於商品業者的付費時間，造成損失；而表演者亦可經此知道是否電台公司是否有無虛報應給與報酬之使用次數費用；(2)追查非法傳播來源：我們可在浮水印中隱藏原購買者的資訊，一旦此購買者於購買商品後非法盜拷傳播，我們便可透過檢測非法傳播品所隱含之浮水印，輕易地追查出非法傳播者；(3)原創者或擁有者的證明：若原創人、原創公司或擁有者希望在其影音軟體中加入以供證明的資訊，我們亦可在浮水印中加入其想隱含之資訊，以便做為日後驗證之證據[13]。

1.2 研究方向

數位浮水印的技術主要應用於智財權的保護，如同一般的密碼系統，需要一組秘密金鑰來製成浮水印，甚至決定浮水印嵌入於音訊的位置。除

此之外，浮水印系統必須具備下列重要的特性：(1)感知透明度(Perceptual transparency)；浮水印的嵌入不能影響原有音質且不易被使用者察覺(imperceptible)，也就是說，數位浮水印隱藏於多媒體的資料中，為了保持原始的音訊資料和浮水印的隱密，從原始音訊中是無法察覺數位浮水印資料的存在；(2)強韌度(Robustness)；無論採用何種訊號處理或遭遇惡意的攻擊，浮水印皆不能遭受到破壞且還能正常取回，以確保數位浮水印的完整性，這些處理包括有類比數位間的轉換(A/D、D/A)、濾波(filtering)和壓縮(compression)等。由於音訊訊號處理的攻擊對浮水印而言是很大的傷害，也是數位浮水印必須克服的最大問題，因此浮水印必須有足夠的強韌度，方能承受音訊處理的攻擊；(3)可靠度(Reliable)；數位浮水印必須保證其隱密性(secure)，使一般人無法任意移除其資料，唯有擁有者方能有效地檢測出浮水印，解碼還原其智財權的訊息，並避免過多誤警情形(false alarm)的發生。

因此理想的浮水印系統設計應兼顧其隱密性與強韌度，前者要求嵌入的認証訊號不能被盜版者察覺其存在，而後者則強調非法的惡意攻擊不致於破壞浮水印的完整性。目前已知的相關研究集中在影像浮水印[14,15]及其檢測演算法(detection algorithm)，主要是基於頻域係數呈高斯機率分佈的假設而推導的相關式檢測器(correlation detector)[10,12]。但這不符合影音訊

號頻域係數的實際量測結果[16]，因此我們深信浮水印的檢測機制仍有許多改善的空間。相對而言，音訊浮水印技術的開發仍在起步階段[10,12,17,18]，而音訊頻域係數的機率分佈模型也未見分析整理。有鑑於此，我們將推導一種廣義的高斯(generalized Gaussian)機率函數，藉以有效地描述不同演奏內容音樂的頻域分佈變化，並建立一種能快速實現的浮水印檢測及解碼演算法。

此外，我們亦探討非特定機率模型的問題，假設待測的浮水印之機率模型未知或很難去近似時，例如非餘弦頻域係數並無適當之機率模型可近似[19]，亦即我們無特定的機率模型可應用於檢測與解碼中，此時須透過一種降維轉換運算子的充分統計特性來進行理論分析，故其可應用於非餘弦頻域中，應用範圍廣泛。由於降維轉換運算子利用一類似投影的方法大量地降低其維度，所以不論在檢測或解碼中皆可大量地降低其計算量，此為一重要之優點，除了可增進驗證時的速度外，亦使得應用於硬體實現上更具可能性。此外，非特定模型無須像特定模型須經事先分析其多項參數，所以節省了事先模型參數分析的步驟，此點亦增進了硬體實現上的可能性。綜合而言，非特定模型擁有著可省略模型分析過程、降低計算量及應用範圍更廣泛之優點。

1.3 章節概要

整篇論文分為五個章節。第一章對於數位浮水印技術作一般性的簡介，及說明本論文的研究方向。第二章描述加成性展頻浮水印的基本架構與嵌入機制。第三章討論浮水印檢測機制，透過離散餘弦轉換係數的統計分析，建構其快速實現的最佳檢測演算法。此外，也針對未知餘弦係數之機率模型時，實現其最佳的浮水印檢測機制，並顯示理論值分析與實驗數據的相關比較。第四章討論特定與非特定模型的浮水印解碼機制，利用最大相似度預估理論，推演出最佳解碼演算法則，並呈現解碼效能分析的實驗數值。最後，第五章對整篇論文做一總結，同時指出未來的研究方向。

第二章　加成性展頻浮水印

數位音訊浮水印技術主要是經由一序列的訊號處理，將智財權認證資料轉換成人耳無法察覺的浮水印，再嵌入各種音樂軟體產品當中。為了有效偵測區隔出非法拷貝，浮水印訊號若未經所有者的允許而自行去除，將嚴重破壞原始音樂訊號的品質。因此浮水印的設計，必須考慮其無法移除和修改等特質，並能抵擋住傳輸錯誤、壓縮失真、以及非法使用者的惡意攻擊。

2.1 基本架構

標準的數位浮水印系統可用圖 2.1 來表示，其中傳輸端的工作為浮水印嵌入(watermark embedding)，而接收端的工作則包括檢測(detection)及解碼(decoding)兩項任務。傳輸端的處理流程敘述如下：先將原始音訊以 L 點作音框分割，其轉換係數以向量表示成 $\mathbf{x} = [x_0, x_1, \cdots x_{L-1}]^T$。再配合秘密金鑰 K 及隱藏位元向量 $\mathbf{b} = [b_0, b_1, \cdots b_{N-1}]^T$，經嵌入函數 f 產生認証用的浮水印訊號 $\mathbf{w}$。最後將 $\mathbf{w}$ 嵌入 $\mathbf{x}$ 而製成了加印(watermarked)音訊訊號 $\mathbf{y} = \mathbf{x} + \mathbf{w}$。由於輸入端的秘密金鑰 K 只有智財權擁有者知曉，其他的人無法任意從加印訊號 $\mathbf{y}$ 中擷取隱藏訊息 $\mathbf{b}$，因此可藉以達到智財權保護的安全性。

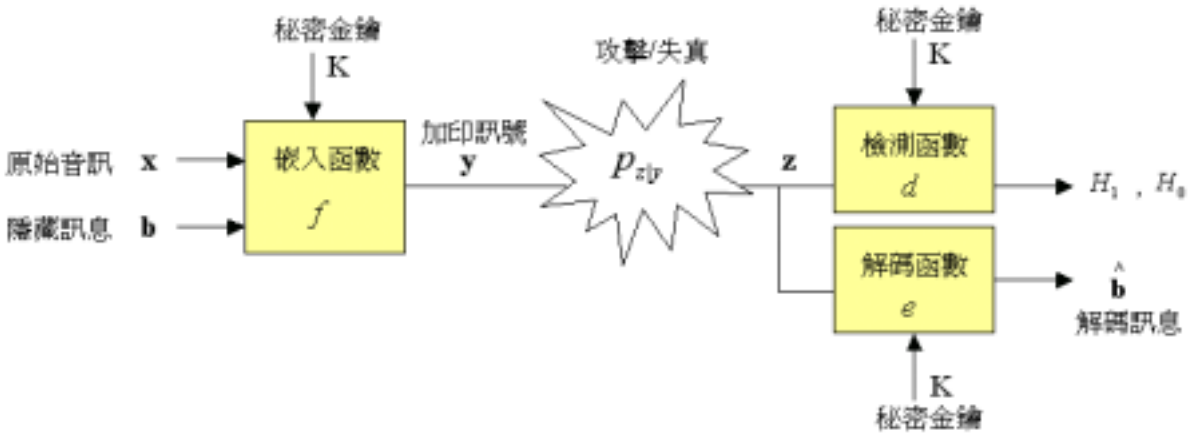


圖 2.1 數位音訊浮水印系統

加印訊號 $\mathbf{y}$ 的特色在於，不僅音樂品質近似原本的音訊 $\mathbf{x}$，更提供浮水印嵌入保護的機制，因此得以在網路上提供散播下載等服務。當著作權的歸屬有問題的時候，將透過秘密金鑰 K 及有效的認證機制解決其爭議。至於在接收端部分，觀察到的音訊 $\mathbf{z}$ 和原來的加印音訊 $\mathbf{y}$ 或許並不相同，其差異源自網路的傳播雜訊、壓縮處理失真，或遭到有心人士的惡意攻擊，我們採用條件機率函數 $p_{z/y}$ 來表示 $\mathbf{y}$ 與 $\mathbf{z}$ 之間的關係。接收端的重要工作是進行浮水印認證的處理程式，其關鍵在於引入檢測及解碼兩個函數來測試此問題。在整個研究過程中，為簡化理論分析，我們將假設無訊號失真的情況，亦即 $\mathbf{z} = \mathbf{y}$。

檢測函數 d 是用來決定訊號 $\mathbf{y}$ 是否含有一待測秘密金鑰 K 所製成的浮水印訊號，因此該檢測問題可以視為兩事件的二元假說測試，其中事件 H_1 代

表音訊$\mathbf{y}$含有金鑰K產生的浮水印，而H_0則代表音訊$\mathbf{y}$不包含金鑰K產生的浮水印，則

$$\begin{aligned} H_1 &: \mathbf{y} = \mathbf{x} + \mathbf{w} \\ H_0 &: \mathbf{y} = \mathbf{x} \end{aligned} \tag{2.1}$$

我們定義誤警機率(probability of false alarm)，$P_F \overset{\Delta}{=} P\{\ d(\mathbf{y},K) = H_1 \mid H_0\ \}$，及確認機率(probability of detection)，$P_D \overset{\Delta}{=} P\{\ d(\mathbf{y},K) = H_1 \mid H_1\ \}$，作為量測浮水印檢測效能的指標。誤警機率表示不含浮水印的音訊$\mathbf{y}$遭誤判為含有浮水印的機率，而確認機率則是能正確檢測出含有浮水印音訊的機率。假如檢測函數d偵測出音訊$\mathbf{y}$中確實含有浮水印訊號，則繼續把音訊$\mathbf{y}$及金鑰K送進浮水印的解碼函數e，進行浮水印訊號的粹取與解碼工作，以期還原出嵌入於原始音訊$\mathbf{x}$中的隱藏訊息$\hat{\mathbf{b}}$。至於評估浮水印解碼效能的指標，則定義為錯誤機率(probability of error)，$P_e \overset{\Delta}{=} P\left\{\hat{\mathbf{b}} \neq \mathbf{b}\right\}$，其值越高則代表該解碼器的功能愈差。

2.2 浮水印嵌入機制

理想的浮水印系統設計應兼顧其隱密性與強韌度，前者要求嵌入的認証訊號不能被盜版者察覺其存在，而後者則強調非法的惡意攻擊不致於破壞浮水印的完整性。本篇論文選用的加成性展頻浮水印系統，主要是仿造數位通訊系統中對抗干擾的直序展頻通訊技術，把原始音訊當成通道雜

訊，並運用虛擬亂數序列調變生成一組隱藏資訊製成浮水印，再嵌入音訊中以保護其智慧財產權。加成性展頻音訊浮水印系統如圖 2.2 所示。

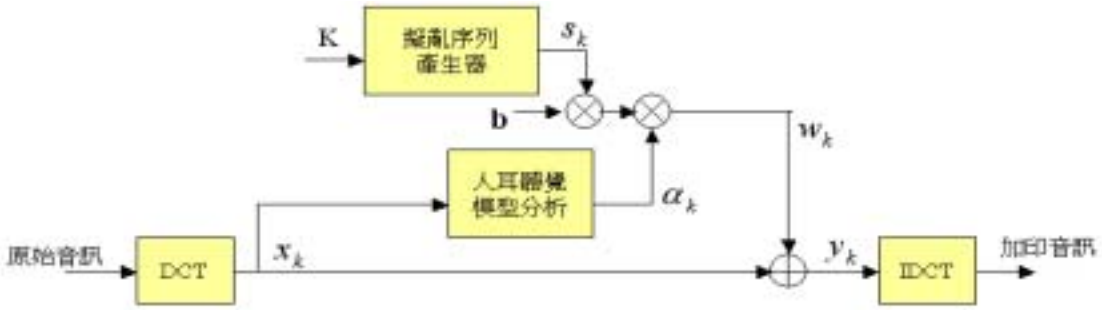


圖 2.2 加成性展頻浮水印系統

浮水印嵌入機制的處理細節如下：

(1)先對一音框的 L 個取樣點作離散餘弦轉換(Discrete Cosine Transform, DCT)，再將 L 個轉換係數所對應的索引劃分成互不相關的 N 個子集合 $\{S_j\}_{j=0}^{N-1}$，滿足 $S_j \cap S_i = \phi, \quad \forall i \neq j$，則子集合 S_j 代表著第 j 個訊息位元 b_j 可隱藏的空間。在本論文中，音框長度將固定為 $L = 256$。

(2)為了不被人耳察覺出音訊中附加的嵌入訊息，我們執行聲響心理模型分析，計算出個別 DCT 係數 x_k 所對應的加權比重值 α_k。

(3)加權比重值 α_k 與秘密金鑰 K 產生的虛擬亂數 s_k 相乘，再乘上訊息位元 b_j 製成展頻浮水印訊號 w_k。更明確地說，$\mathbf{w} = \mathbf{P}(K, \mathbf{x}) \cdot \mathbf{b}$，其元素 $w_k = b_j \cdot \alpha_k \cdot s_k, \quad \forall k \in S_j$，其中 $k \in \{0,1,\cdots,L-1\}, \quad j \in \{0,1,\cdots,N-1\}$。$S_j$ 代表第 j 個訊息位元 b_j 將嵌入的轉換係數之索引集合，而 $\mathbf{P}(K, \mathbf{x})$ 代表 $L \times N$

的矩陣，其元素 p_{kj} 滿足：

$$p_{kj} = \begin{cases} \alpha_k \cdot s_k, & if\ k \in S_j \\ 0, & otherwise \end{cases} \tag{2.2}$$

(4)嵌入浮水印後的加印音訊為 $\mathbf{y} = \mathbf{x} + \mathbf{w}$，其元素 $y_k = x_k + w_k$， $k = 0,1,\cdots,L-1$。

由此可知，隱藏訊息的 N 個位元 $\mathbf{b}$ 被展頻調變成 L 個維度的碼字 $\mathbf{w}$，進而涵蓋整段的離散餘弦域係數。由於浮水印 $\mathbf{w}$ 的製成和秘密金鑰 K 息息相關，也惟有擁有金鑰的著作原創者能把隱藏訊息 $\mathbf{b}$ 從加印音訊 $\mathbf{y}$ 中粹取出來。

2.3 人耳聽覺模型分析

如果有兩個聲音同時存在，則較高音量的聲音會使低音量的聲音聽不見，這種現象我們稱為「遮蔽效應」。遮蔽效應常常出現在日常生活當中，例如在安靜的街道中講話音量很小彼此就可聽見，若此時有一輛卡車從旁經過，若講話音量仍保持不變就聽不見對方說些什麼，也就是說講話的聲音被卡車的噪音給遮蔽了。卡車經過前跟經過後對講話者的影響都很短暫，分別稱之為前遮蔽(pre-masking)及後遮蔽(post-masking)，前遮蔽維持約 20ms 而後遮蔽維持約 200ms。

當卡車正經過時會全程影響說話者，稱之為同時遮蔽(simultaneous masking)。這是因為遮蔽效應發生在頻域上，兩個幾乎同時發生的訊號在頻率軸上很接近，因此能量比較強的訊號會使能量比較弱的訊號聽不見。為了量化地描述遮蔽效應的程度，一般均以遮蔽臨界值(masking threshold)為之。遮蔽者對被遮蔽者的影響，會存在某個臨界值，此臨界值即稱為遮蔽臨界值，此時被遮蔽者的音量必須大於此臨界值才能為人耳所聽見，反之則聽不見。有了遮蔽臨界值的資訊，我們便可設計出頻域處理之浮水印機制。

理想的浮水印設計，就是在人耳的遮蔽效應與浮水印的強韌度之間取得一個平衡。透過傳統的聲響心理學模式，我們可以計算一組傅利葉轉換頻域上的遮蔽臨界曲線，其計算流程包括有臨界頻帶濾波、等響度預處理，以及主觀響度單位轉換。該曲線就是浮水印能嵌入音訊內而不被察覺所允許的最大頻域值，而尚待解決的課題是如何將其改為在離散餘弦轉換軸上展開。我們的解決方案如下[20]：

$$\text{DFT：}\quad x_{DFT}[k]=\sqrt{\frac{1}{L}}\cdot\sum_{n=0}^{L-1}q[n]\cdot e^{-j2\pi kn/L},\ k=0,1,2,\cdots,L-1 \tag{2.3}$$

$$\text{DCT：}\quad x_{DCT}[k]=\sqrt{\frac{2}{L}}\cdot\gamma[k]\cdot\sum_{n=0}^{L-1}q[n]\cdot\cos\left(\frac{\pi\cdot k(2n+1)}{2L}\right),\ k=0,1,2,\cdots,L-1 \tag{2.4}$$

$$\gamma[k]=\begin{cases}1/\sqrt{2} & , \quad k=0\\ 1 & , \quad k=1,2,..,L-1\end{cases}$$

欲求發展兩轉換間的關係式，首先考慮一段訊號序列 $q[n],\ 0 \le n \le L-1$，將其表示為一個行向量 $\mathbf{q} = [\ q[0], q[1], \cdots, q[L-1]\ ]^T$。則離散傅利葉轉換向量 $\mathbf{x_{DFT}} = [\ x_{DFT}[0], x_{DFT}[1], \cdots, x_{DFT}[L-1]\ ]^T$ 可表示為 $\mathbf{x_{DFT}} = \mathbf{Aq}$，其中

$$\mathbf{A} = \frac{1}{\sqrt{L}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & e^{-j2\pi(1)(1)/L} & e^{-j2\pi(1)(2)/L} & \cdots & e^{-j2\pi(1)(L-1)/L} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e^{-j2\pi(L-1)(1)/L} & e^{-j2\pi(L-1)(2)/L} & \cdots & e^{-j2\pi(L-1)(L-1)/L} \end{bmatrix}$$

而餘弦轉換向量 $\mathbf{x_{DCT}} = [x_{DCT}[0],\ x_{DCT}[1], \cdots, x_{DCT}[L-1]]^T$ 亦可轉換為 $\mathbf{x_{DCT}} = \mathbf{Bq}$，其中

$$\mathbf{B} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \cdots & \frac{1}{\sqrt{2}} \\ \cos(\frac{\pi(1)(1)}{2L}) & \cos(\frac{\pi(1)(3)}{2L}) & \cdots & \cos(\frac{\pi(1)(2L-1)}{2L}) \\ \vdots & \vdots & \ddots & \vdots \\ \cos(\frac{\pi(L-1)(1)}{2L}) & \cos(\frac{\pi(L-1)(3)}{2L}) & \cdots & \cos(\frac{\pi(L-1)(L-1)}{2L}) \end{bmatrix}。$$

進一步觀察，可得其間的互轉關係為

$$\mathbf{x_{DCT}} = \mathbf{Bq} = \mathbf{BA}^{-1}\mathbf{x_{DFT}} \tag{2.5}$$

最後，我們整理計算 DCT 域的遮蔽曲線之處理細節如下：

(1) 我們先把 DFT 頻域求得之遮蔽曲線 $\mathbf{u'} = \left[u'[0], u'[1], u'[2], \cdots, u'[L-1]\right]^T$，先將其標準化：

$$\mathbf{u} = \frac{\mathbf{u'}}{\sum_{k=0}^{L-1} u'[k]} \tag{2.6}$$

(2) 再將標準化後之 $\mathbf{u}$ 透過 (2.5) 式轉換到 DCT 域，意即 $\mathbf{u}_{\mathbf{DCT}} = \mathbf{B}\mathbf{A}^{-1}\mathbf{u}$。

(3) 初步實驗證實 $\mathbf{u}_{\mathbf{DCT}}$ 之虛數部份接近 0，故取其實數部份後而得浮水印的加權比重 $\boldsymbol{\alpha}$ 為 $\boldsymbol{\alpha} = \mathrm{Re}\{\mathbf{u}_{\mathbf{DCT}}\}$。

依上述三步驟所得的 $\boldsymbol{\alpha} = \left[\alpha[0], \alpha[1], \alpha[2], \cdots, \alpha[L-1]\right]^T$ 即為容許浮水印嵌入的最大變動值。透過人耳聽覺模型的分析，計算出遮蔽臨界曲線並據以調整各轉換係數的加權比重，將有助於浮水印的透明度及強韌度間取得最佳平衡。

第三章　浮水印檢測分析

傳送端採用離散餘弦轉換配合展頻調變原理建構的浮水印嵌入機制，在接收端如要建立快速實現的浮水印檢測演算法，其關鍵在於設定一能涵蓋音訊轉換係數特性的機率模型[19]，同時依據統計預估原理設計一最佳的浮水印檢測機制，以提昇檢測器效能及其快速實現能力。目前國內外相關研究所採用的相關式檢測器，是依據高斯機率模型的假設來推導，並不足以正確反應不同演奏音樂內容的頻域係數分佈變化。有鑑於此，我們將先量測各種音樂餘弦轉換係數的統計特性，配合廣義高斯機率函數的數學推導[21]，重新規劃其快速實現的最適化浮水印檢測機制。除此之外，我們也探討在未知音樂餘弦轉換係數的統計特性的情況下，如何做最佳的浮水印檢測機制。

3.1 最佳檢測演算法

加印訊號 $\mathbf{y}$ 一旦散播出去，原創者就必須有能力自接收到的音訊 $\mathbf{y}$ 中擷取智財權的資訊，用以證明自己的合法擁有權並追蹤非法的盜版者。在浮水印認證的過程中，首要之務在檢測收到的音訊中是否含有認證用的浮水印訊號 $\mathbf{w}$，其檢測處理流程如圖 3.1 所示。

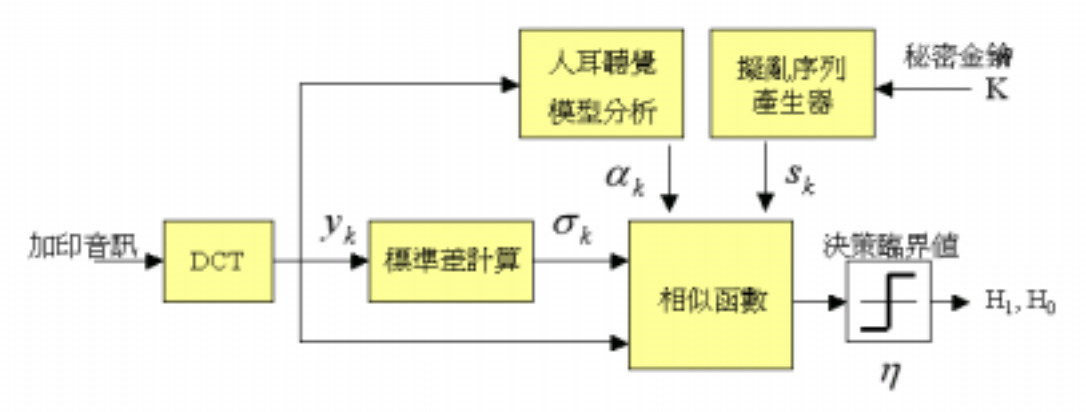


圖 3.1 浮水印檢測流程圖

浮水印檢測機制的處理細節如下：

(1)假設無法取得原始音訊 $\mathbf{x}$，對收到的音訊每 L 個取樣點作離散餘弦轉換，求得該音框的 L 個轉換係數 y_k。

(2)分析轉換係數 y_k 的統計特性，估算出標準差 σ_k，並透過聲響心理分析，計算出個別轉換係數 y_k 所對應的加權比重值 α_k。

(3)將檢測時所必要配合的轉換係數 y_k、標準差 σ_k、加權比重值 α_k、及秘密金鑰 K 產生的虛擬亂數 s_k，輸入檢測器的相似函數中，並透過決策臨界值 η 的判斷，判別該音訊是否含有浮水印。

浮水印檢測器的設計，旨在正確判別待測試的音訊檔內是否含有嵌入認証用的浮水印訊號，此檢測問題可視為兩事件的二元假說測試，其中事件 H_1 代表音訊 $\mathbf{y}$ 經過測試含有金鑰 K 產生的浮水印，H_0 則代表音訊 $\mathbf{y}$ 經過測試不包含金鑰 K 產生的浮水印。最佳化檢測器的設計旨在降低誤警機率

$P_F \overset{\Delta}{=} P\{\ d(\mathbf{y},K) = H_1 \mid H_0\}$且提高確認機率$P_D \overset{\Delta}{=} P\{\ d(\mathbf{y},K) = H_1 \mid H_1\}$。其關鍵在於透過奈曼-皮爾生法則(Neyman-Pearson test)推導出最佳的決策公式。如圖 3.2, 我們限制誤警機率$P_F = \alpha_p$不能超過其上限α_{th}，首先建構一個函數G：

$$
\begin{aligned}
G &= (1 - P_D) + \eta \cdot (P_F - \alpha) \\
&= \left(1 - \int_{Z_1} P_{y|H_1}(y \mid H_1)\, dy\right) + \eta \cdot \left(\int_{Z_1} P_{y|H_0}(y \mid H_0)\, dy - \alpha_p\right) \\
&= \int_{Z_0} P_{y|H_1}(y \mid H_1)\, dy + \eta \cdot \left(1 - \int_{Z_0} P_{y|H_0}(y \mid H_0)\, dy - \alpha_p\right) \\
&= \eta \cdot (1 - \alpha_p) + \int_{Z_0} \left[P_{y|H_1}(y \mid H_1) - \eta \cdot P_{y|H_0}(y \mid H_0)\right]\ dy
\end{aligned}
\tag{3.1}
$$

其中Z_0及Z_1分別表示事件H_0和H_1發生的區域。

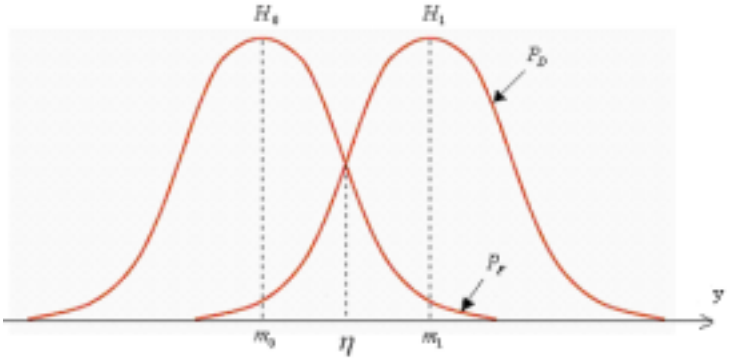


圖 3.2 二元假說下的誤警機率與確認機率分佈圖

明顯地，公式(3.1)在$P_F = \alpha_p \le \alpha_{th}$限制條件下，函數$G$的值越小，則確認機率$P_D$的值就會越大。由於積分式中指向的區域屬於$Z_0$，因此若維持積分項式的值為負數，將可有效滿足降低函數G值的條件，據此我們推導浮水印

檢測的最佳決策法則符合：

$$\Lambda(\mathbf{y}) = \ln \frac{P_{y|H_1}(\mathbf{y}\,|\,H_1)}{P_{y|H_0}(\mathbf{y}\,|\,H_0)} = \ln \frac{f_y(\mathbf{y}\,|\,H_1, K)}{f_y(\mathbf{y}\,|\,H_0)} = \ln \sum_{\mathbf{b}} \frac{p(\mathbf{b}) \cdot f_x(\mathbf{y}-\mathbf{Pb})}{f_x(\mathbf{y})} \underset{H_0}{\overset{H_1}{\gtrless}} \eta = \ln \frac{p(H_0)}{p(H_1)} \quad (3.2)$$

其中η為決策臨界值，若我們偵測音訊為未加印音訊與加印音訊的機率相同，$P(H_1) = P(H_0) = 0.5$，則此決策臨界值$\eta = 0$。

3.2 特定模型的檢測機制

若我們將音訊頻域係數假設為廣義高斯分佈機率，再代入相似函數$\Lambda(\mathbf{y})$中，應可預期推導出浮水印檢測的快速實現演算法，同時保證其整體效能會較基於係數呈高斯分佈假設而推導的相關式檢測器為佳。

3.2.1 廣義高斯機率分析

有鑒於音訊頻域機率分佈的未知性，我們將嘗試建構個別的離散餘弦轉換係數x_k之機率模型$f_x(x)$，再據以設計音訊浮水印訊號的最佳檢測演算法。初步鎖定在廣義高斯分佈函數，其定義如下：

$$f_x(x) = \frac{\beta \cdot c}{2\Gamma(1/c)} \cdot e^{-|\beta \cdot x|^c}, \quad \beta = \frac{1}{\sigma} \cdot \left[\frac{\Gamma(3/c)}{\Gamma(1/c)}\right]^{1/2} \quad (3.3)$$

其中$\Gamma(n) = \int_0^\infty v^{n-1} \cdot e^{-v}\, dv \quad , \quad n > 0$，而$\beta$值則可用標準差$\sigma$及參數$c$來表示。

選擇此機率函數有兩個理由，一則是因為只需精確估算σ及c的數值，即可有效掌握離散餘弦域係數的廣義高斯分佈特性。另一個理由是因為可藉由參數c的調整而能涵蓋不同轉換係數的機率分佈變化，例如$c=1$代表拉普拉斯(Laplace)分佈，而$c=2$代表高斯分佈，如圖 3.3。

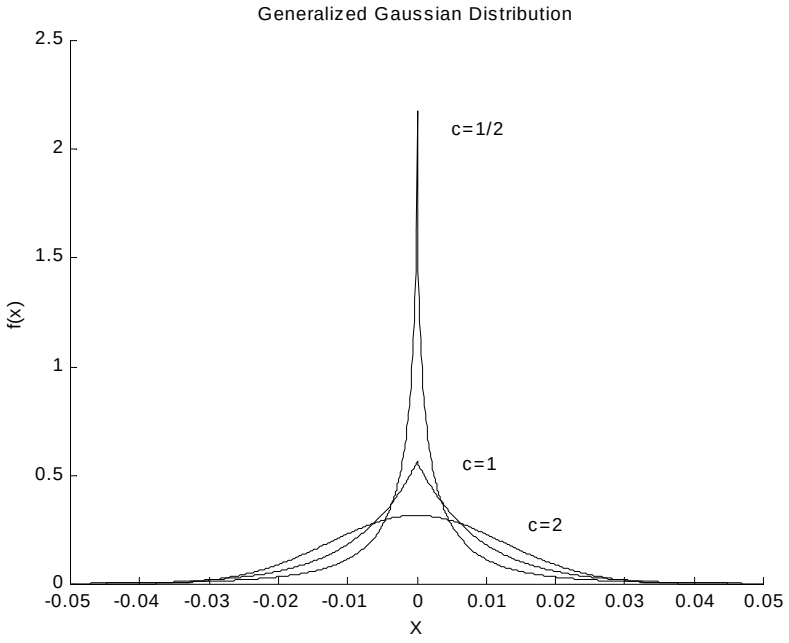


圖 3.3 廣義高斯分佈函數圖

由於廣義高斯函數的β值可用標準差σ及參數c來表示，首要任務在於正確估算出σ及c的值，即可精確建立音訊離散餘弦域係數的廣義高斯分佈函數模型。但是離散餘弦域上每個係數的分佈皆不盡然相同，據此模擬之廣義高斯分佈函數在不同係數x_k所求出之標準差σ_k及最佳c_k值，也存在著明顯的差異。透過統計分析，就是要求出每個係數所對應的最適化機率分佈函數。有了這些參數估計值，我們方能配合廣義高斯機率函數的推導，

建構一適合的浮水印檢測機制。所以在接收端拿到音訊 $\mathbf{y}$ 的第一個步驟，是分析該音訊以估算原始餘弦係數 x_k 的標準差 σ_k 及參數 c_k。有關餘弦係數 x_k 標準差 σ_k 值的推算，由於我們在接收端無法取得原始音訊 $\mathbf{x}$，所以必須從收到的音訊 $\mathbf{y}$ 上著手，第 k 個轉換係數 y_k 所對應的變異值為：

$$\sigma_y^2(k) = \frac{1}{N_b}\sum_{i=0}^{N_b-1}\left[y_k^{(i)}\right]^2 - \frac{1}{N_b^2}\left(\sum_{i=0}^{N_b-1} y_k^{(i)}\right)^2 \qquad k = 0,\cdots,L-1 \tag{3.4}$$

其中 $y_k^{(i)}$ 為第 i 個音框內的第 k 個轉換係數，N_b 表示音訊 $\mathbf{y}$ 依 L 個取樣點分割所得的音框總數。同理可推，因 b_j 及 s_k 均為 ± 1 值，$w_k = b_j \alpha_k s_k$ 的變異值為：

$$\sigma_w^2(k) = \frac{1}{N_b}\sum_{i=0}^{N_b-1}\left[\alpha_k^{(i)}\right]^2 \qquad k = 0,1,\cdots,L-1 \tag{3.5}$$

有了加印訊號 $\mathbf{y}$ 的變異值 $\sigma_y^2(k)$，並假設原始訊號 $\mathbf{x}$ 與浮水印 $\mathbf{w}$ 兩者獨立互不相關，我們利用 $y_k = x_k + w_k$ 來估算原始音訊 $\mathbf{x}$ 內第 k 個係數 x_k 的變異值，公式推導如下：

$$\begin{aligned}
\sigma_x^2(k) &= \sigma_y^2(k) + \sigma_w^2(k) - 2\cdot Cov(y_k, w_k) \\
&= \sigma_y^2(k) + \sigma_w^2(k) - 2(E[y_k \cdot w_k] - E[y_k]\cdot E[w_k]) \\
&= \sigma_y^2(k) + \sigma_w^2(k) - 2(E[(x_k + w_k)\cdot w_k]) \\
&= \sigma_y^2(k) + \sigma_w^2 - 2\cdot E[w_k^2] \\
&= \sigma_y^2(k) - \sigma_w^2(k) \qquad k = 0,\cdots,L-1
\end{aligned} \tag{3.6}$$

至於參數 c 值的估算，原則上雖應由音訊 **y** 求得，但較簡單的方法是利用原始音訊 **x** 事先作分析求得。主要是利用餘弦係數 **x** 的平均絕對值 $E[|x|]$及變異值 σ^2，其推導公式如下：

$$E[|x|]=\int_{-\infty}^{\infty}|x|\cdot f_x(x)\,dx=2\int_0^{\infty}x\cdot f_x(x)\,dx=\frac{\beta\cdot c}{\Gamma(1/c)}\int_0^{\infty}x\cdot e^{-|\beta\cdot x|^c}\,dx \tag{3.7}$$

在(3.7)式中，令 $y=(\beta\cdot x)^c\Rightarrow x=\frac{1}{\beta}\cdot y^{\frac{1}{c}}$, $dx=\frac{1}{\beta\cdot c}y^{\frac{1}{c}-1}dy$ 可得

$$E[|x|]=\frac{\beta\cdot c}{\Gamma(1/c)}\int_0^{\infty}\frac{1}{\beta}\cdot y^{\frac{1}{c}}\cdot e^{-|y|}\cdot\frac{1}{\beta\cdot c}\cdot y^{\frac{1}{c}-1}dy$$

$$=\frac{1}{\beta}\cdot\frac{1}{\Gamma(1/c)}\int_0^{\infty}y^{\frac{2}{c}-1}\cdot e^{-|y|}dy$$

$$=\frac{1}{\beta}\cdot\frac{\Gamma(2/c)}{\Gamma(1/c)} \tag{3.8}$$

同理可推 $\sigma^2=Var[x]=\int_{-\infty}^{\infty}x^2\cdot f_x(x)\cdot dx$ 則

$$\sigma^2=\frac{1}{\beta^2}\cdot\frac{1}{\Gamma(1/c)}\int_0^{\infty}y^{\frac{3}{c}-1}\cdot e^{-|y|}dy=\frac{1}{\beta^2}\cdot\frac{\Gamma(3/c)}{\Gamma(1/c)} \tag{3.9}$$

根據上述公式，第 k 個轉換係數 x_k 所對應的機率模型參數值 c_k 之計算公式為：

$$\frac{E[|x_k|]}{\sigma_k}=\frac{\Gamma(2/c_k)}{\sqrt{\Gamma(1/c_k)\cdot\Gamma(3/c_k)}}=F(c_k) \tag{3.10}$$

$$\Rightarrow\quad c_k=F^{-1}\left(\frac{E[|x_k|]}{\sigma_k}\right)\qquad k=0,1,\cdots,L-1 \tag{3.11}$$

根據公式(3.10)，$F(c)$與c的對應關係如圖 3.4 所示。舉例而言，我們選擇一鋼琴音樂作測試，利用音框長度$L=256$與公式(3.11)，求得該音訊所屬個別的餘弦轉換係數x_k所對應的理論最佳c_k值。結果發現鋼琴音樂的餘弦係數分佈，如圖 3.5 所示，在低頻處c_k值都介於 1.0~0.5 之間，而高頻處則趨近於 2。

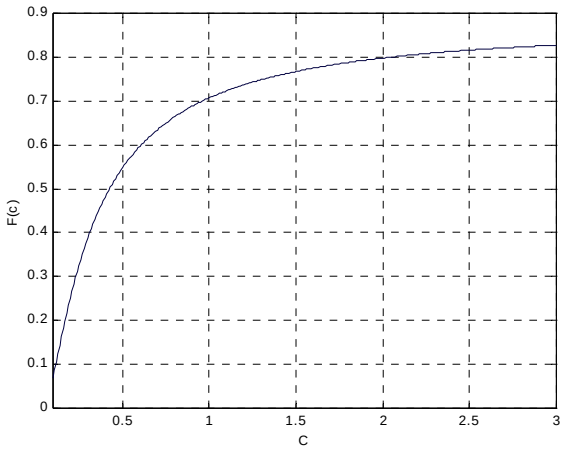


圖 3.4 $F(c)$對應c函數圖

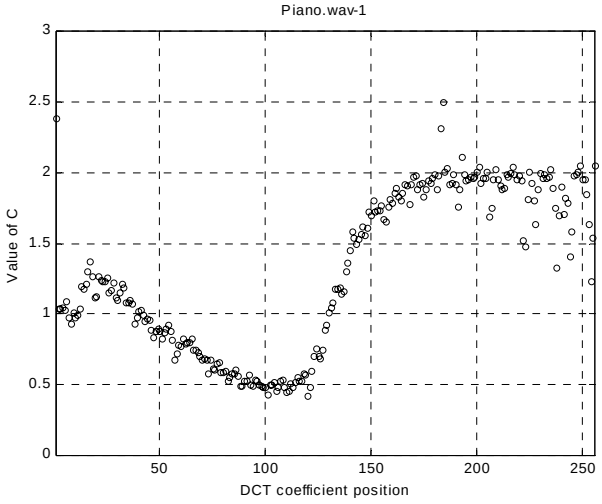


圖 3.5 鋼琴音樂轉換係數的理論c_k值圖

3.2.2 檢測效能理論分析

一旦利用音訊餘弦係數的機率分佈，推導出最佳的浮水印檢測演算法，接下來我們將透過誤警機率 P_F 及確認機率 P_D，作為浮水印檢測效能評估的指標。在實驗中假設秘密金鑰 K 的選取是隨機的，該實驗的目標就是在測試這些金鑰產生的浮水印，嵌入原始音訊 $\mathbf{x}$ 製成加印訊號 $\mathbf{y}$ 後，我們對這些加印訊號檢測的結果。

若給定一共有 $M = 2^N$ 個可隱藏的訊息集合 $\mathbf{B} \triangleq \{\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{M-1}\}$，假設每個隱藏訊息 $\mathbf{b}_l = \{b_{l,0}, b_{l,1}, \cdots, b_{l,N-1}\}$ 被嵌入音訊的機率均相等為 $p(\mathbf{b}_l) = \frac{1}{M}$，且假設不同餘弦係數間互相獨立，則 $f_{\mathbf{x}}(\mathbf{x}) = \prod_{k=0}^{K_x-1} f_{x_k}(x_k)$，再將廣義高斯分佈機率函數代入(3.2)，推導結果如下：

$$\Lambda(\mathbf{y}) = -\ln M + \sum_{k=0}^{\boldsymbol{K}_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot |y_k|^{C_{\hat{k}}} + \ln \sum_{l=0}^{M-1} \prod_{i=0}^{N-1} \exp\left(-\sum_{k \in S_i} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot |y_k - b_{l,i} \cdot \alpha_k \cdot s_k|^{C_{\hat{k}}} \right) \quad (3.12)$$

其中定義 $\hat{k} = (k \bmod L)$，$\boldsymbol{K}_x$ 為音訊取樣點的總數目。(3.12)式中的 $\beta_{\hat{k}}$ 及 $c_{\hat{k}}$ 代表其值不受音框改變而不同，亦即 $\beta_{\hat{k}} = \beta_{(k \bmod L)}$，$c_{\hat{k}} = c_{(k \bmod L)}$，因此每一音框中相同位置上之值皆相同。反之，$\{y_k, \alpha_k\}$ 則會因音框與係數位置的不同而有差異。至於虛擬亂數 s_k，則是用同一組 256 個亂數序列在每一個音框中重覆使用。

在浮水印檢測理論分析的第一部份，我們先將實驗鎖定隱藏的訊息為單一位元($N=1$)且 $b_0=1$ ($M=1$)的特殊狀況，也就是嵌入單一位元的浮水印(pure watermark)。則此條件帶入(3.12)式中，檢測器的相似函數 $\Lambda(\mathbf{y})$ 將可簡化為：

$$\Lambda(\mathbf{y})=\sum_{k=0}^{\mathbf{K}_x-1}\beta_{\hat{k}}^{C_{\hat{k}}}\cdot\left(\left|\,y_k\,\right|^{C_{\hat{k}}}-\left|\,y_k-\alpha_k\cdot s_k\,\right|^{C_{\hat{k}}}\right) \tag{3.13}$$

首先考慮事件 H_0 為真的情況，代表測試的音訊 $\mathbf{y}$ 不包含金鑰 K 產生的浮水印，則(3.13)式可寫成：

$$\Lambda(\mathbf{y})=\sum_{k=0}^{\mathbf{K}_x-1}\beta_{\hat{k}}^{C_{\hat{k}}}\cdot\left(\left|\,x_k\,\right|^{C_{\hat{k}}}-\left|\,x_k-\alpha_k\cdot s_k\,\right|^{C_{\hat{k}}}\right) \tag{3.14}$$

公式(3.14)式中 $\Lambda(\mathbf{y})$ 為 $\mathbf{K}_x$ 個統計獨立的項次總和，所以 $\Lambda(\mathbf{y})$ 在事件 H_0 為真的情況下，其函數趨近於高斯分佈，符合圖 3.2 中當初的假設。再者 s_k 若為+1 及-1 值各佔一半的虛擬亂數，我們將可求出 $\Lambda(\mathbf{y})$ 的平均值與變異值：

$$E\left[\Lambda(\mathbf{y})\,|\,H_0\right]=\sum_{k=0}^{\mathbf{K}_x-1}\beta_{\hat{k}}^{C_{\hat{k}}}\cdot\left|x_k\right|^{C_{\hat{k}}}-\frac{1}{2}\sum_{k=0}^{\mathbf{K}_x-1}\beta_{\hat{k}}^{C_{\hat{k}}}\cdot\left(\left|x_k+\alpha_k\right|^{C_{\hat{k}}}-\left|x_k-\alpha_k\right|^{C_{\hat{k}}}\right) \tag{3.15}$$

$$Var\left(\Lambda(\mathbf{y})\,|\,H_0\right)=E\left[\left(\Lambda(\mathbf{y})-E\left[\Lambda(\mathbf{y})\,|\,H_0\right]\right)^2\right]=\frac{1}{4}\sum_{k=0}^{\mathbf{K}_x-1}\beta_{\hat{k}}^{2C_{\hat{k}}}\cdot\left(\left|x_k+\alpha_k\right|^{C_{\hat{k}}}-\left|x_k-\alpha_k\right|^{C_{\hat{k}}}\right)^2 \tag{3.16}$$

同理可推，在事件 H_1 發生的情況下 $y_k = x_k + \alpha_k \cdot s_k$ ，則(3.13)式等於：

$$\Lambda(\mathbf{y}) = \sum_{k=0}^{\boldsymbol{K}_x - 1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left(\left| x_k + \alpha_k \cdot s_k \right|^{C_{\hat{k}}} - \left| x_k \right|^{C_{\hat{k}}} \right) \tag{3.17}$$

同樣(3.17)式的 $\Lambda(\mathbf{y})$ 亦為 $\boldsymbol{K}_x$ 個統計獨立項次的總和，在事件 H_1 為真的情況下， $\Lambda(\mathbf{y})$ 的函數趨近於高斯分佈，我們並可求出 $\Lambda(\mathbf{y})$ 的平均值與變異值：

$$E\left[\Lambda(\mathbf{y}) \mid H_1\right] = \frac{1}{2} \sum_{k=0}^{\boldsymbol{K}_x - 1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left(\left| x_k + \alpha_k \right|^{C_{\hat{k}}} - \left| x_k - \alpha_k \right|^{C_{\hat{k}}} \right) - \sum_{k=0}^{\boldsymbol{K}_x - 1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left| x_k \right|^{C_{\hat{k}}} \tag{3.18}$$

$$Var\left(\Lambda(\mathbf{y}) \mid H_1\right) = \frac{1}{4} \sum_{k=0}^{\boldsymbol{K}_x - 1} \beta_{\hat{k}}^{2C_{\hat{k}}} \cdot \left(\left| x_k + \alpha_k \right|^{C_{\hat{k}}} - \left| x_k - \alpha_k \right|^{C_{\hat{k}}} \right)^2 \tag{3.19}$$

比較(3.15)、(3.16) 、(3.18) 、(3.19)式，我們發現 $\Lambda(\mathbf{y})$ 在事件 H_1 發生時的分佈函數，在理想狀況恰與事件 H_0 發生時的分佈函數依原點對稱，且皆屬於高斯分佈，因此圖 3.2 的決策臨界值將設定為 $\eta = 0$。我們定義 $m_1 \overset{\Delta}{=} E\left[\Lambda(\mathbf{y}) \mid H_1\right]$ 和 $\sigma_1^2 \overset{\Delta}{=} Var\left(\Lambda(\mathbf{y}) \mid H_1\right)$，則誤警機率 P_F 及確認機率 P_D 可分別表示成：

$$P_F = Q\left(\frac{\eta + m_1}{\sigma_1}\right) \quad , \quad P_D = Q\left(\frac{\eta - m_1}{\sigma_1}\right) \tag{3.20}$$

其中η稱為決策臨界值，也就是$\Lambda(\mathbf{y})$在兩事件下分佈曲線的實際交點，而$Q(v)=\frac{1}{\sqrt{2\pi}}\int_v^{\infty} e^{-t^2/2}dt$。假設我們限制誤警機率不能超過其上限$P_F$，對應至某一臨界值符合此條件，$v=Q^{-1}(P_F)$，也就是說$Q(v)=P_F$。接著我們定義$SNR_1 \overset{\Delta}{=} m_1^2/\sigma_1^2$，則(3.20)式將可改寫成：

$$P_D = Q\left(\frac{\eta - m_1}{\sigma_1}\right) = Q\left(\frac{\eta + m_1}{\sigma_1} - 2\frac{m_1}{\sigma_1}\right) = Q\left(Q^{-1}(P_F) - 2\sqrt{SNR_1}\right) \tag{3.21}$$

透過公式(3.21)我們可以輕易地分析檢測器效能與SNR_1的關係，在固定的誤警機率P_F條件下，SNR_1的值越大則代表確認機率P_D越高，也就是正確檢測出金鑰K產生浮水印的機率越高，代表檢測器效能越好。如圖 3.6 所示，當SNR_1大於$10dB$以上時，P_F臨界值在10^{-6}以下都能達到不錯的檢測效果。

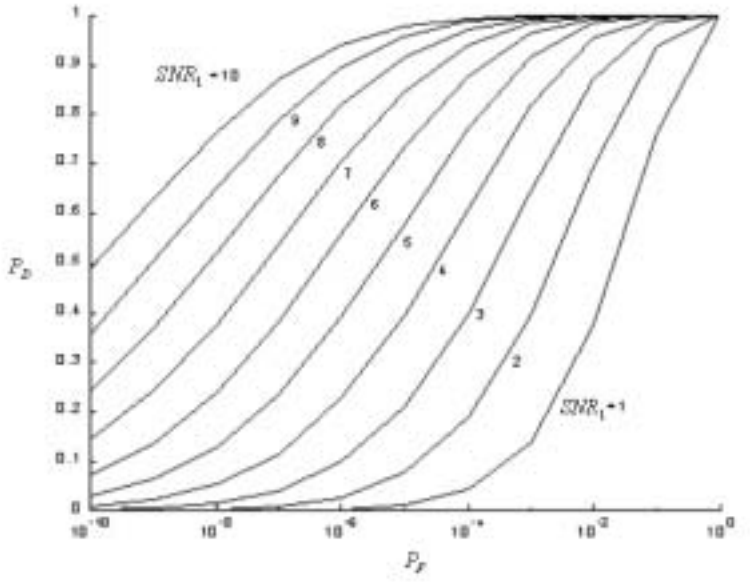


圖 3.6 檢測器效能與SNR_1的關係圖

在理論分析的第二部份，我們針對多位元(N=2)隱藏訊息的環境做進一步推導，修改其檢測演算法如下：

$$\Lambda(\mathbf{y}) = -\ln M + \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|y_k\right|^{C_{\hat{k}}} + \ln \sum_{l=0}^{M-1}\prod_{i=0}^{N-1} \exp\left(-\sum_{k\in S_i} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|y_k - b_{l,i}\cdot\alpha_k \cdot s_k\right|^{C_{\hat{k}}} \right) \underset{H_0}{\overset{H_1}{\gtrless}} 0 \quad (3.22)$$

$$\Rightarrow \Lambda'(\mathbf{y}) = \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|y_k\right|^{C_{\hat{k}}} + \ln \sum_{l=0}^{M-1}\prod_{i=0}^{N-1} \exp\left(-\sum_{k\in S_i} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|y_k - b_{l,i}\cdot\alpha_k \cdot s_k\right|^{C_{\hat{k}}} \right) \underset{H_0}{\overset{H_1}{\gtrless}} \ln M \quad (3.23)$$

因為$\Lambda'(\mathbf{y})$為K_x個統計獨立項次的總和， 由中央極限定理得知，$\Lambda'(\mathbf{y})$的函數趨近於高斯分佈，且s_k若為+1 及-1 值各佔一半的虛擬亂數，在事件H_0為真的情況下我們可求出 N=2 時$\Lambda'(\mathbf{y})$的平均值與變異值：

$$E\left[\Lambda'(\mathbf{y}) \mid H_0\right] \approx \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|x_k\right|^{C_{\hat{k}}} - \frac{1}{2}\sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left(\left|x_k+\alpha_k\right|^{C_{\hat{k}}} - \left|x_k-\alpha_k\right|^{C_{\hat{k}}} \right) \quad (3.24)$$

$$Var\left(\Lambda'(\mathbf{y}) \mid H_0\right) \approx \frac{1}{4}\sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{2C_{\hat{k}}} \cdot \left(\left|x_k+\alpha_k\right|^{C_{\hat{k}}} - \left|x_k-\alpha_k\right|^{C_{\hat{k}}} \right)^2 \quad (3.25)$$

同理，在事件H_1為真的情況，我們也可推得 N=2 時$\Lambda'(\mathbf{y})$的平均值與變異值(詳細推導過程示於附錄 A)：

$$E\left[\Lambda'(\mathbf{y}) \mid H_1\right] \approx \frac{1}{2}\sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left(\left|x_k+\alpha_k\right|^{C_{\hat{k}}} - \left|x_k-\alpha_k\right|^{C_{\hat{k}}} \right) - \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|x_k\right|^{C_{\hat{k}}} \quad (3.26)$$

$$Var\left(\Lambda'(\mathbf{y}) \mid H_1\right) \approx \frac{1}{4}\sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{2C_{\hat{k}}} \cdot \left(\left|x_k+\alpha_k\right|^{C_{\hat{k}}} - \left|x_k-\alpha_k\right|^{C_{\hat{k}}} \right)^2 \quad (3.27)$$

由(3.24)、(3.25)、(3.26)、(3.27)式，我們可發現 N=2 時$\Lambda'(\mathbf{y})$的分佈函數與第一部份(N=1 且 M=1)的$\Lambda(\mathbf{y})$的分怖情形相同，意即其皆為高斯分佈，且平均值與變異值皆相同。不同之處為 N=2 時$\Lambda'(\mathbf{y})$判斷為事件H_1或事件H_0的決策臨界值$\eta = \ln 4$，有別於第一部分的$\eta = 0$。進一步推導後，我們亦發現 N=2 情況的P_D值亦可推出如同(3.21)式之結果，只須設定式中之$\eta = \ln 4$即可。

3.3 非特定模型的檢測機制

在此探討一個更廣泛的問題，假設待測的浮水印之機率模型$f_x(\mathbf{x})$未知或很難去近似時，例如在非餘弦頻域時並無適當之機率模型可近似，在此情況下，那我們該如何進行浮水印檢測呢?在 2.2 節所描述的展頻浮水印產生過程中，N 位元的隱藏訊息 **b** 經展頻成為 L (L>>N)維度的 **w**，再產生加印訊號 **y**=**x**+**w**。若反向思考，我們也可透過一種轉換 *r*=*h(K,y)*，由原本 L 維度的待測訊號 **y** 取得 N 維度的 ***r*** 再作浮水印的檢測[19]。在實際應用上，我們可事先量測原始訊號之統計特性，如：各態歷經(ergodicity)或類各態歷經(quasi-stationarity)，利用其特性得到原始訊號 ***x*** 的一階與二階動差(first- and second-order)。在這些情況下，即使原始訊號 ***x*** 的真正分布情形未知，但至少可得知其平均值、變異值、與互變異值(cross variance)，以便能幫助我們設計效能較佳的降維轉換函數 *h(K,y)*。我們所使用的轉換如下：

$$r_i = 4 \cdot \sum_{\left\{ \begin{matrix} k:0 \le k \le K_x - 1, \\ \hat{k} \in S_i \end{matrix} \right\}} \frac{\alpha_k s_k y_k}{\sigma_{\hat{k}}^2} \quad , \quad i \in \{0, \cdots, \text{N-1}\} \tag{3.28}$$

此為一種透過計算其相關性的方法來降低其維度, 其中 $\sigma_{\hat{k}}^2$ 為第 $\hat{k}$ 個轉換係數的變異值。因為 s_k 為獨立且同型分佈(i.i.d.)隨機變數，由中央極限定理可得知， r_i 可近似為高斯分佈且假設互為獨立。在事件 H_1 為真情況下，$y_k = x_k + b_{l,i}\alpha_k s_k$,假設 x_k 與 s_k 互為獨立，可推導得 r_i 的平均與變異值分別為 $E[r_i \mid H_1] = b_{l,i} a_i$ ， $Var[r_i \mid H_1] = \sigma_{r_i}^2$ ，其中 $a_i = 4\sum_{k \in S_i} \frac{\alpha_k^2}{\sigma_{\hat{k}}^2}$ ， $\sigma_{r_i}^2 = 16\sum_{k \in S_i} \frac{\alpha_k^2 x_k^2}{\sigma_{\hat{k}}^4}$ 。其機率分布則為 $f_r(\boldsymbol{r} \mid H_1) = \frac{1}{(2\pi)^{N/2} \prod_{i=0}^{N-1} \sigma_{r_i}} \cdot \exp[-\frac{1}{2}\sum_{i=0}^{N-1} \frac{(r_i - b_{l,i} a_i)^2}{\sigma_{r_i}^2}]$ 。

而在事件 H_0 為真情況下， $y_k = x_k$,假設 x_k 與 s_k 互為獨立，可推導得 r_i 的平均與變異值分別為：$E[r_i \mid H_0] = 0$ ， $Var[r_i \mid H_0] = \sigma_{r_i}^2 = 16\sum_{k \in S_i} \frac{\alpha_k^2 x_k^2}{\sigma_{\hat{k}}^4}$ 。其機率分布則為 $f_r(\boldsymbol{r} \mid H_0) = \frac{1}{(2\pi)^{N/2} \prod_{i=0}^{N-1} \sigma_{r_i}} \cdot \exp[-\frac{1}{2}\sum_{i=0}^{N-1} \frac{(r_i)^2}{\sigma_{r_i}^2}]$ 。進一步利用奈曼-皮爾生法則推導出最佳決策法則如下：

$$\Lambda(r) = \ln \frac{f_r(\boldsymbol{r} \mid H_1)}{f_r(\boldsymbol{r} \mid H_0)} = \ln \sum_{\mathbf{b}} P(\mathbf{b}) \frac{f_r(\boldsymbol{r} \mid H_1)}{f_r(\boldsymbol{r} \mid H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} \eta = \ln \frac{P(H_0)}{P(H_1)} \tag{3.29}$$

其中η為決策臨界值。假設$P(\mathbf{b}) = 1/M$且$P(H_1) = P(H_0) = 0.5$，則

$$\Lambda(r) = \ln\{\sum_{l=0}^{M-1}\frac{1}{M}\cdot\frac{\frac{1}{(2\pi)^{N/2}\prod_{i=0}^{N-1}\sigma_{r_i}}\cdot\exp[-\frac{1}{2}\sum_{i=0}^{N-1}\frac{(r_i - b_{l,i}a_i)^2}{\sigma_{r_i}^2}]}{\frac{1}{(2\pi)^{N/2}\prod_{i=0}^{N-1}\sigma_{r_i}}\cdot\exp[-\frac{1}{2}\sum_{i=0}^{N-1}\frac{(r_i)^2}{\sigma_{r_i}^2}]}\} \underset{H_0}{\overset{H_1}{\gtrless}} \eta = \ln\frac{0.5}{0.5} = 0$$

$$\Lambda(r) = -\frac{1}{2}\sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} + \sum_{i=0}^{N-1}\ln[\cosh(\frac{a_i r_i}{\sigma_{r_i}^2})] \underset{H_0}{\overset{H_1}{\gtrless}} \eta = 0 \qquad (3.30)$$

在附錄 B 中，我們進一步推出在事件H_0與H_1為真的情況下，$\Lambda(r)$期望值與變異值如下：

$$E[\Lambda(r)\,|\,H_1] \approx \frac{1}{2}\sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} - N\cdot\ln 2 \qquad (3.31)$$

$$E[\Lambda(r)\,|\,H_0] \approx -\frac{1}{2}\sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} - N\cdot\ln 2 \qquad (3.32)$$

$$Var[\Lambda(r)\,|\,H_1] = Var[\Lambda(r)\,|\,H_0] \approx \sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} \qquad (3.33)$$

由此可求出$SNR_1 \overset{\Delta}{=} \frac{E[\Lambda(r)\,|\,H_1]^2}{Var[\Lambda(r)\,|\,H_1]}$，進而利用(3.21)式計算其確認機率$P_D$。同樣地，我們可以輕易地分析檢測器效能與$SNR_1$的關係，在固定的誤警機率$P_F$條件下，$SNR_1$的值越大則代表確認機率$P_D$越高，也就是正確檢測出金鑰$K$產生浮水印的機率越高，代表檢測器效能越好。

3.4 實驗結果與分析

[實驗 3-1]

目的：針對弦樂四重奏音樂，探討在特定的廣義高斯模型中，不同位元之隱藏訊息 $\mathbf{b}$，及模型參數 c 對浮水印檢測函數 $\Lambda(\mathbf{y})$ 及其效能之影響。

步驟：我們考慮單一位元（$N=1$ 且 $M=1$）的浮水印 $\mathbf{B}=\{\mathbf{b}_0=1\}$，及兩個位元（$N=2$，$M=2^2=4$）的浮水印 $\mathbf{B}=\{\mathbf{b}_0,\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3\}$，及四個位元（$N=4$，$M=2^4=16$）的浮水印 $\mathbf{B}=\{\mathbf{b}_0,\mathbf{b}_1,\cdots,\mathbf{b}_{15}\}$。在實驗中，我們將這些隱藏訊息分別以不同的 100 組虛擬亂數製成浮水印，再嵌入於相同的弦樂四重奏音樂中，製成 100 組不同的加印音訊。並以經事先分析所得到的可調 c 值(如圖 3.7 所示)，及固定 c 值(0.5、1、2)來做比較。在此所謂的可調 c 值，是利用(3.11)式事先估算個別轉換係數的 c_k，而固定 c 值則是為了簡化分析而設定所有 c_k 值為相同。

結論：圖 3.8、圖 3.9 及圖 3.10 顯示出針對不同隱藏位元及不同秘密金鑰之檢測函數 $\Lambda(\mathbf{y})$ 值的分布情形，可發現不論固定 c 值或可調 c 值，對加印音訊及原始音訊所得到之 $\Lambda(\mathbf{y})$ 值的分布有明顯差距，可據此準確地判斷音訊是否嵌入浮水印。另外將其統計特性分別列於表 3.1、表 3.2 及表 3.3 中，比較檢測器對不同位元浮水印的檢測效能，可觀察出實

驗值與理論值具有一致性。進一步觀察，發現因為我們所加入之浮水印之長度皆相同，故在 N=1、N=2、N=4 之情況下，檢測效能亦無明顯差距。此外餘弦係數機率模型的參數 c 對檢測效能有很大之影響，在固定 c 值中以 c=0.5 之檢測效能達到最佳，可調式 c 值亦與 c=0.5 之效能相當接近。

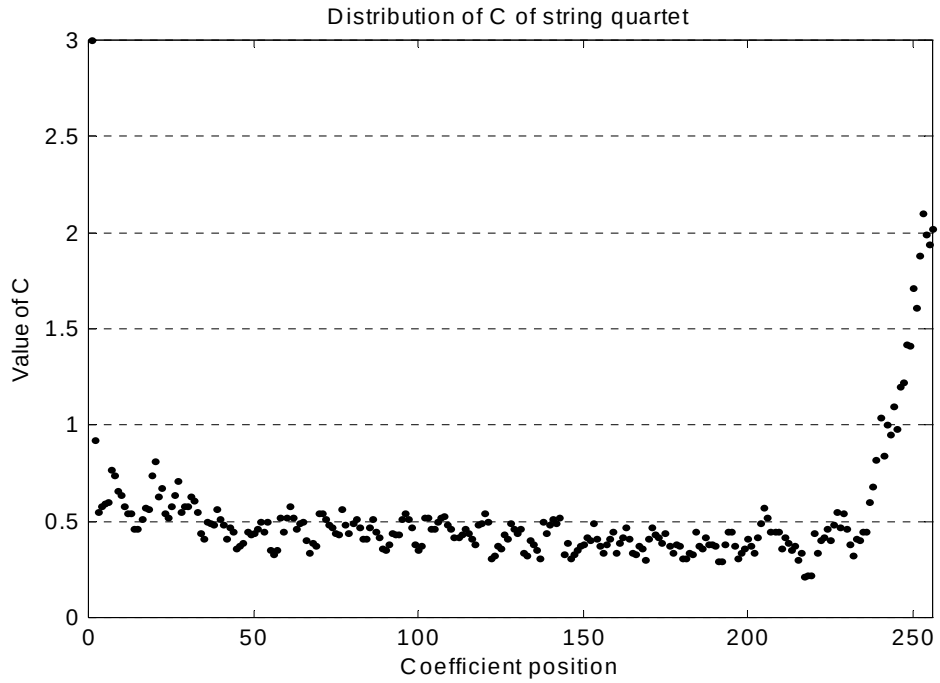


圖 3.7 弦樂四重奏音樂轉換係數之理論 c_k 值圖

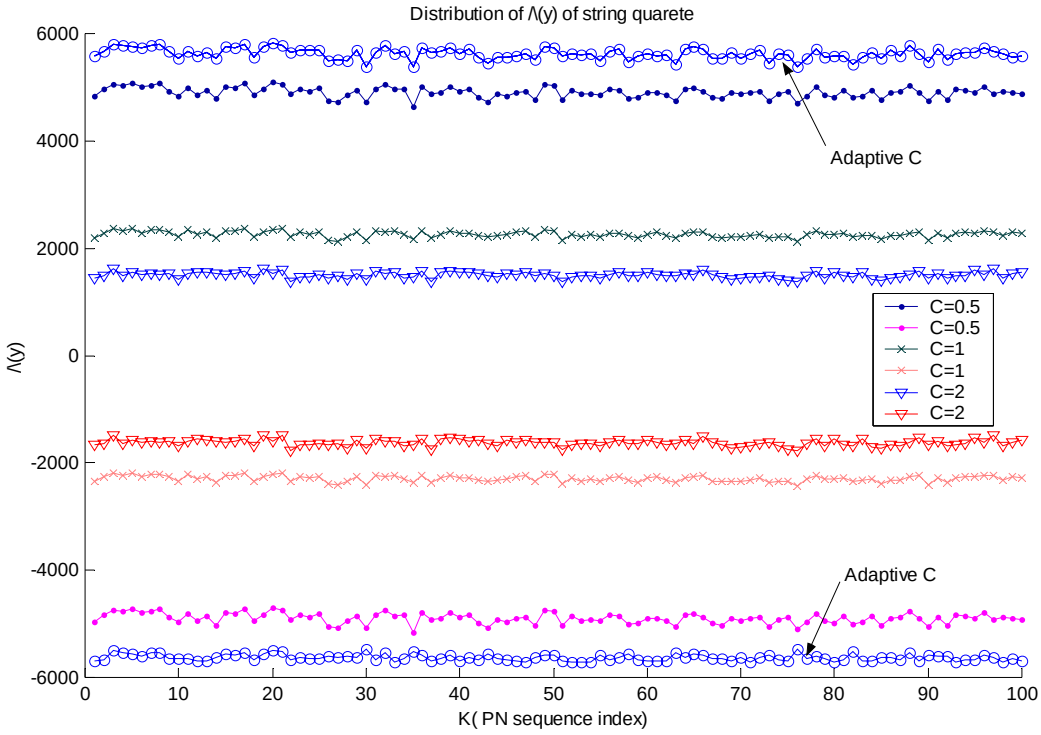


圖 3.8 弦樂四重奏單一位元特定模型中加印音訊與原始音訊的檢測值分布

	C=0.5		C=1		C=2		Adaptive C	
N=1, M=1	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR_1(dB)	34.05	33.41	32.02	32.85	28.44	27.63	34.72	33.38
$E[\Lambda(\mathbf{y})\mid H_1]$	$4.90\cdot10^3$	$4.88\cdot10^3$	$2.26\cdot10^3$	$2.25\cdot10^3$	$1.50\cdot10^3$	$1.49\cdot10^3$	$5.63\cdot10^3$	$5.56\cdot10^3$
$Var[\Lambda(\mathbf{y})\mid H_1]$	$9.46\cdot10^3$	$1.08\cdot10^4$	$3.21\cdot10^3$	$2.62\cdot10^3$	$3.21\cdot10^3$	$3.84\cdot10^3$	$1.07\cdot10^4$	$1.42\cdot10^4$
$E[\Lambda(\mathbf{y})\mid H_0]$	$-4.90\cdot10^3$	$-4.88\cdot10^3$	$-2.29\cdot10^3$	$-2.25\cdot10^3$	$-1.63\cdot10^3$	$-1.49\cdot10^3$	$-5.63\cdot10^3$	$-5.56\cdot10^3$
$Var[\Lambda(\mathbf{y})\mid H_0]$	$9.46\cdot10^3$	$1.08\cdot10^4$	$3.21\cdot10^3$	$2.62\cdot10^3$	$3.21\cdot10^3$	$3.84\cdot10^3$	$1.07\cdot10^4$	$1.42\cdot10^4$

表 3.1 弦樂四重奏單一位元特定模型檢測值的統計特性

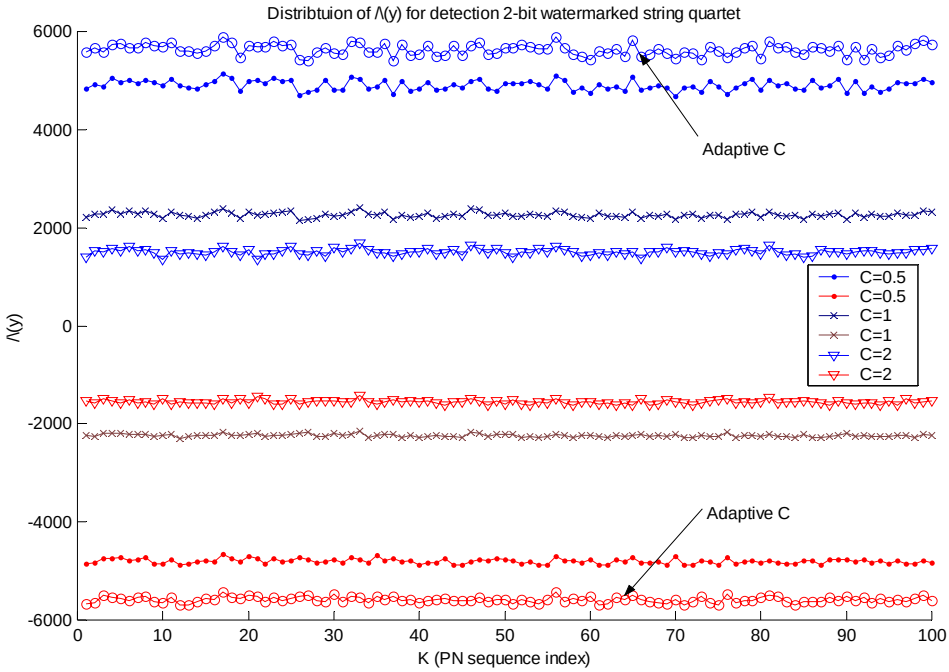


圖 3.9 弦樂四重奏兩位元特定模型中加印音訊與原始音訊的檢測值分布

	C=0.5		C=1		C=2		Adaptive C	
N=2, M=4	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR_1 (dB)	33.91	33.41	32.40	32.85	27.58	27.63	33.82	33.38
$E[\Lambda(\mathbf{y})\mid H_1]$	$4.91\cdot10^3$	$4.88\cdot10^3$	$2.26\cdot10^3$	$2.25\cdot10^3$	$1.50\cdot10^3$	$1.49\cdot10^3$	$5.63\cdot10^3$	$5.56\cdot10^3$
$Var[\Lambda(\mathbf{y})\mid H_1]$	$9.79\cdot10^3$	$1.08\cdot10^4$	$2.95\cdot10^3$	$2.62\cdot10^3$	$3.96\cdot10^3$	$3.84\cdot10^3$	$1.32\cdot10^4$	$1.42\cdot10^4$
$E[\Lambda(\mathbf{y})\mid H_0]$	$-4.80\cdot10^3$	$-4.88\cdot10^3$	$-2.24\cdot10^3$	$-2.25\cdot10^3$	$-1.55\cdot10^3$	$-1.49\cdot10^3$	$-5.58\cdot10^3$	$-5.56\cdot10^3$
$Var[\Lambda(\mathbf{y})\mid H_0]$	$9.79\cdot10^3$	$1.08\cdot10^4$	$2.95\cdot10^3$	$2.62\cdot10^3$	$3.96\cdot10^3$	$3.84\cdot10^3$	$1.32\cdot10^4$	$1.42\cdot10^4$

表 3.2 弦樂四重奏兩位元特定模型檢測值的統計特性

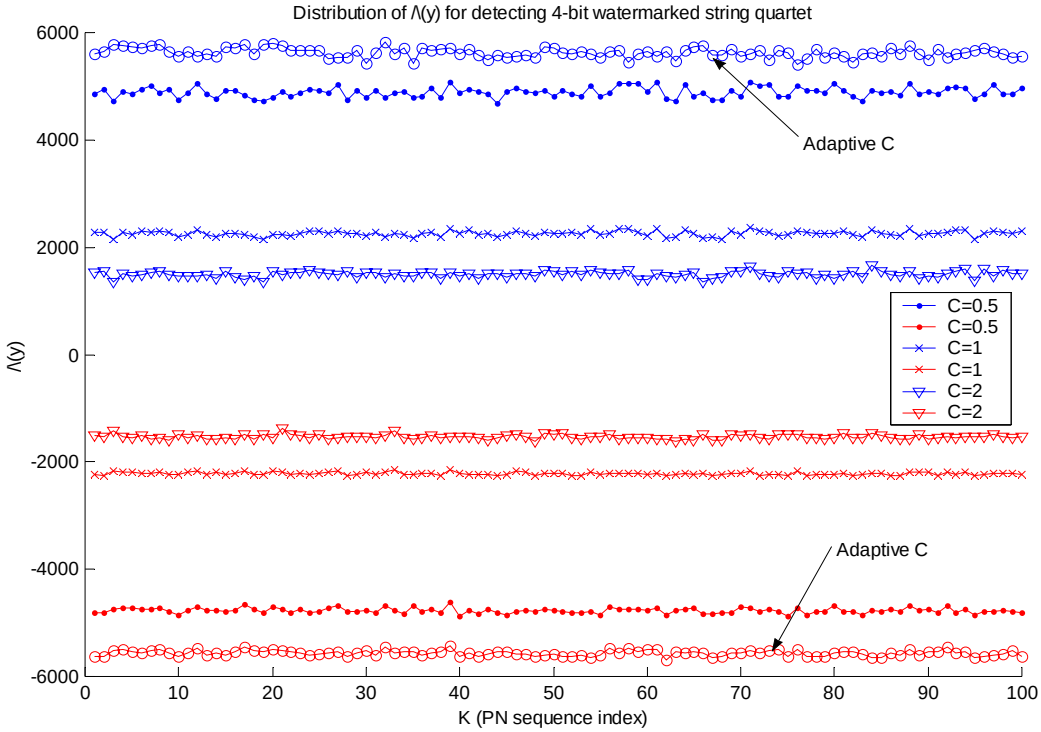


圖 3.10 弦樂四重奏四位元特定模型加印音訊與原始音訊的檢測值分布

	C=0.5	C=1	C=2	Adaptive C
N=4, M=16	實驗值	實驗值	實驗值	實驗值
SNR_1(dB)	34.14	33.02	28.24	35.82
$E[\Lambda(\mathbf{y})\mid H_1]$	$4.89\cdot10^3$	$2.26\cdot10^3$	$1.50\cdot10^3$	$5.63\cdot10^3$
$Var[\Lambda(\mathbf{y})\mid H_1]$	$9.22\cdot10^3$	$2.54\cdot10^3$	$3.36\cdot10^3$	$8.29\cdot10^3$
$E[\Lambda(\mathbf{y})\mid H_0]$	$-4.77\cdot10^3$	$-2.22\cdot10^3$	$-1.53\cdot10^3$	$-5.51\cdot10^3$
$Var[\Lambda(\mathbf{y})\mid H_0]$	$9.22\cdot10^3$	$2.54\cdot10^3$	$3.36\cdot10^3$	$8.29\cdot10^3$

表 3.3 弦樂四重奏四位元特定模型檢測值的統計特性

[實驗 3-2]

目的：針對弦樂四重奏音樂，探討在非特定之轉換係數機率模型中，不同位元之隱藏訊息 b 對浮水印檢測函數 $\Lambda(\mathbf{y})$ 及其效能之影響。

步驟：我們考慮單一位元($N=1$ 且 $M=1$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0=1\}$，及兩個位元($N=2$， $M=2^2=4$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0,\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3\}$，及四個位元($N=4$ ， $M=2^4=16$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0,\mathbf{b}_1,\cdots,\mathbf{b}_{15}\}$。實驗中我們將這些隱藏訊息分別以不同的 100 組虛擬亂數製成浮水印，再嵌入於相同的弦樂四重奏音樂中，製成 100 組不同的加印音訊，再對其做偵測。

結論:表 3.4 列出不同隱藏位元的檢測值統計特性，其中亦可發現理論值與實驗值具有一致性，且針對加印音訊與非加印音訊所得之檢測值 $\Lambda(\mathbf{y})$ 具有相當差距，故亦可正確偵測出音訊是否嵌入浮水印。特別強調的是與實驗 3-1 作比較，我們可發現特定模型確實比非特定模型得到較佳的檢測效能。

	N=1		N=2		N=4	
	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR_1(dB)	28.02	27.63	26.99	28.44	30.17	28.84
$E[\Lambda(\mathbf{r})\|H_1]$	$1.16\cdot10^3$	$1.16\cdot10^3$	$1.40\cdot10^3$	$1.40\cdot10^3$	$1.54\cdot10^3$	$1.53\cdot10^3$
$Var[\Lambda(\mathbf{r})\|H_1]$	$2.12\cdot10^3$	$2.32\cdot10^3$	$3.94\cdot10^3$	$2.80\cdot10^3$	$2.27\cdot10^3$	$3.07\cdot10^3$
$E[\Lambda(\mathbf{r})\|H_0]$	$-1.12\cdot10^3$	$-1.16\cdot10^3$	$-1.34\cdot10^3$	$-1.40\cdot10^3$	$-1.45\cdot10^3$	$-1.53\cdot10^3$
$Var[\Lambda(\mathbf{r})\|H_0]$	$2.12\cdot10^3$	$2.32\cdot10^3$	$3.94\cdot10^3$	$2.80\cdot10^3$	$2.27\cdot10^3$	$3.07\cdot10^3$

表 3.4 弦樂四重奏在非特定模型中檢測值的統計特性

[實驗 3-3]

目的：針對鋼琴音樂，探討在特定模型與非特定模型中，單一隱藏位元浮水印檢測效能，並與弦樂四重奏音樂的實驗結果作比較。

步驟：我們考慮單一位元(M=1, N=1)的浮水印。實驗中我們將這些隱藏訊息分別以不同的 100 組虛擬亂數製成浮水印，再嵌入於鋼琴音樂中，製成 100 組不同的加印音訊，再對其做偵測。

結論: 比較表 3.5 與表 3.1，表 3.4 與表 3.6，我們可發現鋼琴音樂之檢測效能較差，這是因為鋼琴音樂之理論 c_k 值(示於圖 3.5)分布較亂，不若弦樂四重奏音樂般集中。此外，亦可發現鋼琴音樂在固定 c 值之檢測效能以 c=1 時達到最佳。至於其它統計特性，則可得到與弦樂四重奏音樂類似的結果，舉例而言，不論固定 c 值或可調 c 值，對加

印音訊及原始音訊所得到之 $\Lambda(\mathbf{y})$ 值的分布有明顯差距，可據此準確地判斷音訊是否嵌入浮水印；亦可觀察出實驗值與理論值具有一致性。

Piano	C=0.5		C=1		C=2		Adaptive C	
N=1, M=1	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR_1(dB)	19.45	21.08	20.35	22.51	19.65	20.10	20.45	21.73
$E[\Lambda(\mathbf{y})\|H_1]$	$7.09\cdot10^2$	$7.18\cdot10^2$	$3.84\cdot10^2$	$3.89\cdot10^2$	$2.29\cdot10^2$	$2.30\cdot10^2$	$4.73\cdot10^2$	$4.77\cdot10^2$
$Var[\Lambda(\mathbf{y})\|H_1]$	$5.71\cdot10^3$	$4.02\cdot10^3$	$1.36\cdot10^3$	$8.49\cdot10^2$	$5.67\cdot10^2$	$5.18\cdot10^2$	$2.01\cdot10^3$	$1.53\cdot10^3$
$E[\Lambda(\mathbf{y})\|H_0]$	$-7.08\cdot10^2$	$-7.18\cdot10^2$	$-3.84\cdot10^2$	$-3.89\cdot10^2$	$-2.30\cdot10^2$	$-2.30\cdot10^2$	$-4.42\cdot10^2$	$-4.77\cdot10^2$
$Var[\Lambda(\mathbf{y})\|H_0]$	$5.71\cdot10^3$	$4.02\cdot10^3$	$1.36\cdot10^3$	$8.49\cdot10^2$	$5.67\cdot10^2$	$5.18\cdot10^2$	$2.01\cdot10^3$	$1.53\cdot10^3$

表 3.5 鋼琴單一位元特定模型檢測值的統計特性

Piano	N=1	
	實驗值	理論值
SNR_1(dB)	19.62	20.08
$E[\Lambda(\mathbf{r})\|H_1]$	$2.02\cdot10^2$	$2.04\cdot10^2$
$Var[\Lambda(\mathbf{r})\|H_1]$	$4.48\cdot10^2$	$4.10\cdot10^2$
$E[\Lambda(\mathbf{r})\|H_0]$	$-1.89\cdot10^2$	$-2.06\cdot10^2$
$Var[\Lambda(\mathbf{r})\|H_0]$	$4.48\cdot10^2$	$4.10\cdot10^2$

表 3.6 鋼琴單一位元非特定模型檢測值的統計特性

[實驗 3-4]

目的：針對長笛音樂，探討在特定模型與非特定模型中，單一隱藏位元浮水印檢測效能，並與弦樂四重奏、鋼琴音樂的實驗結果作比較。

步驟：我們考慮單一位元(M=1, N=1)的浮水印。實驗中我們將這些隱藏訊息分別以不同的 100 組虛擬亂數製成浮水印，再嵌入於長笛音樂中，製成 100 組不同的加印音訊，再對其做偵測。

結論: 比較表 3.7 與表 3.5、表 3.1，表 3.8 與表 3.4、表 3.6，我們可發現長笛音樂之檢測效能與弦樂四重奏相近，比鋼琴較佳，這是因為長笛音樂之理論 c_k 值(示於圖 3.11)分布較鋼琴集中，而與弦樂四重奏相近。此外，亦可發現長笛音樂在固定 c 值之檢測效能以 c=0.5 時達到最佳。至於其它統計特性，則可得到與弦樂四重奏音樂類似的結果，舉例而言，不論固定 c 值或可調 c 值，對加印音訊及原始音訊所得到之 $\Lambda(\mathbf{y})$ 值的分布有明顯差距，可據此準確地判斷音訊是否嵌入浮水印；亦可觀察出實驗值與理論值具有一致性。另一值得注意的是：長笛音樂在可調式 c 值的檢測效能達到最佳。

Flute	C=0.5		C=1		C=2		Adaptive C	
N=1, M=1	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR_1(dB)	35.16	38.00	34.62	37.83	33.50	35.42	36.13	38.84
$E[\Lambda(\mathbf{y})\|H_1]$	$1.04\cdot10^4$	$1.04\cdot10^4$	$5.49\cdot10^3$	$5.49\cdot10^3$	$6.24\cdot10^3$	$6.24\cdot10^3$	$1.07\cdot10^4$	$1.06\cdot10^4$
$Var[\Lambda(\mathbf{y})\|H_1]$	$3.30\cdot10^4$	$1.71\cdot10^4$	$1.04\cdot10^4$	$4.97\cdot10^3$	$1.74\cdot10^4$	$1.12\cdot10^4$	$2.80\cdot10^4$	$1.47\cdot10^4$
$E[\Lambda(\mathbf{y})\|H_0]$	$-1.06\cdot10^4$	$-1.04\cdot10^4$	$-6.02\cdot10^3$	$-5.49\cdot10^3$	$-6.58\cdot10^3$	$-6.24\cdot10^3$	$-1.19\cdot10^4$	$-1.06\cdot10^4$
$Var[\Lambda(\mathbf{y})\|H_0]$	$3.30\cdot10^4$	$1.71\cdot10^4$	$1.04\cdot10^4$	$4.97\cdot10^3$	$1.74\cdot10^4$	$1.12\cdot10^4$	$2.80\cdot10^4$	$1.47\cdot10^4$

表 3.7 長笛單一位元特定模型檢測值的統計特性

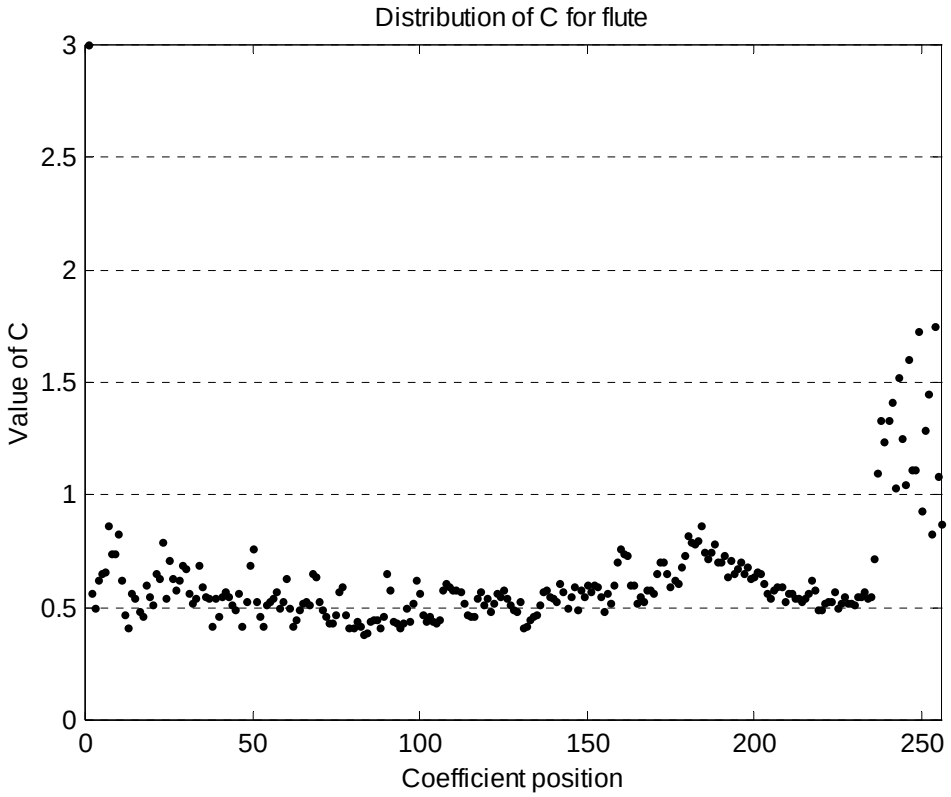


圖 3.11 長笛音樂轉換係數之理論 c_k 值

Flute	N=1	
	實驗值	理論值
SNR_1(dB)	32.75	35.42
$E[\Lambda(\mathbf{r})\mid H_1]$	$6.95\cdot10^3$	$6.96\cdot10^3$
$Var[\Lambda(\mathbf{r})\mid H_1]$	$2.57\cdot10^4$	$1.39\cdot10^4$
$E[\Lambda(\mathbf{r})\mid H_0]$	$-6.83\cdot10^3$	$-6.96\cdot10^3$
$Var[\Lambda(\mathbf{r})\mid H_0]$	$2.57\cdot10^4$	$1.39\cdot10^4$

表 3.8 長笛單一位元非特定模型檢測值的統計特性

第四章　浮水印解碼分析

接收到的音訊經過檢測確認含有金鑰 K 製成的浮水印後，接下來的工作便是要把隱藏訊息 $\mathbf{b}$ 自加印訊號 $\mathbf{y}$ 中擷取出來，還原成為提供智財權認證的重要資訊。而浮水印解碼亦可視為展頻通訊系統的解調問題，把隱藏訊息當成傳輸位元，至於原始音訊就是傳輸通道中的雜訊，利用擬亂序列的自相關特性，把隱藏位元逐一解碼回來。如同第三章的檢測機制，我們運用音訊餘弦係數的廣義高斯機率模型，配合最大相似度演算法(maximum likelihood algorithm)，來推導出快速實現的最適化浮水印解碼機制[21]；並在最後探討在未知餘弦係數模型的情況下，如何設計最佳的浮水印解碼機制。

4.1 最佳解碼演算法則

浮水印解碼器的設計旨在正確還原加印音訊 $\mathbf{y}$ 中嵌入的隱藏訊息 $\mathbf{b}$，假設我們共有 $M = 2^N$ 個可隱藏的訊息集合 $\mathbf{B} \triangleq \{\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{M-1}\}$，則此問題可視為選擇一個最大可能性的訊息作為解碼輸出結果。假設嵌入的隱藏訊息 $\mathbf{b} = \mathbf{b}_l$，　$l \in \{0,1,\cdots,M-1\}$，則產生的浮水印訊號為 $\mathbf{w}_l = \mathbf{P}(K,\mathbf{x}) \cdot \mathbf{b}_l$，且其元素可寫成 $w_{l,k} = b_{l,j} \cdot \alpha_k \cdot s_k$，　$\forall k \in S_j$，其中 $k \in \{0,1,\cdots,L-1\}$，　$j \in \{0,1,\cdots,N-1\}$。因此解碼器的輸出便是在給定金鑰 K 的情況下，搜尋所有的訊息集合 $\mathbf{B}$，最後找

到的輸出訊息 $\mathbf{b}_l$ 必須使得誤碼機率 P_e 最小。假設訊息集合中的每個訊息 $\{\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{M-1}\}$ 擁有相同的先驗機率 $P(\mathbf{b}_l) = 1/M$，則最大相似度解碼器所搜尋輸出的訊息 $\mathbf{b}_l$ 必須滿足：

$$\hat{\mathbf{b}} = \arg \max_{\{\mathbf{b}_l\}_{l=0}^{M-1}} f_y(\mathbf{y} \mid \mathbf{b}_l)$$

$$\hat{\mathbf{b}} = \mathbf{b}_l \quad if \quad \ln \frac{f_y(\mathbf{y} \mid \mathbf{b}_l)}{f_y(\mathbf{y} \mid \mathbf{b}_m)} = \ln \frac{f_x(\mathbf{y} - \mathbf{w}_l)}{f_x(\mathbf{y} - \mathbf{w}_m)} > 0, \quad \forall\, m \neq l \tag{4.1}$$

我們定義誤碼機率 $P_e \triangleq P\left\{\hat{\mathbf{b}} \neq \mathbf{b}\right\}$，作為評估浮水印解碼效能優劣的指標。誤碼機率 P_e 表示從浮水印擷取還原的訊息資料 $\hat{\mathbf{b}}$ 與嵌入的原始隱藏訊息 $\mathbf{b}$ 之間存在差異的機率，當誤碼機率過大時，還原的訊息 $\hat{\mathbf{b}}$ 則可能無法提供作為認證與辨識使用。所以我們在將隱藏訊息製成浮水印前，可適時加入錯誤修正碼(forward control code)或交插編碼(interleaving)等保護，來對抗網路傳輸的失真或惡意的攻擊。

把浮水印從加印訊號 $\mathbf{y}$ 中擷取出來，還原回隱藏訊息 $\hat{\mathbf{b}}$ 的過程，稱之為浮水印解碼。如圖 4.1 所示，解碼處理過程可視為浮水印嵌入程式的逆向操作。訊號處理細節敘述如下，首先對收到的音訊每 L 個取樣點作離散餘弦轉換，求得該音框的 L 個轉換係數 y_k，將所求得的轉換係數 y_k、標準差 σ_k、加權比重值 α_k、及秘密金鑰 K 產生的虛擬亂數 s_k 共同輸入解碼器當中，再利用解碼函數將嵌入音訊內的浮水印每個訊息位元逐一還原。

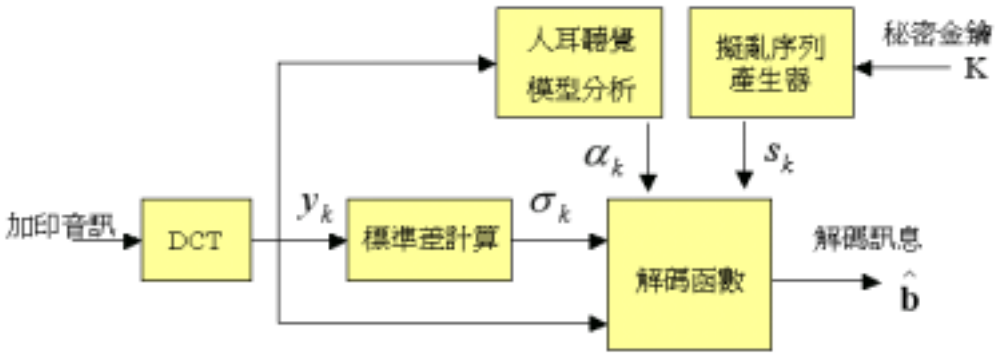


圖 4.1 浮水印解碼流程圖

4.2 特定模型的解碼機制

若我們將音訊頻域係數假設為廣義高斯分佈機率，再代入(4.1)式之解碼法則中，應可預期推導出浮水印解碼之快速實現演算法。根據廣義高斯分佈函數公式(3.3)，並假設 y 元素之間互相獨立，則

$$f_{\mathbf{y}}(\mathbf{y}\,|\,\mathbf{b}_l) = f_{\mathbf{y}}(\mathbf{y}-\mathbf{w}_l)$$

$$= \prod_{k=0}^{K_x-1}\left[\frac{\beta_{\hat{k}}\, c_{\hat{k}}}{2\Gamma(1/c_{\hat{k}})}\cdot\exp(-\beta_{\hat{k}}^{c_{\hat{k}}}\cdot\left|y_k - w_{l,k}\right|^{c_{\hat{k}}})\right]$$

$$\ln\frac{f_{\mathbf{y}}(\mathbf{y}\,|\,\mathbf{b}_l)}{f_{\mathbf{y}}(\mathbf{y}\,|\,\mathbf{b}_m)} = \sum_{k=0}^{K_x-1}\left[\left|y_k - w_{m,k}\right|^{c_{\hat{k}}} - \left|y_k - w_{l,k}\right|^{c_{\hat{k}}}\right]\cdot\beta_{\hat{k}}^{c_{\hat{k}}}$$

其中 $\beta_{\hat{k}}^{C_{\hat{k}}} = \frac{1}{\sigma_k^{C_{\hat{k}}}}\left[\frac{\Gamma(3/C_{\hat{k}})}{\Gamma(1/C_{\hat{k}})}\right]^{\frac{1}{2}}$ 而 $\left[\frac{\Gamma(3/C_{\hat{k}})}{\Gamma(1/C_{\hat{k}})}\right]^{\frac{1}{2}} > 0$。因此(4.1)式可簡化為

$$\ln\frac{f_{\mathbf{y}}(\mathbf{y}\,|\,\mathbf{b}_l)}{f_{\mathbf{y}}(\mathbf{y}\,|\,\mathbf{b}_m)} > 0 \;\equiv\; \sum_{k=0}^{K_x-1}\frac{\left|y_k - w_{m,k}\right|^{C_{\hat{k}}} - \left|y_k - w_{l,k}\right|^{C_{\hat{k}}}}{\sigma_{\hat{k}}^{C_{\hat{k}}}} > 0 \quad , \quad \forall\, m \neq l \qquad (4.2)$$

4.2.1 解碼演算的簡化

若依轉換係數索引集合S_j來分別考量，(4.2)式可改寫成：

$$\sum_{k\in S_0}[A_0]+\sum_{k\in S_1}[A_1]+\cdots+\sum_{k\in S_{N-1}}[A_{N-1}]>0\ ,\quad \forall\ m\neq l \tag{4.3}$$

其中 $A_j=\dfrac{\left|y_k-b_{m,j}\cdot\alpha_k\cdot s_k\right|^{C_{\hat{k}}}-\left|y_k-b_{l,j}\cdot\alpha_k\cdot s_k\right|^{C_{\hat{k}}}}{\sigma_{\hat{k}}^{C_{\hat{k}}}}$ ， $k\in S_j$

再進一步分析得知，當$k\in S_j$時滿足$y_k=x_k+b_{l,j}\cdot\alpha_k\cdot s_k$，而隱藏訊息位元符合$b_j=1$或$b_j=-1$，所以經由表 4.1 的歸納，我們又可將$k\in S_j$的轉換係數索引集合，分成$k\in S_j^+$及$k\in S_j^-$兩項子集合。

$b_{l,j}$	$b_{m,j}$	A_j
1	1	0
1	-1	S_j^+
-1	1	S_j^-
-1	-1	0

表 4.1 $b_{l,j}$與$b_{m,j}$關係對照表

因此公式(4.3)中的每項 A_j 皆可分成：

$$A_j = \frac{\left|y_k - b_{m,j}\cdot\alpha_k\cdot s_k\right|^{C_{\hat{k}}} - \left|y_k - b_{l,j}\cdot\alpha_k\cdot s_k\right|^{C_{\hat{k}}}}{\sigma_{\hat{k}}^{C_{\hat{k}}}} \quad , k\in S_j$$

$$= \sum_{k\in S_j^+}\frac{\left|x_k + 2\alpha_k\cdot s_k\right|^{C_{\hat{k}}} - \left|x_k\right|^{C_{\hat{k}}}}{\sigma_{\hat{k}}^{C_{\hat{k}}}} + \sum_{k\in S_j^-}\frac{\left|x_k - 2\alpha_k\cdot s_k\right|^{C_{\hat{k}}} - \left|x_k\right|^{C_{\hat{k}}}}{\sigma_{\hat{k}}^{C_{\hat{k}}}} \qquad (4.4)$$

[定理]：最大相似度解碼器的輸出訊息 $\hat{\mathbf{b}}$ 可簡化為：

$$\hat{\mathbf{b}} = \arg\max_{\mathbf{b}_l\in\mathbf{B}} \ \mathbf{b}_l^T\cdot\mathbf{r} \qquad (4.5)$$

其中 $\mathbf{r} = \{r_0, r_1, \cdots, r_{N-1}\}^T$ ， $r_j \triangleq \sum_{k\in S_j}\frac{\left|y_k + \alpha_k\cdot s_k\right|^{C_{\hat{k}}} - \left|y_k - \alpha_k\cdot s_k\right|^{C_{\hat{k}}}}{\sigma_{\hat{k}}^{C_{\hat{k}}}}$ (4.6)

[證明]：若嵌入的隱藏訊息為 $\mathbf{b} = \mathbf{b}_l$ ，則由公式(4.5)，我們解出的訊息應為 $\hat{\mathbf{b}} = \mathbf{b}_l$ ，且符合：

$$\mathbf{b}_l^T\cdot\mathbf{r} > \mathbf{b}_m^T\cdot\mathbf{r}, \ \Rightarrow \ \left(\mathbf{b}_l^T - \mathbf{b}_m^T\right)\cdot\mathbf{r} > 0, \ \forall\, m\neq l \qquad (4.7)$$

將(4.7)式依轉換係數索引集合 S_j 來個別展開：

$$\left(\mathbf{b}_l^T - \mathbf{b}_m^T\right)\cdot\mathbf{r} = \sum_{j=0}^{N-1}\left\{ \left(b_{l,j} - b_{m,j} \right)\cdot \sum_{k\in S_j} \frac{\left| y_k + \alpha_k \cdot s_k \right|^{C_{\hat{k}}} - \left| y_k - \alpha_k \cdot s_k \right|^{C_{\hat{k}}}}{\sigma_k^{C_{\hat{k}}}} \right\}$$

$$= \sum_{j=0}^{N-1}\left\{ \sum_{k\in S_j^+} \frac{2\left[\left| x_k + 2\alpha_k \cdot s_k \right|^{C_{\hat{k}}} - \left| x_k \right|^{C_{\hat{k}}} \right]}{\sigma_k^{C_{\hat{k}}}} + \sum_{k\in S_j^-} \frac{2\left[\left| x_k - 2\alpha_k \cdot s_k \right|^{C_{\hat{k}}} - \left| x_k \right|^{C_{\hat{k}}} \right]}{\sigma_k^{C_{\hat{k}}}} \right\} > 0 \quad (4.8)$$

(4.8)式的條件與(4.4)式代入(4.3)所得的結果相同，因此最大相似度解碼器的解碼函數可用(4.5)式來表示。

[定理]：最大相似度解碼器的輸出位元可簡化為

$$\hat{b}_j = sign\left(r_j\right), \quad j \in \{\, 0,1,\cdots,N-1 \,\} \qquad (4.9)$$

[證明]：因為隱藏訊息集合 $\mathbf{B}$ 的每個訊息皆為 N 位元的雙極性(binary antipodal)碼字，也就是 $b_{l,j} \in \{\, 1,-1\}$。所以在訊息集合 $\mathbf{B}$ 中的 $M = 2^N$ 個可能訊息裡，最大相似度解碼器就是要從其中挑選出一個嵌入訊息 $\hat{\mathbf{b}}$，使得 $\mathbf{b}_l^T \cdot \mathbf{r}$ 的值為最大。由於 $\mathbf{b}_l^T \cdot \mathbf{r} = b_{l,0}\cdot r_0 + b_{l,1}\cdot r_1 + \cdots + b_{l,N-1}\cdot r_{N-1}$，所以當 $b_{l,j}$ 和 r_j 的正負號相同時，就能滿足 $\mathbf{b}_l^T \cdot \mathbf{r}$ 乘積值為最大的條件。因此最大相似度隱藏訊息 $\hat{\mathbf{b}}$ 的可由每個位元的逐一解碼而得：$\hat{b}_j = sign\left(r_j\right), \quad j \in \{\, 0,1,\cdots,N-1 \,\}$

4.2.2 解碼函數的統計分析

解碼的過程是將 L 個維度的碼字 $\mathbf{w}$，還原成 N 個位元的隱藏訊息 $\mathbf{b}$，且在減少維度的過程中不遺漏任何有用的資訊，我們是採用誤碼機率 P_e 來作為浮水印解碼效能的評估。首先我們考量解碼函數中參數 r_j 的統計特性，因為 $y_k = x_k + b_j \cdot \alpha_k \cdot s_k$，當 $b_j = 1$ 時，將 $y_k = x_k + \alpha_k \cdot s_k$ 帶回公式(4.6)的 r_j 定義中可得到：

$$r_j = \sum_{k \in S_j} \frac{\left| x_k + 2\alpha_k \cdot s_k \right|^{C_{\hat{k}}} - \left| x_k \right|^{C_{\hat{k}}}}{\sigma_{\hat{k}}^{C_{\hat{k}}}} \tag{4.10}$$

假設 s_k 為+1 及-1 值各佔一半機率的虛擬亂數，則我們可計算 r_j 的平均值與變異值，推導過程如下：

$$E\left[r_j\right] = \sum_{k \in S_j} \frac{E\left[h_k\right]}{\sigma_{\hat{k}}^{C_{\hat{k}}}} \tag{4.11}$$

$$Var\left[r_j\right] = E\left[\left(r_j - E\left[r_j\right]\right)^2\right] = \sum_{k \in S_j} \frac{Var\left[h_k\right]}{\sigma_{\hat{k}}^{2C_{\hat{k}}}} \tag{4.12}$$

其中 $h_k = \left|x_k + 2\alpha_k \cdot s_k\right|^{C_{\hat{k}}} - \left|x_k\right|^{C_{\hat{k}}}$，由公式(4.10)可知

$$E\left[h_k\right] = h_k(s_k = 1) \cdot P(s_k = 1) + h_k(s_k = -1) \cdot P(s_k = -1)$$

$$E\left[h_k\right] = \frac{1}{2}\left[\left(\left| x_k + 2\alpha_k \right|\right)^{C_{\hat{k}}} + \left(\left| x_k - 2\alpha_k \right|\right)^{C_{\hat{k}}}\right] - \left|x_k\right|^{C_{\hat{k}}} \tag{4.13}$$

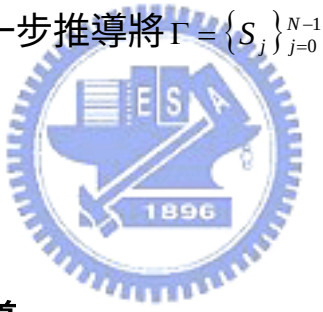
$$Var[h_k] = E\left\{[h_k - E[h_k]]^2\right\}$$

$$= \frac{1}{2}\left[\left|x_k + 2\alpha_k\right|^{C_{\hat{k}}} - \frac{1}{2}\left|x_k + 2\alpha_k\right|^{C_{\hat{k}}} - \frac{1}{2}\left|x_k - 2\alpha_k\right|^{C_{\hat{k}}}\right]^2 \qquad (when\ s_k = 1)$$

$$+ \frac{1}{2}\left[\left|x_k - 2\alpha_k\right|^{C_{\hat{k}}} - \frac{1}{2}\left|x_k + 2\alpha_k\right|^{C_{\hat{k}}} - \frac{1}{2}\left|x_k - 2\alpha_k\right|^{C_{\hat{k}}}\right]^2 \qquad (when\ s_k = -1\ )$$

$$Var[h_k] = \frac{1}{4}\left[\ \left(\ |\ x_k + 2\alpha_k|\ \right)^{C_{\hat{k}}} - \left(\ |\ x_k - 2\alpha_k|\ \right)^{C_{\hat{k}}}\right]^2 \qquad (4.14)$$

我們將(4.13)、(4.14)式帶回(4.11)、(4.12)式中，便可求得$b_j = 1$時r_j的平均與變異值，其中$j \in \{0,1,2,\cdots,N-1\}$。依此類推，我們亦可求得與$b_j = -1$時$r_j$的平均與變異值，與$b_j = 1$時的結果比較，兩者擁有相同的$Var[r_j]$，但$E[r_j]$正負號則相反。附錄C進一步推導將$\Gamma = \{S_j\}_{j=0}^{N-1}$視為一隨機變數情況下的$r_j$統計特性



4.2.3 誤碼機率的推導

應用中央極限定理(central limit theorem)，可把(4.10)式中r_j的分佈當成是高斯的向量機率函數，據此再推出其位元誤碼機率。列出r_j平均與變異值如下:

$$E[r_j] = a_j, \qquad a_j = \sum_{k \in S_j} \frac{E[h_k]}{\sigma_{\hat{k}}^{C_{\hat{k}}}}, \qquad j = 0,1,2,\cdots,N-1 \qquad (4.15)$$

其中$\begin{cases} a_j > 0, \ if\ b_j = 1 \\ a_j < 0, \ if\ b_j = -1 \end{cases}$

$$Var\left[r_j\right]=\sigma_{r_j}^2=\sum_{k\in S_j}\frac{Var\left[h_k\right]}{\sigma_{\hat{k}}^{2C_{\hat{k}}}},\quad j=0,1,2,\cdots,N-1 \tag{4.16}$$

亦即 r_j 的機率分布為 $f_r(r_j)=\frac{1}{\sqrt{2\pi}\sigma_{r_j}}\exp(\frac{-(r_j-a_j)^2}{2\sigma_{r_j}^2})$。

我們可推出第 j 個位元的誤碼機率如下:

$$\begin{aligned}P_{e,j}&=P(\hat{b}_j=-1\mid b_j=1)=P(r_j<0\mid b_j=1)\\&=\int_{-\infty}^{0}\frac{1}{\sqrt{2\pi}\sigma_{r_j}}\exp(\frac{-(r_j-a_j)^2}{2\sigma_{r_j}^2})\,dr_j \qquad (\because b_j=1\ \therefore a_j>0)\\&=Q(\frac{a_j}{\sigma_{r_j}})\quad,\quad j=0,1,2,\cdots,N-1\end{aligned}$$

同理，$P_{e,j}=P(\hat{b}_j=1\mid b_j=-1)=Q(-\frac{a_j}{\sigma_{r_j}})$ $(\because b_j=-1\ \therefore a_j<0)$。故可知第 j 個位元的誤碼機率 $P_{e,j}=Q\left(\frac{\left|a_j\right|}{\sigma_{r_j}}\right)$。定義 r_j 之訊雜比為：$SNR_j\triangleq\frac{E^2\left[r_j\right]}{Var\left[r_j\right]}=\frac{a_j^2}{\sigma_{r_j}^2}$，$j=0,1,2,\cdots,N-1$，所以 j 個位元的誤碼機率如下：

$$P_{e,j}=Q\left(\sqrt{SNR_j}\right)\quad,\quad j=0,1,2,\cdots,N-1 \tag{4.17}$$

由此可知解碼效能與 SNR_j 息息相關，亦即若 SNR_j 越大，則誤碼機率越低，反之亦然。最後我們定義 $SNR=\frac{1}{N}\sum_{j=0}^{N-1}SNR_j$，做為整體評量的指標。

4.3 非特定模型的解碼機制

如同 3.3 節所探討的，在某些情況下，待測訊號的機率模型 $f_{\mathbf{x}}(\mathbf{x})$ 未知，或很難去近似時，則無法使用上述之廣義高斯機率模型做解碼分析。我們須透過一種轉換 $r=h(K,y)$，由原本 L 維度的接收音訊 y 透過(3.28)式轉換成 N 維度的 r，再進行浮水印的解碼，其中轉換關係式為：

$$r_i = 4 \cdot \sum_{k \in S_i} \frac{\alpha_k s_k y_k}{\sigma^2_{\hat{k}}} \quad , i \in \{0,1,\cdots,N\text{-}1\} \tag{4.18}$$

如同 4.1 節所討論的，浮水印解碼器的設計旨在正確還原加印音訊 $\mathbf{y}$ 中嵌入的隱藏訊息 $\mathbf{b}$，所以此解碼器的輸出便是在給定金鑰 K 的情況下，搜尋所有的訊息集合 $\mathbf{B}$，最後找到的輸出訊息 $\mathbf{b}_l$ 必須使得誤碼機率 P_e 最小。假設訊息集合中的每個訊息 $\{\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{M-1}\}$ 擁有相同的先驗機率，則由最大相似度解碼原理，必須滿足：

$$\hat{\mathbf{b}} = \arg \max_{\{\boldsymbol{b}_l\}_{l=0}^{M-1}} f_r(r \mid \boldsymbol{b}_l) \tag{4.19}$$

$$\hat{\mathbf{b}} = \mathbf{b}_l \quad if \ \ln \frac{f_r(\boldsymbol{r} \mid \boldsymbol{b}_l)}{f_r(\boldsymbol{r} \mid \boldsymbol{b}_m)} > 0, \forall m \neq l \tag{4.20}$$

[定理]：最大相似度解碼器的輸出位元可簡化為

$$\hat{b}_i = sign(r_i), \quad i = 0,1,2,\cdots,N-1 \tag{4.21}$$

[證明]：因為 s_k 為獨立且同型分佈(i.i.d.)隨機變數，由中央極限定理可得知， r_i 可近似為高斯分佈且假設互為獨立。在事件 H_1 為真情況下，$y_k = x_k + b_{l,i}\alpha_k s_k$,假設 x_k 與 s_k 互為獨立，可推導得 r_i 的平均與變異值分別為 $E[r_i] = b_{l,i}a_i$ 且 $Var[r_i] = \sigma_{r_i}^2$ ，其中 $a_i = 4\sum_{k\in S_i}\frac{\alpha_k^2}{\sigma_{\hat{k}}^2}$ ， $\sigma_{r_i}^2 = 16\sum_{k\in S_i}\frac{\alpha_k^2 x_k^2}{\sigma_{\hat{k}}^4}$ 。故可得知 $\boldsymbol{r}$ 的機率分布如下：

$$f_r(\boldsymbol{r}\,|\,\boldsymbol{b}_l) = \frac{1}{(2\pi)^{N/2}\prod_{i=0}^{N-1}\sigma_{r_i}}\cdot\exp[-\frac{1}{2}\sum_{i=0}^{N-1}\frac{(r_i - b_{l,i}a_i)^2}{\sigma_{r_i}^2}] \qquad (4.22)$$

把(4.22)式代入(4.20)式中可得:

$$-\frac{1}{2}\sum_{i=0}^{N-1}\frac{(r_i - b_{l,i}a_i)^2}{\sigma_{r_i}^2} + \frac{1}{2}\sum_{i=0}^{N-1}\frac{(r_i - b_{m,i}a_i)^2}{\sigma_{r_i}^2} > 0, \quad \forall m \neq l$$

$$\Rightarrow \sum_{i=0}^{N-1}(b_{l,i} - b_{m,i})\cdot r_i > 0, \ \forall m \neq l$$

因要使在所有 $m \neq l$ 情況下，皆滿足(4.22)式，故須滿足：

$$\Rightarrow b_{l,i}\cdot r_i \geq b_{m,i}\cdot r_i, \quad i = 0,1,2,\cdots,N-1, \quad \forall m \neq l \qquad (4.23)$$

$\because b_{l,i} \in \{1,-1\},\ b_{m,i} \in \{1,-1\}$，唯有當所有 $b_{l,i}$ 與 r_i 正負號相同時才可滿足(4.23)式。

$$\Rightarrow b_{l,i} = sign(r_i), \quad i = 0,1,2,\cdots,N-1$$

$$\Rightarrow \hat{b}_i = sign(r_i), \quad i = 0,1,2,\cdots,N-1 \qquad (4.24)$$

因此最大可能性隱藏訊息的決定可以當成是每個位元的逐一解碼，如(4.24)式所示。

如同 4.2.2 節之理論，非特定機率模型的解碼效能計算與(4.17)式相同，意即 $SNR_i \overset{\Delta}{=} \frac{E^2[r_i]}{Var[r_i]}$， $P_{e,i} = Q\left(\sqrt{SNR_i}\right)$。亦可知解碼效能與 SNR_i 息息相關，亦即若 SNR_i 越大，則誤碼機率越低，反之亦然。同樣地，我們定義 $SNR = \frac{1}{N}\sum_{i=0}^{N-1} SNR_i$，做為整體評量之指標。

4.4 實驗結果與分析

[實驗 4-1]

目的：探討不同隱藏訊息位元 $\mathbf{b}$ 對浮水印解碼效能 SNR 的影響。

步驟：我們考慮單一位元($N=1$ 且 $M=2$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0\}$，及兩個位元($N=2$，$M=2^2=4$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0,\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3\}$，及四個位元($N=4$，$M=2^4=16$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0,\mathbf{b}_1,\cdots,\mathbf{b}_{15}\}$。在實驗中，我們將這些隱藏訊息分別以不同的 100 組虛擬亂數製成浮水印，再嵌入於相同的弦樂四重奏音樂中，製成 100 組不同的加印音訊。並以經事先分析所得到的可調 c 值(如圖 3.7 所示)，及固定 c 值(0.5、1、2)來做比較。

在此所謂的可調 c 值，是利用(3.11)式事先估算個別轉換係數的 c_k，而固定 c 值則是為了簡化分析而設定所有 c_k 值為相同。

結論：圖 4.2 與圖 4.3 顯示出單一位元($\mathbf{b}_0 \in \{1, -1\}$)、不同秘密金鑰之解碼函數 r_0 的分布情形。可發現不論固定 c 值或可調 c 值，對加印音訊嵌入訊息 $b_0 = 1$ 或 $b_0 = -1$ 所得到之 r_0 值的分布有明顯差距，可據此準確地判斷音訊嵌入之隱藏訊息為 1 或-1。另外將不同位元(N=1、2、4)解碼函數之統計特性分別列於表 4.2、表 4.3、表 4.4 及表 4.5 中，比較解碼器對不同位元浮水印的解碼效能，可觀察出實驗值與理論值具有一致性。進一步觀察，餘弦係數機率模型的參數 c 對解碼效能有很大之影響，在固定 c 值中以 c=0.5 之解碼效能達到最佳，可調式 c 值亦與 c=0.5 之效能相當接近。弦樂四重奏 N 位元特定模型解碼效能的理論值示於圖 4.4，觀察可得在位元數愈高時，可調式 c 值能得到較佳的解碼效能；而固定 c 值中以 c=0.5 之解碼效能達到最佳。特別強調的一點是，解碼效能隨著位元數的增加而遞減，因為在位元數越高時，所加入訊息的可能情形越多，造成解碼越不易。

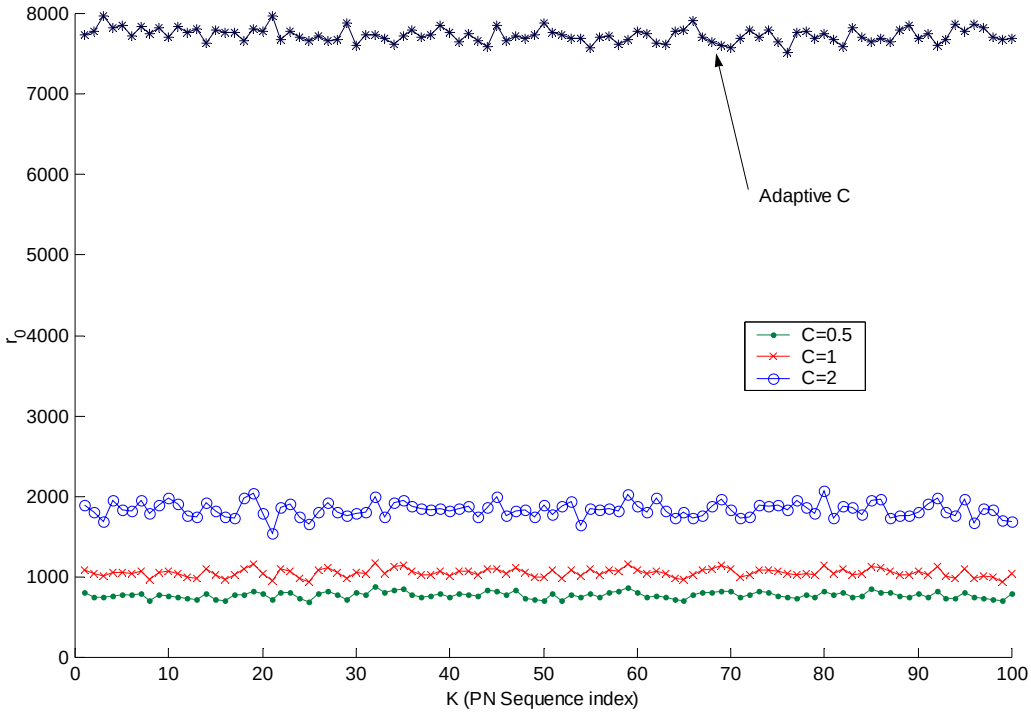


圖 4.2 弦樂四重奏在單一位元($b_0 = 1$)特定模型中的解碼值分布

	C=0.5		C=1		C=2		Adaptive C	
N=1, $b_0 = 1$	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR (dB)	38.44	39.47	36.67	38.42	34.83	33.65	39.06	37.82
$E[r_0]$	$4.61 \cdot 10^3$	$4.60 \cdot 10^3$	$5.32 \cdot 10^3$	$5.30 \cdot 10^3$	$1.20 \cdot 10^4$	$1.19 \cdot 10^4$	$7.73 \cdot 10^3$	$7.74 \cdot 10^3$
$Var[r_0]$	$3.05 \cdot 10^3$	$2.39 \cdot 10^3$	$6.08 \cdot 10^3$	$4.03 \cdot 10^3$	$4.73 \cdot 10^4$	$6.14 \cdot 10^4$	$7.43 \cdot 10^3$	$9.88 \cdot 10^3$

表 4.2 弦樂四重奏單一位元($b_0 = 1$)特定模型解碼值的統計特性

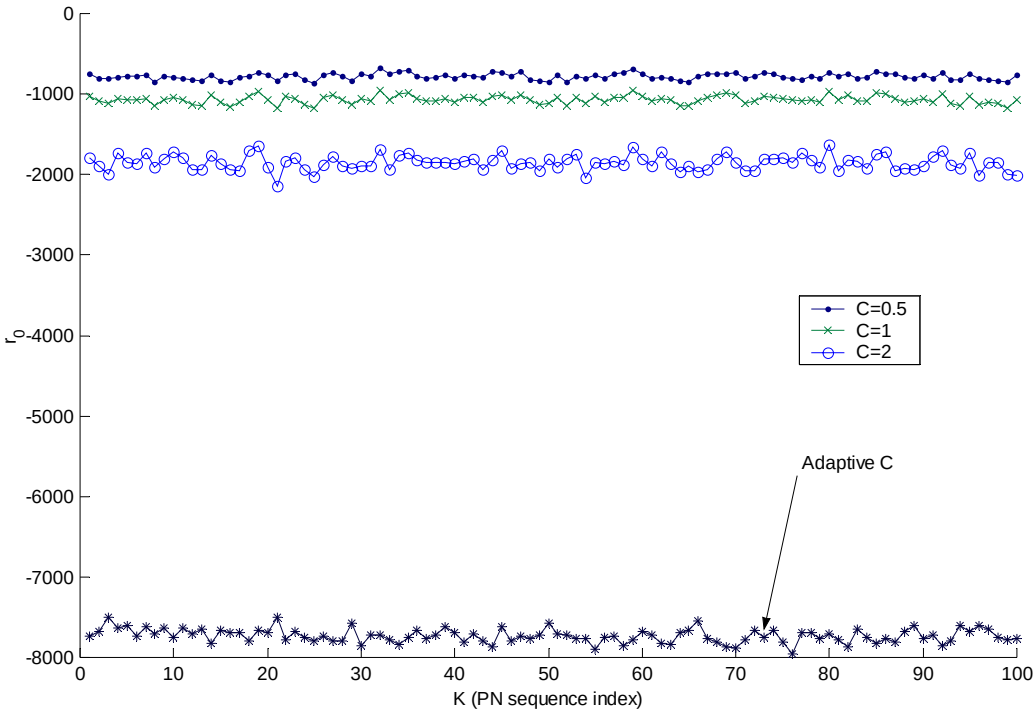


圖 4.3 弦樂四重奏在單一位元($b_0 = -1$)特定模型中的解碼值分布

	C=0.5		C=1		C=2		Adaptive C	
N=1, $b_0 = -1$	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR (dB)	38.43	39.47	36.66	38.42	34.82	33.65	39.06	37.82
$E[r_0]$	$-4.60 \cdot 10^3$	$-4.60 \cdot 10^3$	$-5.30 \cdot 10^3$	$-5.30 \cdot 10^3$	$-1.20 \cdot 10^4$	$-1.19 \cdot 10^4$	$-7.73 \cdot 10^3$	$-7.74 \cdot 10^3$
$Var[r_0]$	$3.05 \cdot 10^3$	$2.39 \cdot 10^3$	$6.08 \cdot 10^3$	$4.03 \cdot 10^3$	$4.73 \cdot 10^4$	$6.14 \cdot 10^4$	$7.43 \cdot 10^3$	$9.88 \cdot 10^3$

表 4.3 弦樂四重奏單一位元($b_0 = -1$)特定模型解碼值的統計特性

	C=0.5		C=1		C=2		Adaptive C	
N=2, $\mathbf{b}=(1,-1)$	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
Aveeage *SNR* (dB)	35.53	36.53	34.65	35.46	32.09	31.46	36.43	36.64
$E[r_0]$	$3.57\cdot10^3$	$3.56\cdot10^3$	$3.72\cdot10^3$	$3.69\cdot10^3$	$5.20\cdot10^3$	$5.13\cdot10^3$	$3.53\cdot10^3$	$3.53\cdot10^3$
$Var[r_0]$	$2.35\cdot10^3$	$1.71\cdot10^3$	$4.69\cdot10^3$	$3.00\cdot10^3$	$3.20\cdot10^4$	$3.97\cdot10^4$	$2.35\cdot10^3$	$1.77\cdot10^3$
$SNR[r_0]$(dB)	37.33	38.68	34.70	36.58	29.27	28.21	37.25	38.48
$E[r_1]$	$-1.05\cdot10^3$	$-1.05\cdot10^3$	$-1.60\cdot10^3$	$-1.60\cdot10^3$	$-6.82\cdot10^3$	$-6.81\cdot10^3$	$-4.21\cdot10^3$	$-4.21\cdot10^3$
$Var[r_1]$	$6.32\cdot10^2$	$6.83\cdot10^2$	$8.91\cdot10^2$	$1.03\cdot10^3$	$1.94\cdot10^4$	$2.17\cdot10^4$	$5.10\cdot10^3$	$8.12\cdot10^3$
$SNR[r_1]$(dB)	32.38	32.04	34.61	33.94	33.79	33.29	35.41	33.39

表 4.4 弦樂四重奏兩位元特定模型解碼值的統計特性

	C=0.5		C=1		C=2		Adaptive C	
N=4, $\mathbf{b}=(-1,1,1,-1)$	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
Aveeage *SNR* (dB)	33.15	33.57	32.60	32.55	29.18	28.86	34.10	33.80
$SNR[r_0]$(dB)	30.33	34.30	26.63	32.60	21.97	25.49	30.05	33.48
$SNR[r_1]$(dB)	37.36	36.81	36.12	34.59	28.65	26.13	37.43	36.84
$SNR[r_2]$(dB)	30.17	29.24	28.62	28.35	16.79	17.11	29.85	28.90
$SNR[r_3]$(dB)	28.42	28.80	33.00	32.58	33.76	33.54	34.45	32.44

表 4.5 弦樂四重奏四位元特定模型解碼值的統計特性

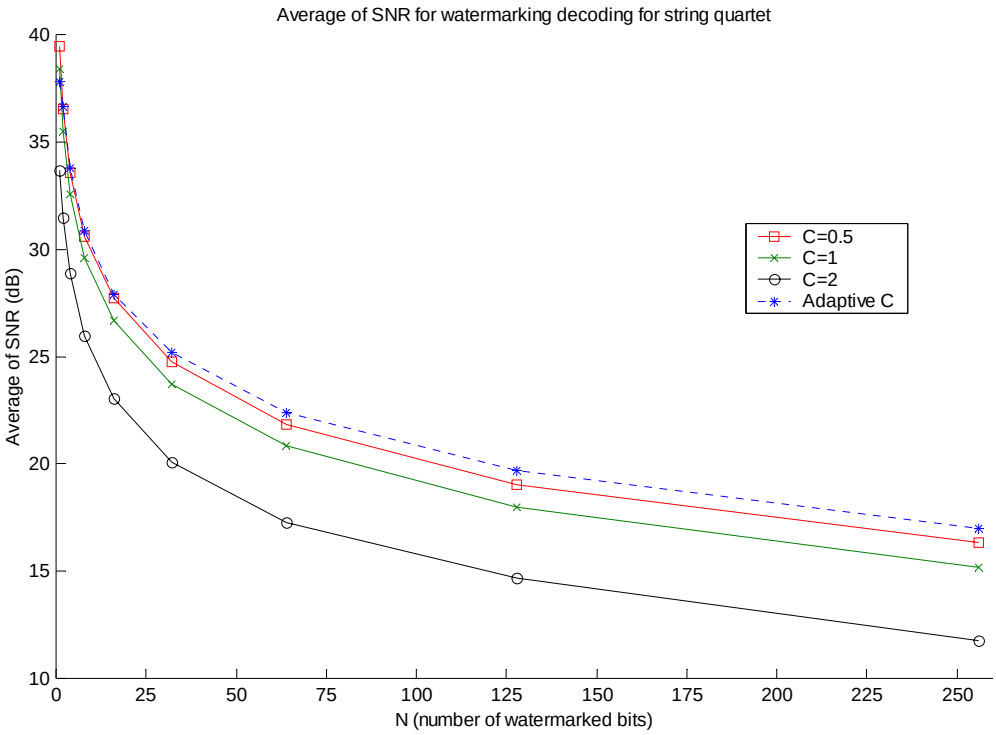


圖 4.4 弦樂四重奏 N 位元特定模型解碼效能的理論值

[實驗 4-2]

目的:針對弦樂四重奏音樂，探討在非特定之轉換係數機率模型中，不同位元之隱藏訊息 b 對浮水印解碼函數 r_i 及其效能之影響。

步驟: 我們考慮單一位元($N=1$ 且 $M=2$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0\}$，及兩個位元($N=2$ ， $M=2^2=4$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0,\mathbf{b}_1,\mathbf{b}_2,\mathbf{b}_3\}$，及四個位元 $N=4$ ($M=2^4=16$)的浮水印 $\mathbf{B}=\{\mathbf{b}_0,\mathbf{b}_1,\cdots,\mathbf{b}_{15}\}$。實驗中我們將這些隱藏訊息分別以不同的 100 組虛擬亂數製成浮水印，再嵌入於相同的弦樂四重奏音樂中，製成 100 組不同的加印音訊，再對其做解碼。

結論: 圖 4.5 顯示出在單一位元、不同秘密金鑰，非特定模型的解碼值 r_0 分布情形，可發現針對不同隱藏訊息，解碼值 r_0 的分布具有相當差距，故可正確解碼出嵌入之隱藏訊息。表 4.6 及表 4.7 列出不同隱藏位元的解碼值統計特性，其中亦可發現理論值與實驗值具有一致性，且解碼效能隨著位元數的增加而遞減。特別強調的是與實驗 4-1 作比較，我們可發現特定模型確實比非特定模型得到較佳的解碼效能，這是因為在我們所實驗的環境下，係數分布確實可用廣義高斯機率模型來近似；但非特定模型解碼器可省略模型分析過程且應用範圍更廣泛。

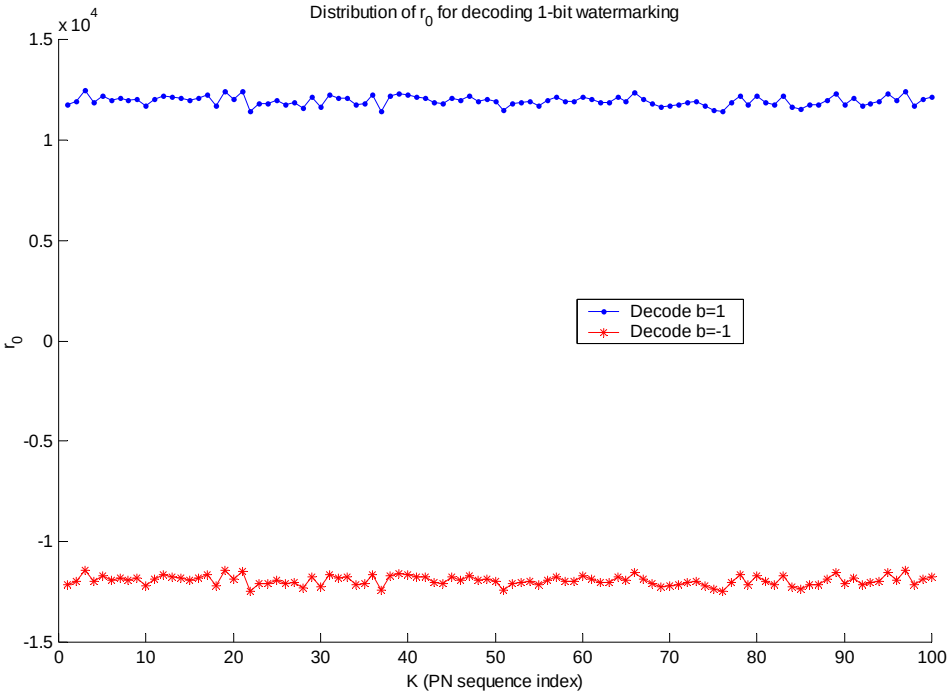


圖 4.5 弦樂四重奏單一位元在非特定模型解碼值分布

	N=1, $b_0=1$		N=1, $b_0=-1$	
	實驗值	理論值	實驗值	理論值
SNR (dB)	34.04	33.65	34.03	33.65
$E[r_0]$	$1.19\cdot10^4$	$1.19\cdot10^4$	$-1.19\cdot10^4$	$-1.19\cdot10^4$
$Var[r_0]$	$5.62\cdot10^4$	$6.14\cdot10^4$	$5.62\cdot10^4$	$6.14\cdot10^4$

表 4.6 弦樂四重奏單一位元非特定模型解碼值的統計特性

	N=2		N=4	
	實驗值	理論值	實驗值	理論值
Aveeage *SNR* (dB)	30.60	31.46	27.57	28.86
$SNR[r_0]$(dB)	29.12	28.21	21.82	25.49
$SNR[r_1]$(dB)	31.70	33.29	28.54	26.13
$SNR[r_2]$(dB)	X	X	16.79	17.11
$SNR[r_3]$(dB)	X	X	31.37	33.54

表 4.7 弦樂四重奏雙位元、四位元在非特定模型中解碼值的統計特性

[實驗 4-3]

目的：針對鋼琴音樂，探討在特定模型與非特定模型中，單一隱藏位元之浮水印解碼效能，並與弦樂四重奏音樂的實驗結果作比較。

步驟：我們考慮單一位元(M=1, M=2)的浮水印。實驗中我們將這些隱藏訊息分別以不同的 100 組虛擬亂數製成浮水印，再嵌入於鋼琴音樂中，製成 100 組不同的加印音訊，再對其做解碼。

結論：比較表 4.8 與表 4.3，表 4.9 與表 4.6，我們可發現鋼琴音樂之解碼效能較差，這是因為鋼琴音樂之理論 c_k 值(示於圖 3.5)分布較亂，不若弦樂四重奏音樂般集中。此外，亦可發現鋼琴音樂在固定 c 值之解碼效能以 c=1 時達到最佳。至於其它統計特性，則可得到與弦樂四重奏音樂類似的結果，舉例而言，不論固定 c 值或可調 c 值，對加印音訊及原始音訊所得到之 r_i 值的分布有明顯差距，可據此準確地判斷音訊嵌入之隱藏訊息；亦可觀察出實驗值與理論值具有一致性，由圖 4.6 我們亦可發現解碼效能隨著位元數的增加而遞減。

Piano	C=0.5		C=1		C=2		Adaptive C	
N=1, $b_0=-1$	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR (dB)	25.89	27.40	26.58	28.54	25.79	26.13	27.03	27.47
$E[r_0]$	$-7.83\cdot10^{2}$	$-7.79\cdot10^{2}$	$-1.07\cdot10^{3}$	$-1.06\cdot10^{3}$	$-1.85\cdot10^{3}$	$-1.84\cdot10^{3}$	$-1.31\cdot10^{3}$	$-1.29\cdot10^{3}$
$Var[r_0]$	$1.58\cdot10^{3}$	$1.10\cdot10^{3}$	$2.51\cdot10^{3}$	$1.57\cdot10^{3}$	$9.05\cdot10^{3}$	$8.29\cdot10^{3}$	$3.41\cdot10^{3}$	$2.98\cdot10^{3}$

表 4.8 鋼琴單一位元特定模型解碼值的統計特性

Piano	N=1	
N=1, $b_0=-1$	實驗值	理論值
SNR_1 (dB)	25.82	26.13
$E[r_0]$	$-1.86\cdot10^{3}$	$-1.84\cdot10^{3}$
$Var[r_0]$	$9.05\cdot10^{3}$	$8.29\cdot10^{3}$

表 4.9 鋼琴單一位元非特定模型解碼值的統計特性

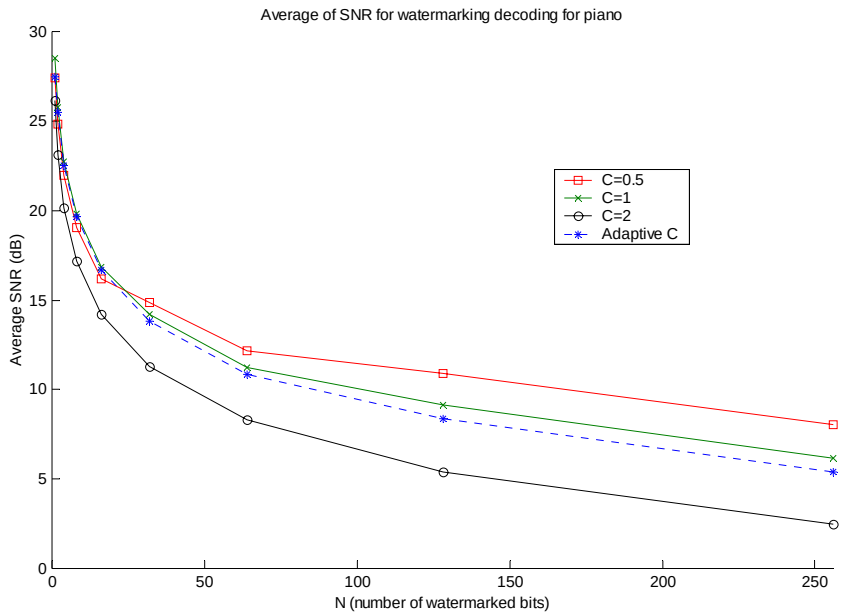


圖 4.6 鋼琴 N 位元特定模型解碼效能的理論值

[實驗 4-4]

目的：針對長笛音樂，探討在特定模型與非特定模型中，單一隱藏位元之浮水印解碼效能，並與弦樂四重奏、鋼琴音樂的實驗結果作比較。

步驟：我們考慮單一位元(M=1, M=2)的浮水印。實驗中我們將這些隱藏訊息分別以不同的 100 組虛擬亂數製成浮水印，再嵌入於長笛音樂中，製成 100 組不同的加印音訊，再對其做解碼。

結論：比較表 4.10、表 4.8 與表 4.3，表 4.11 表 4.9 與表 4.6，我們可發現長笛音樂之解碼效能與弦樂四重奏相近，比鋼琴較佳，這是因為長笛

音樂之理論 c_k 值(示於圖 3.11)分布較鋼琴集中，而與弦樂四重奏音樂相近。其統計特性則可得到與弦樂四重奏音樂類似的結果，舉例而言，不論固定 c 值或可調 c 值，對加印音訊及原始音訊所得到之 r_i 值的分布有明顯差距，可據此準確地判斷音訊嵌入之隱藏訊息；亦可觀察出實驗值與理論值具有一致性，由圖 4.7 我們亦可發現解碼效能隨著位元數的增加而遞減。另一值得注意的是:長笛音樂在可調 c 值的解碼效能達到最佳。

Flute	C=0.5		C=1		C=2		Adaptive C	
N=1, $b_0=-1$	實驗值	理論值	實驗值	理論值	實驗值	理論值	實驗值	理論值
SNR (dB)	38.64	41.83	38.21	41.89	40.05	41.44	43.64	44.48
$E[r_0]$	$-7.85\cdot10^3$	$-7.84\cdot10^3$	$-1.10\cdot10^4$	$-1.10\cdot10^4$	$-5.00\cdot10^4$	$-4.99\cdot10^4$	$-1.59\cdot10^4$	$-1.59\cdot10^4$
$Var[r_0]$	$8.42\cdot10^3$	$4.03\cdot10^3$	$1.83\cdot10^4$	$7.82\cdot10^3$	$2.47\cdot10^5$	$1.79\cdot10^5$	$1.09\cdot10^4$	$9.02\cdot10^3$

表 4.10 長笛單一位元特定模型解碼值的統計特性

Flute	N=1	
N=1, $b_0=-1$	實驗值	理論值
SNR_1 (dB)	38.78	41.44
$E[r_0]$	$-4.99\cdot10^4$	$-4.99\cdot10^4$
$Var[r_0]$	$3.30\cdot10^5$	$1.79\cdot10^5$

表 4.11 長笛單一位元非特定模型解碼值的統計特性

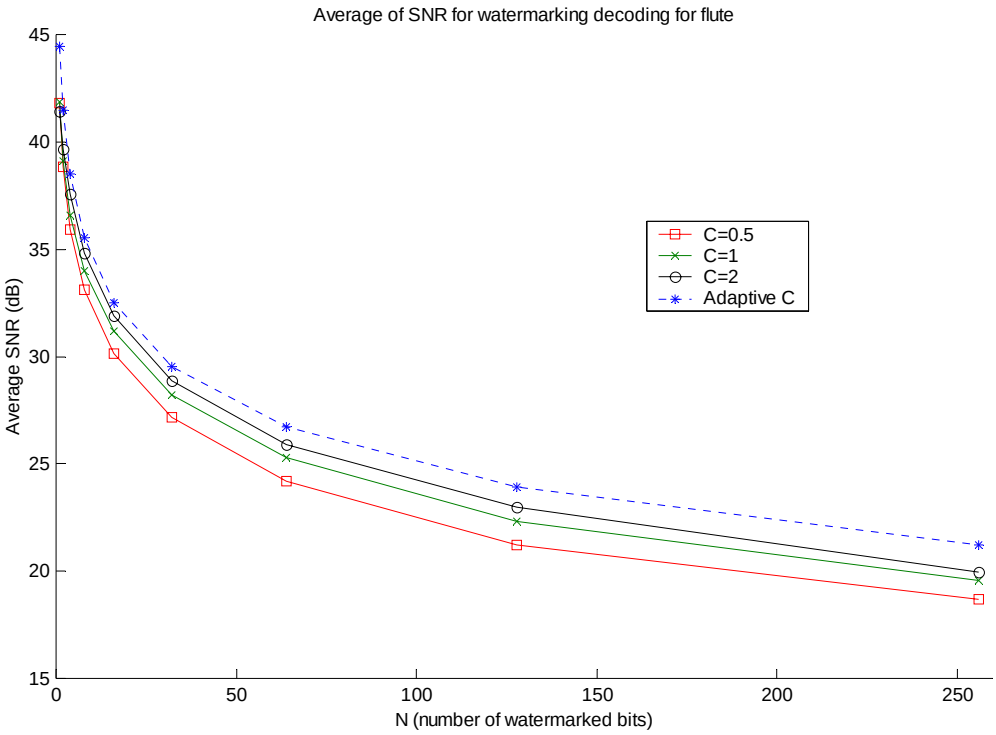


圖 4.7 長笛 N 位元特定模型解碼效能的理論值

第五章　結論與未來展望

回顧本篇論文內容，主要是探討離散餘弦轉換域的加成性展頻音訊浮水印設計，及浮水印檢測器與解碼器的整體效能分析。一開始我們先建立音訊餘弦係數的廣義高斯機率分佈函數，並透過最大相似度檢測理論，推導最小誤警機率 P_F 且最大確認機率 P_D 的浮水印檢測演算法；再根據最大相似度解碼理論，推導最小誤碼機率 P_e 的浮水印解碼演算法。接著我們探討一更廣泛之方法，如果無適當之機率模型可近似時，我們仍可透過降維轉換 $\mathbf{r} = h(K, \mathbf{y})$ 之充分統計特性，應用最大相似度檢測與解碼理論，推導出相關演算法；此方法並可得到降低計算量、省略模型分析過程及應用層面更廣之優點。在論文中我們引入人耳遮蔽效應於音訊浮水印的嵌入架構，並嘗試於浮水印檢測與解碼演算法則下建立一個效能分析的平台，藉以探討各參數及不同之音樂與浮水印檢測解碼效能間的關係。經由分析模型的推演結果發現，當可能隱藏訊息個數 M 值增加時，對整個檢測的效能並無很大的影響，但對解碼器的效能卻造成下降的現象。

不論是特定的廣義高斯的機率分佈函數模擬，或是非特定的機率模型，再配合人耳聽覺模型分析，發展出兼具透明度及安全性的音訊展頻浮水印機制，推導出具快速實現的浮水印檢測與解碼演算法，並在理論分析

的實驗上有了初步令人滿意的具體成果。不過這些條件都是假設無訊號處理失真，也就是 $\mathbf{y} = \mathbf{z}$ 的情況下推導出來的，因此在實際應用的層級上仍有一段距離。畢竟經過網路傳輸或訊號處理，在正常的狀態下，接收端所接收到的加印訊號 $\mathbf{z}$ 並不完全等於 $\mathbf{y}$。因此未來我們必須先推導條件機率函數 $p_{z/y}$，用來表示 $\mathbf{y}$ 與 $\mathbf{z}$ 之間的關係，再應用最大相似度檢測與解碼理論，求出 $\mathbf{y} \neq \mathbf{z}$ 的情況下，快速可實現的相關演算法。

此外，我們將浮水印先鎖定在音樂 CD，由於現今高壓縮率 MP3 技術的廣泛應用，使得非法盜拷嚴重影響到智慧財產權。因此未來我們必須先求出有無適用於 MP3 音樂的特定機率模型，再由此特定或非特定模型，配合最大相似度檢測與解碼之理論分析，求出快速可實現之相關演算法。若能成功發展出適用在 MP3 音樂上的技術，對智慧財產權之保護，將可得到更佳之效果。

參考文獻

[1] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, “Multimedia Data-embedding and Watermarking Technologies,” Proceedings of the IEEE, Vol. 86, Jun 1998, pp. 1064-1087.

[2] F. Hartung, and M. Kutter, “Multimedia Watermarking Techniques,” Proceedings of the IEEE, Vol. 87, Jul 1999, pp. 1079-1107.

[3] C. I. Podilchuk, and E. J. Delp, “Digital Watermarking: Algorithms and Applications,” IEEE Signal Processing Magazine, Vol. 18, Jul 2001, pp. 33-46.

[4] P. Bassia, I. Pitas, and N. Nikolaidis, “Robust Audio Watermarking in the Time Domain,” IEEE Transactions on multimedia, Vol. 3, Jun 2001, pp. 232-241.

[5] A. N. Lemma, J. Aprea, W. Oomen, and L. van de Kerkhof, “A Temporal Domain Audio Watermarking Technique,” IEEE Transactions on Signal Processing, Vol. 51, Apr 2003, pp. 1088-1097.

[6] Ye Wang, “A New Watermarking Method of Digital Audio Content for Copyright Protection,” Signal Processing Proceedings of ICSP '98, Vol. 2, 1998, pp. 1420-1423.

[7] Xin Li, and H. H. Yu, “Transparent and Robust Audio Data Hiding in Subband Domain,” International Conference on Information Technology: Coding and Computing, 2000.

[8] Sang-Kwang Lee and Yo-Sung Ho, “Digital Audio Watermarking in the Cepstrum Domain,” IEEE Transactions on Consumer Electronics, Vol. 46, Aug 2000, pp. 744-750.

[9] L. Boney, A. H. Tewfik and K. N. Hamdy, “Digital Watermarking for Audio Signals,” Processings of MULTIMEDIA '96, IEEE, 1996, pp. 473-480.

[10] M. D. Swanson, B. Zhu, A. H. Tewfik and L. Boney, “Robust audio watermarking using perceptual masking,” Signal Processing, Vol. 66, Nov 1997, pp. 337-355.

[11] C. Neubauer, and J. Herre, “Digital Watermarking and its Influence on Audio Quality,” AES.

[12] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Transactions on Image Processing, Vol. 6, Dec 1997, pp. 1673-1687.

[13] I. I. Cox, M. L. Miller, and J. A. Bloom, “Digital Watermarking,” Morgan Kaufmann Publishers , 1st Edition, 2001.

[14] M. Kutter, and S. Winkler, “A vision-based masking model for spread-spectrum image watermarking,” IEEE Transactions on Image Processing, Vol. 11, Jan 2002, pp. 16-25.

[15] J. R. Hernandez, M. Amado, and F. Perez-Gonzalez, “DCT-domain watermarking techniques for still images: detector performance analysis and a new structure,” IEEE Transactions on Image Processing, Vol. 9, Jan 2000, pp.55-68.

[16] K. A. Birney, and T. R. Fischer, “On the modeling of DCT and subband image data for compression,” IEEE Transactions on Image Processing, Vol. 4, Feb 1995, pp.186-193.

[17] 許宇鳳, “影像與音訊之數位浮水印技術,” 國立台灣大學電信工程研究所碩士論文, 2001.

[18] 張北辰, “音樂信號上的數位浮水印,” 國立台灣大學資訊工程研究所碩士論文, 2001.

[19] J. R. Hernandez, and F. Perez-Gonzalez, “Statistical Analysis of watermarking schemes for copyright protection of images,” Proceedings of the IEEE, Vol. 87, Jul 1999, pp.1142-1166.

[20] A. V. Oppenheim, R. W. Schafer, and J. R. Back, “Discrete-Time Signal Processing,” Prentice Hall International, Inc, Second Edition, 1998.

[21] 蔡若望,“餘弦轉換統計模型在音訊浮水印之研究,”國立交通大學電信工程研究所碩士論文,2003.

附錄

附錄 A. 雙位元特定模型檢測函數的平均與變異值之推導：

$$\text{首先定義 } D(\mathbf{y}) = \ln \sum_{l=0}^{M-1} \prod_{i=0}^{N-1} \exp\left(-\sum_{k \in S_i} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left| y_k - b_{l,i} \cdot \alpha_k \cdot s_k \right|^{C_{\hat{k}}} \right) \tag{A.1}$$

考慮雙位元(N=2，M=4)及事件 H_1 為真之情況：

$$D(\mathbf{y}) = \ln \sum_{l=0}^{3} \exp\left(-\sum_{k \in S_0} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left| y_k - b_{l,0} \cdot \alpha_k \cdot s_k \right|^{C_{\hat{k}}} - \sum_{k \in S_1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left| y_k - b_{l,1} \cdot \alpha_k \cdot s_k \right|^{C_{\hat{k}}} \right) \tag{A.2}$$

$$\text{定義 } D'(l) = -\sum_{k \in S_0} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left| y_k - b_{l,0} \cdot \alpha_k \cdot s_k \right|^{C_{\hat{k}}} - \sum_{k \in S_1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left| y_k - b_{l,1} \cdot \alpha_k \cdot s_k \right|^{C_{\hat{k}}} \tag{A.3}$$

且 $MaxD = \max\{D'(l), l = 0,1,2,3\}$

$$D(\mathbf{y}) = \ln \sum_{l=0}^{3} \exp\left[D'(l) \right] = \ln \left\{ \exp\left[MaxD \right] \cdot \sum_{l=0}^{3} \exp\left[D'(l) - MaxD \right] \right\}$$

$$\approx MaxD + \ln \left\{ \sum_{l=0}^{3} \exp\left[D'(l) - MaxD \right] \right\}$$

因為實驗結果顯示 $\exp[D'(l) - MaxD]$ 為 1 或趨近零之值，所以 $D(\mathbf{y}) \approx MaxD$ 。

假設從集點 $\mathbf{B} = \{\mathbf{b_0}, \mathbf{b_1}, \cdots, \mathbf{b_{M-1}}\}$ 中選擇 $\boldsymbol{b}_{l^*}$ 作嵌入，則 $y_k = x_k + b_{l^*,i} \alpha_k s_k,\ k \in S_i$

$$MaxD = -\sum_{k \in S_0} \beta_{\hat{k}}^{C_{\hat{k}}} \left| y_k - b_{l^*,0} \alpha_k s_k \right|^{C_{\hat{k}}} - \sum_{k \in S_1} \beta_{\hat{k}}^{C_{\hat{k}}} \left| y_k - b_{l^*,1} \alpha_k s_k \right|^{C_{\hat{k}}} \tag{A.4}$$

$$\Lambda'(\mathbf{y}) = \sum_{k=0}^{K_x - 1} \beta_{\hat{k}}^{c_{\hat{k}}} \cdot \left| y_k \right|^{c_{\hat{k}}} + \ln \sum_{l=0}^{M-1} \prod_{i=0}^{N-1} \exp\left(-\sum_{k \in S_i} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left| y_k - b_{l,i} \cdot \alpha_k \cdot s_k \right|^{C_{\hat{k}}} \right) \underset{H_0}{\overset{H_1}{\gtrless}} \ln M$$

$$\Rightarrow \Lambda'(\mathbf{y}) \approx \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|y_k\right|^{C_{\hat{k}}} - \sum_{k\in S_0} \beta_{\hat{k}}^{C_{\hat{k}}} \left|y_k - b_{l^*,0}\alpha_k s_k\right|^{C_{\hat{k}}} - \sum_{k\in S_1} \beta_{\hat{k}}^{C_{\hat{k}}} \left|y_k - b_{l^*,1}\alpha_k s_k\right|^{C_{\hat{k}}}$$

$$= \sum_{k\in S_0} \beta_{\hat{k}}^{C_{\hat{k}}} \left|x_k + b_{l^*,0}\alpha_k s_k\right|^{C_{\hat{k}}} + \sum_{k\in S_1} \beta_{\hat{k}}^{C_{\hat{k}}} \left|x_k + b_{l^*,1}\alpha_k s_k\right|^{C_{\hat{k}}} - \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|y_k\right|^{C_{\hat{k}}} \quad \text{(A.5)}$$

因為 S_k 為唯一變數，且 $P(s_k = 1) = P(s_k = -1) = 0.5$

$$E[\Lambda'(\mathbf{y}) \mid H_1, \mathbf{b}_{l^*}] \approx \frac{1}{2}\left\{\sum_{k\in S_0} \beta_{\hat{k}}^{C_{\hat{k}}} \left(\left|x_k + \alpha_k\right|^{C_{\hat{k}}} + \left|x_k - \alpha_k\right|^{C_{\hat{k}}}\right)\right\}$$

$$+\frac{1}{2}\left\{\sum_{k\in S_1} \beta_{\hat{k}}^{C_{\hat{k}}} \left(\left|x_k + \alpha_k\right|^{C_{\hat{k}}} + \left|x_k - \alpha_k\right|^{C_{\hat{k}}}\right)\right\} + \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|x_k\right|^{C_{\hat{k}}}$$

$$\Rightarrow E\left[\Lambda'(\mathbf{y}) \mid H_1\right] \approx \frac{1}{2}\sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left(\left|x_k + \alpha_k\right|^{C_{\hat{k}}} - \left|x_k - \alpha_k\right|^{C_{\hat{k}}}\right) - \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|x_k\right|^{C_{\hat{k}}} \quad \text{(A.6)}$$

$$Var[\Lambda'(\mathbf{y}) \mid H_1, \mathbf{b}_{l^*}] \approx E\left\{\left[\Lambda'(\mathbf{y}) - E[\Lambda'(\mathbf{y}) \mid H_0, \mathbf{b}_{l^*}]\right]^2\right\}$$

$$\Rightarrow Var\left[\Lambda'(\mathbf{y}) \mid H_1\right] \approx \frac{1}{4}\sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{2C_{\hat{k}}} \cdot \left(\left|x_k + \alpha_k\right|^{C_{\hat{k}}} - \left|x_k - \alpha_k\right|^{C_{\hat{k}}}\right)^2 \quad \text{(A.7)}$$

由實驗得知，在事件 H_0 為真之情況，仍會造成 $D(\mathbf{y}) \approx MaxD$ 之結果，同理：

$$E\left[\Lambda'(\mathbf{y}) \mid H_0\right] \approx \sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left|x_k\right|^{C_{\hat{k}}} - \frac{1}{2}\sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{C_{\hat{k}}} \cdot \left(\left|x_k + \alpha_k\right|^{C_{\hat{k}}} - \left|x_k - \alpha_k\right|^{C_{\hat{k}}}\right) \quad \text{(A. 8)}$$

$$Var\left(\Lambda'(\mathbf{y}) \mid H_0\right) \approx \frac{1}{4}\sum_{k=0}^{K_x-1} \beta_{\hat{k}}^{2C_{\hat{k}}} \cdot \left(\left|x_k + \alpha_k\right|^{C_{\hat{k}}} - \left|x_k - \alpha_k\right|^{C_{\hat{k}}}\right)^2 \quad \text{(A.9)}$$

附錄 B. N位元非特定模型檢測函數的平均與變異值之推導:

由(4.21)式得知 $\hat{b} = sign(r_i), \quad i = 0,1,2,\cdots,N-1$ ，

1) if $b_{l,i} = 1 \rightarrow r_i > 0$ ，實驗數據也顯示 $r_i \gg 1$ ，所以 $\exp(-\frac{2a_i r_i}{\sigma_{r_i}^2}) \ll 1$ 且

$$\ln[1+\exp(-\frac{2a_i r_i}{\sigma_{r_i}^2})] \approx 0$$

$$\Rightarrow \ln[\cosh(\frac{a_i r_i}{\sigma_{r_i}^2})] = \ln\left[\exp(\frac{a_i r_i}{\sigma_{r_i}^2})\cdot[1+\exp(-\frac{2a_i r_i}{\sigma_{r_i}^2})]\right] - \ln 2$$

$$\approx \frac{a_i r_i}{\sigma_{r_i}^2} - \ln 2 \qquad \text{(B.1)}$$

2) if $b_{l,i} = -1 \rightarrow r_i < 0$ ，且 $\because \exp(\frac{2a_i r_i}{\sigma_{r_i}^2}) \ll 1 \quad \therefore \ln[1+\exp(\frac{2a_i r_i}{\sigma_{r_i}^2})] \approx 0$

$$\Rightarrow \ln[\cosh(\frac{a_i r_i}{\sigma_{r_i}^2})] = \ln\left[\exp(-\frac{a_i r_i}{\sigma_{r_i}^2})\cdot[\exp(\frac{2a_i r_i}{\sigma_{r_i}^2})+1]\right] - \ln 2$$

$$\approx -\frac{a_i r_i}{\sigma_{r_i}^2} - \ln 2 \qquad \text{(B.2)}$$

綜合 1) & 2) $\Rightarrow \ln[\cosh(\frac{a_i r_i}{\sigma_{r_i}^2})] \approx \frac{b_{l,i} a_i r_i}{\sigma_{r_i}^2} - \ln 2$ (B.3)

故 $\Lambda(r) = -\frac{1}{2}\sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} + \sum_{i=0}^{N-1}\ln[\cosh(\frac{a_i r_i}{\sigma_{r_i}^2})]$

$$\approx -\frac{1}{2}\sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} + \sum_{i=0}^{N-1}\frac{a_i r_i b_{l,i}}{\sigma_{r_i}^2} - N\cdot\ln 2 \qquad \text{(B.4)}$$

據此可推得 $E[\Lambda(r)\,|\,H_1] = -\frac{1}{2}\sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} + \sum_{i=0}^{N-1}\frac{a_i b_{l,i}}{\sigma_{r_i}^2}\cdot E[r_i] - N\cdot\ln 2$ 且 $E[r_i] = b_{l,i}a_i$

$$\Rightarrow E[\Lambda(r)\,|\,H_1] = \frac{1}{2}\sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} - N\cdot\ln 2 \qquad \text{(B. 5)}$$

$$Var[\Lambda(r)\,|\,H_1] = Var[\sum_{i=0}^{N-1}\frac{a_i\, r_i b_{l,i}}{\sigma_{r_i}^2}]$$

$$= \sum_{i=0}^{N-1}(\frac{a_i b_{l,i}}{\sigma_{r_i}^2})^2\cdot Var[r_i]$$

$$= \sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} \qquad (\text{因為 } b_{l,i} = \pm 1 \text{ 且 } Var[r_i] = \sigma_{r_i}^2) \qquad \text{(B. 6)}$$

同理，亦可推出 $E[\Lambda(r)\,|\,H_0] \approx -\frac{1}{2}\sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} - N\cdot\ln 2$ (B. 7)

$$Var[\Lambda(r)\,|\,H_0] \approx \sum_{i=0}^{N-1}\frac{a_i^2}{\sigma_{r_i}^2} \qquad \text{(B. 8)}$$

附錄 C. 不固定分區時解碼函數之平均與變異值之推導：

4.2.2 節所推導結果只適用於描述單一特定集合$\{S_j\}_{j=0}^{N-1}$時r_j的統計特性，問題是依金鑰K所產生的集合有許多分割方式，$\Gamma=\{S_j\}_{j=0}^{N-1}$可視為一隨機變數，更明確地說，(4.11)的$E[r_j]=E[r_j|\Gamma]$，(4.12)的$Var[r_j]=Var[r_j|\Gamma]$。由於餘弦轉換係數所對應的$N$個子集合$\{S_j\}_{j=0}^{N-1}$互不相關，滿足$S_j\cap S_i=\phi,\ \forall i\neq j$，且這些子集合代表著訊息位元元$b_j$可嵌入的空間，所以對每個子集合考慮的參數$r_j$，彼此之間也是互相獨立不相關。所以我們可將(4.11)及(4.12)式在$\Gamma=\{S_j\}_{j=0}^{N-1}$發生的條件下展開，計算整段音訊$r_j$的統計特性，進而推導出評估該音訊解碼時誤碼機率$P_e$的關係式。

[定理]：$E[r_j]=E_\Gamma\left[\ E\left[\ r_j|\Gamma\right]\ \right]$ (C.1)

$$Var[r_j]=E_\Gamma\left[\ Var\left[\ r_j|\Gamma\right]\ \right]+Var_\Gamma\left[\ E\left[\ r_j|\Gamma\right]\ \right] \quad \text{(C.2)}$$

[證明]：

$$E_\Gamma\left[E\left[r_j|\Gamma\right]\right]=\int_{-\infty}^{\infty}E\left[r_j|\Gamma\right]\cdot f_\Gamma(\Gamma)\,d\Gamma$$

$$=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}r_j\cdot f_{r_j}\left(r_j|\Gamma\right)dr_j\cdot f_\Gamma(\Gamma)\,d\Gamma$$

$$=\int_{-\infty}^{\infty}r_j\int_{-\infty}^{\infty}f_{r_j,\Gamma}\left(r_j,\Gamma\right)dr_j\,d\Gamma$$

$$=\int_{-\infty}^{\infty}r_j\cdot f_{r_j}\left(r_j\right)dr_j=E\left[r_j\right]$$

$$E_\Gamma\left[Var\left[r_j \mid \Gamma\right]\right] = \int_{-\infty}^{\infty} Var\left[r_j \mid \Gamma\right] \cdot f_\Gamma(\Gamma) d\Gamma$$

$$= \int_{-\infty}^{\infty} E\left[\left(r_j - E\left[r_j \mid \Gamma\right]\right)^2 \mid \Gamma\right] \cdot f_\Gamma(\Gamma) d\Gamma$$

$$= \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \left(r_j - E\left[r_j \mid \Gamma\right]\right)^2 \cdot f_{r_j}\left(r_j \mid \Gamma\right) dr_j \cdot f_\Gamma(\Gamma)\, d\Gamma$$

$$= \int_{-\infty}^{\infty} r_j^2 f_{r_j}\left(r_j\right) dr_j - 2\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} E\left[r_j \mid \Gamma\right] r_j f_{r_j}\left(r_j \mid \Gamma\right) dr_j f_\Gamma(\Gamma) d\Gamma + \int_{-\infty}^{\infty} \left(E\left[r_j \mid \Gamma\right]\right)^2 f_\Gamma(\Gamma) d\Gamma$$

$$= E\left[r_j^2\right] - 2\int_{-\infty}^{\infty} \left(E\left[r_j \mid \Gamma\right]\right)^2 \cdot f_\Gamma(\Gamma) d\Gamma + \int_{-\infty}^{\infty} \left(E\left[r_j \mid \Gamma\right]\right)^2 \cdot f_\Gamma(\Gamma) d\Gamma$$

$$= E\left[r_j^2\right] - \int_{-\infty}^{\infty} \left(E\left[r_j \mid \Gamma\right]\right)^2 \cdot f_\Gamma(\Gamma) d\Gamma$$

$$Var_\Gamma\left[E\left[r_j \mid \Gamma\right]\right] = \int_{-\infty}^{\infty} \left(E\left[r_j \mid \Gamma\right]\right)^2 \cdot f_\Gamma(\Gamma) d\Gamma - \left(\int_{-\infty}^{\infty} E\left[r_j \mid \Gamma\right] \cdot f_\Gamma(\Gamma) d\Gamma\right)^2$$

$$= \int_{-\infty}^{\infty} \left(E\left[r_j \mid \Gamma\right]\right)^2 \cdot f_\Gamma(\Gamma) d\Gamma - \left(E\left[r_j\right]\right)^2$$

$$\Rightarrow E_\Gamma\left[Var\left[r_j \mid \Gamma\right]\right] + Var_\Gamma\left[E\left[r_j \mid \Gamma\right]\right] = E\left[r_j^2\right] - \left(E\left[r_j\right]\right)^2 = Var\left[r_j\right]$$

假設 $\Pr\{k \in S_j\} = 1/N$，將(4.11)及(4.12)式重新展開，求得 $\Gamma = \{S_j\}_{j=0}^{N-1}$ 視為一隨機變數的 r_j 的統計特性：

$$E\left[r_j\right] = E_\Gamma\left[\sum_k \frac{E\left[h_k\right]}{C_{\hat{k}}}\right] = \sum_{k=0}^{K_x-1} \frac{E\left[h_k\right]}{C_{\hat{k}}} \cdot P_r\left\{\ k \in S_j\right\} = \frac{1}{N}\sum_{k=0}^{K_x-1} \frac{E\left[h_k\right]}{C_{\hat{k}}} \qquad \text{(C.3)}$$

$$Var\left[r_j\right] = Var\left[\sum_k \frac{Var\left[h_k\right]}{2C_{\hat{k}}}\right] = E_\Gamma\left[\ Var\left[\ r_j \mid \Gamma\right]\ \right] + Var_\Gamma\left[\ E\left[\ r_j \mid \Gamma\right]\ \right] \qquad \text{(C.4)}$$

其中 $E_\Gamma\left[\ Var\left[\ r_j \mid \Gamma\right]\ \right] = \sum_{k=0}^{K_x-1} \frac{Var\left[h_k\right]}{\sigma_{\hat{k}}^{2C_{\hat{k}}}} \cdot P_r\left\{\ k \in S_j\right\} = \frac{1}{N}\sum_{k=0}^{K_x-1} \frac{Var\left[h_k\right]}{\sigma_{\hat{k}}^{2C_{\hat{k}}}}$ (C.5)

$$Var_\Gamma\left[E\left[r_j \mid \Gamma\right]\right] = E_\Gamma\left[E^2\left[r_i \mid \Gamma\right]\right] - \left(E_\Gamma\left[E\left[r_j \mid \Gamma\right]\right]\right)^2 \quad \text{(C.6)}$$

$$E_\Gamma\left[E^2\left[r_i \mid \Gamma\right]\right] = \sum_{k=0}^{K_x-1}\sum_{k'=0}^{K_x-1} \frac{E\left[h_k\right]\cdot E\left[h_{k'}\right]}{\left(\sigma_{\hat{k}}\cdot\sigma_{\hat{k}'}\right)^{C_{\hat{k}}}} \cdot P_r\left\{\ k \in S_j,\quad k' \in S_j\right\}$$

$$= \frac{N-1}{N^2}\sum_{k=0}^{K_x-1} \frac{E^2\left[h_k\right]}{\sigma_{\hat{k}}^{2C_{\hat{k}}}} + \left(\frac{1}{N}\sum_{k=0}^{K_x-1} \frac{E\left[h_k\right]}{\sigma_{\hat{k}}^{C_{\hat{k}}}}\right)^2$$

$$= \frac{N-1}{N^2}\sum_{k=0}^{K_x-1} \frac{E^2\left[h_k\right]}{\sigma_{\hat{k}}^{2C_{\hat{k}}}} + \left(E_\Gamma\left[E\left[r_j \mid \Gamma\right]\ \right]\right)^2 \quad \text{(C.7)}$$

將(C.7)式帶入(C.6)式中，就可得到：

$$Var_\Gamma\left[\ E\left[\ r_j \mid \Gamma\right]\ \right] = E_\Gamma\left[E^2\left[r_i \mid \Gamma\right]\right] - \left(E_\Gamma\left[E\left[r_j \mid \Gamma\right]\ \right]\right)^2 = \frac{N-1}{N^2}\sum_{k=0}^{K_x-1} \frac{E^2\left[h_k\right]}{\sigma_{\hat{k}}^{2C_{\hat{k}}}} \quad \text{(C.8)}$$

因此整體的 r_j 變異值就為：

$$Var\left[r_j\right] = \frac{1}{N}\sum_{k=0}^{K_x-1} \frac{Var\left[h_k\right]}{\sigma_{\hat{k}}^{2c_{\hat{k}}}} + \frac{N-1}{N^2}\sum_{k=0}^{K_x-1} \frac{E^2\left[h_k\right]}{\sigma_{\hat{k}}^{2c_{\hat{k}}}} \quad \text{(C.9)}$$