

頻域混音器的自動化解密設計

Automated Cryptanalysis of Frequency-Domain Speech Scramblers

計劃編號：NSC-88-2218-E009-035

執行期限：87.8.1~88.7.31

主持人：張文輝 交通大學電信工程系所 副教授

一、中文摘要

(關鍵字：頻域混音器、統計型解密、最大相似預估、理想匹配問題、遺傳演算)

頻域混音器是利用語音頻譜係數位位的擬亂置換，使竊聽者無法辨認其殘存寓音，同時不能輕易破解加密用擬亂序列的金匙。在傳統的分立式金匙空間考慮下，解密者只能依序比對所有可能的置換才能發現金匙。統計型解密的主要構想則是比對密語頻譜與置換後樣本頻譜之間的相似性，將密語攻擊問題簡化為能作漸進處理的最大相似預估過程。我們考慮連續頻譜係數互不相關的假設，定義相似性函數以及有關的頻譜分布機率。一般而言，秘密的置換矩陣是固定不變或間隔一段時間才調整，因此累積連續音框的資訊並透過適當處理，這個解密攻擊可以轉換成為一個符合最佳化計算的理想匹配問題。使用隨機性神經網路是一個可行的方案，但它有容易落入局部極小點與運算量複雜的缺點；解決之道則在建立一個以遺傳演算技術為主體的統計型解密技術以達到搜尋其能量函數整體極小值之目的。

英文摘要

(Keyword: frequency domain scramblers, statistical cryptanalysis, maximum likelihood estimation, perfect matching problem, genetic algorithm)

The frequency domain speech scrambler derives its cryptanalytic strength from random permutation of speech spectrum. Since in most systems the entire security resides in the permutation (the key), it is worth discussing the process of deducing correct key from insufficiently scrambled speech. Through the statistical cryptanalysis, the discrete key is imbedded in a continuous

keyspace and the key search is realized in the maximum likelihood estimation process. To derive the likelihood function, we assume that successive spectral components are mutually independent. For greater efficiency, this task can be formulated as one of the perfect matching problems that leads to search of the permutation associated with the minimum cost. One possible solution is to use stochastic neural networks, in which both the learning phase and the search phase are involved. The former is to determine the synaptic weights and the thresholds required for defining the neural model. This trained model will then be used in the search phase. But it is easily trapped into local optimal solution and the computational complexity will increase with the dimension of permutation matrix. To overcome these shortages, we will investigate a genetic algorithm to find the global optimal solution. As compared with Baum's iterative maximization algorithm, the genetic-based search is shown to yield better performance by taking into account the doubly stochastic constraint of the underlying keyspace.

二、計劃緣由與目的

電信交換網路因分布普及且撥接方便，已被廣泛接受為人類溝通的最重要媒介。為了確保通訊隱私而發展的語音保密技術，則可區分為類比混音器(scrambler)與數位加密器(encrypter)兩大項，前者製作簡單而後者保密效果較佳[1,2]。基於類比電話仍支配目前電信市場之事實，許多商業化語音保密設備仍採用類比混音技術，主要對明語(palintext)頻譜結構進行擬亂置換(pseudo-random permutation)而得到難懂的密語(ciphertext)。相對而言，解密學者(cryptanalyst)的研究動機在於嘗試破解啟

動擬亂序列的金匙(key)。最近澳洲學者 Goldberg[3]提出的自動化解密技術，是利用訓練語料的頻譜特性建立碼書(codebook)內容，再依序與密語頻譜進行比對找出置換金匙。它主要缺點在於耗時的解密過程，這是因為分立式金匙空間只能依賴地毯式搜尋。因此在此計劃中，我們重新定義一個連續性金匙空間，並將原本複雜的金匙比對簡化為漸進處理的最大相似預估(maximum likelihood estimation)演算。有關語音頻譜分佈將作獨立不相關的假設。之後再透過適當處理使問題轉化為以隨機性神經網路作最佳化計算的理想匹配問題(perfect matching problem)[4]。如何解決假穩定點和局部極小點問題，仍是目前國際上神經最佳化計算的重要課題。傳統的梯度漸近(gradient iterative)法，只能依循能量降低方向搜尋，因此有停頓在局部極小點的潛在危機。有鑑於此，我們將考慮隨機搜尋的遺傳演算法[5]，善用其染色體配對與基因突變的世代交替遺傳演化，以期求得整體最佳值。

三、研究方法與成果

頻域混音器是目前常見的商業化語音加密技術。信號處理流程如下：先將輸入語音作傅立葉轉換取得明語頻譜， $X=[X(1), X(2), \dots, X(N)]^T$ ，再作擬亂置換處理 $C=R \cdot X$ 取得密語頻譜 $C=[C(1), C(2), \dots, C(N)]^T$ 。這種擬亂置換能有效破壞語音頻譜結構，使殘存密語寓意難以辨認。整個加密系統的安全性取決於能否破解置換矩陣 $R=[r_{ij}]$ ，其中 $r_{ij}=1$ 代表第 j 個明語頻譜係數 $X(j)$ 被置換到第 i 個密語頻譜係數 $C(i)$ 位置，其餘值設定為 0。為避免分立式金匙空間的搜尋比對，我們將重新定義一個連續性金匙空間，再利用最大相似預估理論發展更有效的解密技術。針對各項研究方法與進行步驟，詳細說明如下：

(一) 統計型密語攻擊過程：

主要構想是將密語的頻譜置換視為隨機變數，並埋藏(embed)待解的置換矩陣於一個連續性金匙空間。它包含了所有可能的 doubly stochastic matrix $H=[h_{ij}]$ ，其中 h_{ij} 值為介於 0 到 1 之間

的任何實數，同時滿足行約束 $\sum_j h_{ij}=1$ 以及列約束 $\sum_i h_{ij}=1$ 。解密程序如下：首先

搜集大量語料，建立一個能涵蓋語音頻譜特性的樣本(template)機率分布 P_x ，我們考慮以連續頻譜係數互不相關的假設來計算語音頻譜機率分布。具體地說， $P_x=[P_{jl}]_{q \times m}$ ，其中 P_{jl} 代表第 j 個頻譜係數被量化為第 l 個量化層次的機率， q 為頻譜係數數目， m 為各個頻譜係數能量的量化層次數目。配合第 n 個音框使用的連續性置換矩陣 H_n ，樣本頻譜經置換處理後的機率分布可以推論為 $H_n P_x$ 。再計算它與密語頻譜 C 之間的相似性(likelihood) $L(C_n, H_n P_x)$ 。透過這層詮釋，我們可以進行最大相似估測演算取得最佳化攻擊結果 $\hat{H}_n$ ，進一步量化求得分立式置換矩陣 $\hat{R}_n$ ，在據以反向解密處理始能還原出易懂的明語。

(二) 理想匹配問題描述：

對於統計型解密觀念而言，其目的是要在滿足 doubly stochastic constraint 的條件下，搜尋出使相似函數為最大的置換矩陣。這個研究動機正符合所謂的理想匹配問題。此問題描述如下：在兩組相同元素數目的集合 S_1 及 S_2 中，給定一成本矩陣 $\{d_{ij}\}$ ，找出一個每個元素只能對應一次的連接矩陣 $\{a_{ij}\}$ 使得成本函數 $\sum_i \sum_j d_{ij} a_{ij}$ 為最小。因此我們將最大相似函數轉換為成本函數的形式：

$$F = -\log L(C_n, R_n) = \sum_{j=1}^q \sum_{k=1}^q \beta_{jk} r_{jk}$$

其中 $\beta_{jk} = \sum_{l=1}^m c_{n,ij} \left(1 - \frac{\log(n_{kl})}{\log(N)} \right)$ 。接下來我們所要面臨的問題將是如何尋找一個最佳置換矩陣 $\{r_{jk}\}$ 使它的成本函數為最小。

(三) 神經最佳化計算：

常用於解決理想匹配問題的方法之一為考慮使用 Hopfield 隨機性回饋神經網路做最佳化計算。它的特色為穩態收斂值會對應到能量極小值。此過程可分為兩個階段執行：訓練階段與搜尋階段。前者決定網路內部不同層級間傑點連接

所需的權值(weights)，後者則利用神經網路的漸進穩定狀態完成能量極小值的搜尋任務。在我們問題中，能量函數為

$$E = \frac{A_1}{2} \sum_{j=1}^q \sum_{k=1}^q \beta_{jk} r_{jk} + \frac{A_2}{2} \sum_{j=1}^q \sum_{k=1}^q \sum_{k \neq j} r_{jk} r_{jk} + \frac{A_3}{2} \sum_{j=1}^q \sum_{k=1}^q \sum_{j \neq k} r_{jk} r_{jk} + \frac{A_4}{2} \left(\sum_{j=1}^q \sum_{k=1}^q r_{jk} - q \right)^2$$

為了方便網路計算，能量函數必須改寫如下：

$$E = \frac{-1}{2} \sum_{j=1}^q \sum_{k=1}^q \sum_{j'=1}^q \sum_{k'=1}^q W_{jkj'k'} r_{jk} r_{j'k'} - \sum_{j=1}^q \sum_{k=1}^q \theta_{jk} r_{jk}$$

其中節點所用的權值與門檻值計算如下：

$$W_{jkj'k'} = -A_2 \delta_{jj'} (1 - \delta_{kk'}) - A_3 \delta_{kk'} (1 - \delta_{jj'}) - A_4$$

$$\theta_{jk} = q \cdot A_4 - \frac{A_1}{2} \beta_{jk}$$

一旦權值與門檻值確定，我們就可以利用 Hopfield-like continuous-valued model 來搜尋能量極小值。

(四) 隨機搜尋的遺傳演算法：

神經網路的最佳化計算將會遭遇掉入區域最小值(local minimum)與計算複雜度會隨著維度(dimension)迅速增加等問題。為克服這些缺點，我們採用遺傳演算法(genetic algorithm)，善用其全域平行的隨機搜尋能力以保證系統趨於全域最佳解(global optimum)。遺傳演算試述如下：基於適者生存的原則，讓基因庫內的親代染色體依其適性(fitness)的優劣排序決定所賦予子代的數目。再利用配對將兩個親代基因做交換重組，以產生能遺傳部分性徵的子代。至於突變的功能，則是在基因進化過程適時加入干擾，始能保持足夠的群體亂度以避免過早收斂的問題。在我們問題中，我們將以置換(permutation)表示法的基因形式，

$$\log L(C_n, R_n) = - \sum_{j=1}^q \sum_{k=1}^q \beta_{jk} r_{jk} \text{ 為適性函數，}$$

並採用適應性選擇運算子，部分對應交換運算子(partial-mapped crossover)以及相互交換突變運算子(reciprocal exchange mutation)，以達到全域最小值求得最佳置換矩陣。

四、結論與討論

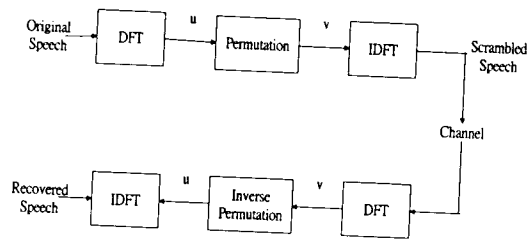
為測試我們提出解密方法的有效

性，我們需要使用兩個資料庫：第一個資料庫用來計算語音頻譜機率分布，它由三位男性及三位女性產生的 30 句語音組成；另一個資料庫是為了產生加密後的語音，它由 4 句語音組成。針對所有測試樣本，皆為 8KHz 取樣率，每個音框有 256 個取樣點。我們以客觀測試 matrix coincidence ratio(MCR)與 LPC distance 來判別解密效果的好壞。若 MCR 增加或 LPC distance 減小，則代表所聽到之破解語音效果上有所進步。

在此計劃中，我們針對 DFT 頻域混音器實行破解，金匙維度為 87。我們將加密後的語音分別以 Baum's 疊代演算法與遺傳演算法進行破解，MCR 與 LPC distance 的結果分別列於表一、表二，由結果可以看出遺傳演算法確實有極佳的破解效果，並優於 Baum's 疊代演算法。另外我們也考慮時變性 DFT 頻域混音器的情況，它是隨機選擇四個置換矩陣並每四個音框重複使用。由表三我們可以得知，遺傳演算法在攻擊時變性 DFT 混音器方面也有不錯的成果。最後，我們期望在未來發展中，試圖理論分析遺傳運算子，以使遺傳演算法能夠更有效地應用於不同最佳化問題上。

參考文獻

- [1] H. Beker and F. Piper, *Secure Speech Communication*, Academic Press, 1985.
- [2] B. Schneier, *Applied Cryptography*, John Wiley & Sons, New York, 1994.
- [3] B. Goldberg, E. Dawson, and S. Sridharan, "The automated cryptanalysis of analog speech scramblers," *Proceedings of EUROCRYPT'91*, Springer-Verlag, New York, pp. 422-430, 1991.
- [4] S. Y. Kung, *Digital Neural Networks*, Prentice Hall, Englewood Cliffs, NJ, 1993.
- [5] J. Hertz, A. Krogh, and R. G. Palmer, *Introduction to the Theory of Neural Computation*, Addison-Wesley, Reading, MA, 1991.

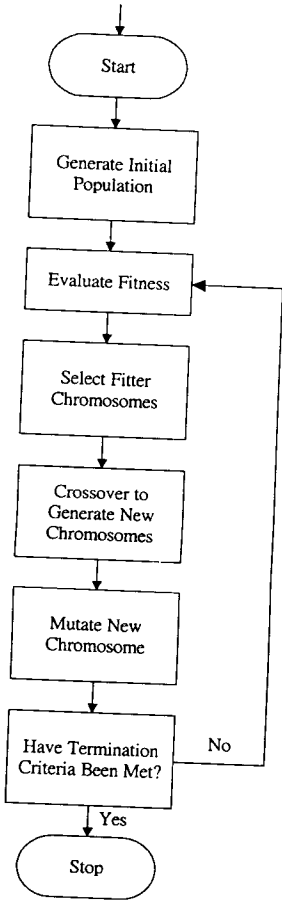


圖一 頻域混音器之流程圖

	Original/scrambled	Original/recovered (Baum's Method)	Original/recovered (Genetic Method)
Data1	1.72	0.68	0.20
Data2	1.73	1.00	0.26
Data3	1.86	1.17	0.26
Data4	2.19	0.62	0.26
Avg.	1.88	0.87	0.25

表三 時變性 DFT 頻域混音器解密結果

	MCR	LPC distance	
		Original/scramble d	Original/recovered
Data1	50.00	1.88	0.28
Data2	50.57	2.00	0.28
Data3	47.13	2.10	0.25
Data4	47.70	2.57	0.26



圖二 遺傳演算法流程

表一 不同解密方法 MCR 之比較

Method	Data1	Data2	Data3	Data4
Baum's method	34.49	31.90	31.79	30.80
Genetic method	47.05	45.99	42.97	46.84

表二 LPC-distance 比較結果