使用展頻技術之數值型資料庫浮水印
Watermarking of Numerical Databases Using Spread Spectrum Techniques

楊英一(Yin-Yi Yang)
國立高雄第一科技大學
高雄市卓越路 2 號

吳大鈞(Da-Chun Wu)
國立高雄第一科技大學
高雄市卓越路 2 號
dcwu@ccms.nkfust.edu.tw

蔡文祥(Wen-Hsiang Tsai)
國立交通大學
新竹市大學路 1001 號
亞洲大學
臺中縣霧峰鄉柳豐路 500 號
whtsai@cis.nctu.edu.tw

摘要

本論文應用展頻概念，發展出兩種可使用於資料庫之強韌性浮水印技術。我們對不同的授權者給與不同識別碼，以產生特定之浮水印訊號，並將其嵌入資料庫之部份值組中，以保護資料庫之版權。第一種技術是一種針對極少變動之資料倉儲，在有原始資料可供參考之前提下，以輕微修改值組資料來藏入版權訊號的方法。此方法藉由比對原始資料和被偵測資料庫中的相對資料，擷取出所嵌入的浮水印訊號，並利用統計上計算相關係數的方式，來提高偵測浮水印之精確度。第二種技術是針對異動頻繁之資料庫，在沒有原始資料可供參考的情況下，嵌入版權保護訊號的一種方法。此方法利用統計假設檢定的方式進行浮水印分析，並以設定顯著水準α值的方式，控制誤判的可能性。在資料庫進行新增、刪除或修改之攻擊後，所提方法仍然可以偵測出所嵌入之版權訊號。使用者使用已嵌入版權資訊之資料庫時，並不會感覺到浮水印的存在。一旦發現資料庫之資料可能被濫用時，即可透過偵測嫌疑資料庫是否有隱藏浮水印訊號，以判別資料是否被盜用，並可得知資料之來源，以達到嚇阻濫用之效果。實驗顯示所提方法之有效性。

關鍵詞

版權保護、資料庫、展頻、浮水印

1. 簡介

數位化的資訊因為複製成本低廉且流通快速，非常容易被盜用。將他人的心血結果販售圖利，更會造成其原著作人或擁有者之損失。網際網路出現後，資訊傳送更加便利，使得此類問題日趨嚴重。數位浮水印技術[1-3]為近年來熱門的資訊保護技術之一，是以不引人注意的方式將版權相關訊息嵌入數位資料中，以達到保護之目的。常見的數位資料包括影像、視訊、音樂等多媒體產品。當資料之版權發生爭議時，可將所嵌入之浮水印訊息擷取出，以解決糾紛。數位浮水印主要的應用為驗證資料真確性之竄改防護及與智財權相關之版權保護。其中版權保護之浮水印技術須具有忍受破壞攻擊之強韌性。

資料庫是機構或企業之重要資源，以大量時間與金錢維護之資料萬一被盜拷，不但機密會外洩，也可能會流失大量利益。目前有些機構或企業願意將未含敏感性資料之資料庫，出售給單位或是個人從事資料探勘等相關研究，以增加收入。要如何嚇阻盜用者整批盜拷、違法逐筆收錄資料，或防止已售出之資料庫不被買方二次販售而喪失原擁有者應有之利益，實為當前嶄新之重要課題。

資料庫中所儲存的資料，多是對於事實的客觀記錄，例如買賣交易。這類型資料要找出可供修改之空間以嵌入版權資訊，並不是件容易的事。然而並非所有資料記錄都不

允許修改。以一般實驗性數值資料而言，因為測量儀器本身就會存在可能之誤差，重複同一測量，數據也會不盡相同。這些誤差便造就出來微小的修改空間，可以用來嵌入浮水印。相較於線上作業用的資料庫，資料倉儲內的資料是用來進行分析和彙總，所以若對資料倉儲內的資料，即使如交易之金額與數量等資訊做局部修改，對資料分析之結果也不會有太大的影響，也就是說不會喪失資料倉儲之可用性。Wagner, Fountain 和 Hazy[4]曾運用隨機產生的位元資料當作嵌入資料庫之訊號，將每個位元資料對應到資料庫中的一個值組。嵌入方法是依據所對應值組之數值屬性，將屬性值以加上或減去其可容忍之誤差，表示所嵌入的訊號為“0”或“1”。偵測浮水印訊號時，抽取部份被偵測之資料庫內的資料，和原始資料庫之資料相減，將結果與原始浮水印做假設檢定，以檢驗是否有嵌入浮水印。Agrawal 等人提出的方法[5, 6]是假設檢驗浮水印時沒有原始資料庫可供參考。在浮水印嵌入的過程中，必須有可供嵌入浮水印的目標屬性及可供參考以產生浮水印之參考屬性。參考屬性是用來決定須嵌入浮水印之值組。嵌入浮水印資料時，將資料分為重要位元(MSB)和不重要位元(LSB)兩部份，將 LSB 部份視為資料之可忍受誤差範圍。利用參考屬性資料，設定 LSB 中的一個位元之值，代表所嵌入的浮水印訊號。用來參考以產生浮水印訊號之屬性資料，須具有唯一性(Identity)。在檢驗浮水印訊號時可用參考屬性來判斷值組中是否有藏入浮水印訊號。一般來說主鍵屬性很適合擔任參考屬性，若沒有主鍵屬性時，則可以利用其他較為重要的候選鍵屬性當作參考屬性。Sion, Atallah 和 Prahakar 提出利用資料所呈現的分配，嵌入浮水印訊號的方法[7]。其方法為將資料分群，被分群的資料具常態分配(Normal Distribution)的特性，資料呈現出鐘形(Bell Shape)分佈。利用修改鐘形兩端資料的方式，嵌入浮水印訊號。

通訊領域之展頻[8]概念是利用雜訊產生器產生連續之雜訊，並把欲傳送資料延展於此雜訊中，使其可以抵抗外來之干擾與攻擊。接收方必須使用與傳送方相同之雜訊產生器，擷取藏在雜訊中之資料。若是有惡意之竊聽者意圖擷取雙方傳送之資料，在沒有同一雜訊產生器之情況下，很難得知雙方實際通信之訊息為何。展頻技術可分為跳頻展頻(frequency hopping spread spectrum)和直接序列展頻(direct sequence spread spectrum)兩種。Cox 等人[1]曾提出之展頻浮水印技術為強韌性浮水印經典技術。該技術將浮水印訊號打散，嵌入於影像之離散餘弦係數中。當影像遭受惡意攻擊時，仍能正確地擷取出浮水印訊號。本論文將提出運用展頻概念，設計資料庫版權保護之強韌性浮水印技術，在資料庫中嵌入浮水印訊號，以建構強韌性浮水印。我們將以跳頻展頻概念，選擇資料庫之部份值組嵌入浮水印訊號，以避免嵌入浮水印之值組被發覺。在資料庫進行新增、刪除或修改之攻擊後，仍然可以偵測出所嵌入之版權訊號。使用者使用已嵌入版權資訊之資料庫時，並不會感覺到浮水印的存在。一旦發現資料庫之資料可能被盜用時，即可透過偵測嫌疑資料庫是否有隱藏浮水印訊號，得知資料之來源，以達到嚇阻濫用之效果。

有關本論文之後的章節編排，在第二節中將介紹在有原始資料庫可供參考的版權浮水印之嵌入及偵測方法。第三節將探討沒有原始資料庫可供參考的版權浮水印嵌入及偵測方法。第四節中將展示以上兩種方法之實驗結果，最後一節為結論。

2. 有原始資料庫可供參考之版權保護

2.1 版權浮水印嵌入

本方法利用輕微修改可以容忍誤差之數值型屬性資料以嵌入版權識別碼 k。首先設定資料庫中欲修改之值組比例 θ(百分比)，以避免因大規模修改資料，喪失資料庫之可用性。以主鍵或候選鍵為參考屬性。利用跳頻展頻概念逐一檢視資料庫中所有值組之參考屬性之屬性值 p，以布林雜湊函數 S 決定那些值組須嵌入浮水印訊號。雜湊函數 S 之參數為 k、θ、p，運作方式為

$$S(k, p, \theta) = \begin{cases} true & embed \\ flase & skip \end{cases} \qquad (1)$$

識別碼 k 代表欲嵌入之版權浮水印，利用直接序列展頻概念設計以識別碼 k 及參考屬性之屬性值 p 為參數之浮水印訊號產生函數 $W(k, p)$，所產生之浮水印訊號為 $w = \{+1, -1\}$。假設欲嵌入浮水印的目標屬性之屬性值 d 之可容忍誤差範圍 δ。浮水印訊號 w 之嵌入方式係對 d 作正向(+)或是負向(-)的修改，修改後之結果值 $\hat{d}$ 可表示成

$$\hat{d} = d + \alpha \times \delta \times w \tag{2}$$

其中 α 為嵌入訊號之強度，$0 < \alpha \le 1$。

2.2 版權浮水印偵測

本方法面對有侵權嫌疑之資料庫時，先利用原始資料庫和嫌疑資料庫進行資料交集(union)運算，排除嫌疑資料庫中與原資料庫沒有關係的值組，縮小偵測之值組範圍。再以原布林雜湊函數 $S(k, p, \theta)$ 過濾出有嵌入訊號之相對應值組，接著進行浮水印偵測。偵測浮水印的方式有兩種：一種是使用在影像浮水印常用之相似度(similarity)，另一種是以統計學中之關係係數(correlation coefficient)。第一種方式以原始值組中目標屬性值 d 與嫌疑資料庫中相對應屬性值 d' 來決定所擷取出之浮水印訊號 w'，w' 決定方式為

$$w' = \begin{cases} +1 & d' \ge d \\ -1 & d' < d \end{cases} \tag{3}$$

將各值組中之原嵌入訊號 $w=W(k, p)$ 與所擷取出之浮水印資料 w' 進行比對，以證明浮水印的存在性。當 w 與 w' 相同時，代表所取出的浮水印訊號和原始浮水印訊號正相關；當 w 與 w' 不同時，代表兩者負相關。兩組浮水印訊號之相關性 C 可表示為

$$C = \sum_{i=1}^{m} C_i = \sum_{i=1}^{m} w_i \times w_i' \tag{4}$$

其中 w_i 和 w_i' 分別代表第 i 個受偵測值組之原始浮水印訊號和所擷取出之浮水印訊號，m 代表受偵測之值組數。若受偵測之資料庫有嵌入版權浮水印，且 k 與 θ 選用正確時，則 C 值會為 m；若兩資料庫內之資料沒有關係，或是偵測用之 k 或 θ 不正確時，C 值理論上應會趨近於 0。Cox 等人所提出之浮水印之相似度(similarity)計算公式也可簡化為

$$Sim = \frac{\sum_{i=1}^{m} w_i \times w_i'}{\sqrt{\sum_{i=1}^{m} w_i' \times w_i'}} = \frac{C}{\sqrt{m}} \tag{5}$$

若是某識別碼產生之浮水印訊號之相似度值明顯高過於其他識別碼產生之浮水印訊號之相似度或設定之門檻值，則可以判定被偵測的嫌疑資料庫，其資料的來源為具此識別碼的資料庫。門檻值可以依據正確性和強韌性的需求，先設定適當的值組比例值 T_θ(百分比)，當值組中擷取出的浮水印正確之比例超過 T_θ，即可判定結果為明顯峰值，也就是確定有隱藏識別碼之浮水印訊號。當設定 T_θ 後，則其相對應之相似度門檻值可表示為

$$\frac{2m \times T_\theta - m}{\sqrt{m}} \tag{6}$$

其中 m 代表受偵測之值組數。第二種方法是以各值組之原始資料在嵌入浮水印時，屬性值之實際修改量，和嫌疑資料庫相對應原屬性值之差異量，利用統計學之相關係數表示浮水印訊號比對的結果。若某值組之原始屬性值為 d，嵌入浮水印後屬性值為 $d+\Delta$，資料修改量為 $\Delta = \alpha \times \delta \times w$；而偵測時，從被偵測的資料庫取出之屬性值為 d'，則與原始資料庫內屬性值之差異為 $\Delta' = d' - d$。集合所有嵌入浮水印的值組之 Δ 和相對應的 Δ'，會形成兩數列。相關係數的計算方式，是由兩數列之標準差(standard deviation)和共同變異數(covariance)相比之結果而得。相關係數之計算公式為

$$\rho = \frac{\sum_{i=1}^{m} \Delta_i \Delta_i' - \left(\sum_{i=1}^{m} \Delta_i \sum_{i=1}^{m} \Delta_i'\right) \Big/ m}{\sqrt{\sum_{i=1}^{m} \Delta_i^2 - \left(\sum_{i=1}^{m} \Delta_i\right)^2 \Big/ m} \sqrt{\sum_{i=1}^{m} \Delta_i'^2 - \left(\sum_{i=1}^{m} \Delta_i'\right)^2 \Big/ m}} \tag{7}$$

其中 m 為被偵測值組數。相關係數計算之結果會介於 1 到 −1 之間。若相關係數為正數，則稱兩數列存在正相關之關聯性；若為負值

則稱兩數列存在負相關之關聯性；若結果為零，則稱兩數列無關聯性。在統計上，若是 $|\rho| \geq 0.7$ 時為高度相關，而 $0.7 > |\rho| \geq 0.3$ 時為低度相關，$|\rho| < 0.3$ 時為無相關。因此，本方法之門檻值 ρ_θ 取介於 0.7 到 0.3 之值，以判定浮水印是否存在。

3. 無原始資料庫可供參考之版權保護

3.1 版權浮水印嵌入

在沒有原始資料庫可供參考之情況下，本論文所提出之浮水印嵌入步驟與有原始資料庫可供參考一樣，利用展頻概念，以主鍵或候選鍵為參考屬性。以使用者識別碼 k、修改值組比例 θ、值組之主鍵屬性之屬性值 p 進行雜湊運算以決定那些值組須嵌入浮水印訊號。各個值組所嵌入之浮水印訊號也仍是以識別碼 k 及參考屬性之屬性值 p 為參數之浮水印訊號產生函數 $W(\mathrm{k}, \mathrm{p})$，所產生之浮水印訊號為 $w = \{+1, -1\}$。

所不同的是浮水印訊號嵌入方法。假設欲嵌入浮水印之目標屬性之屬性值 d，令其可忍受之誤差範圍為 δ。本方法適當地調整 d 值，以 d 除以 δ 之餘數來代表所嵌入之浮水印訊號 w。如果所得之餘數大於或等於 $\delta/2$ 時，則代表所嵌入之 w 為+1；若餘數小於 $\delta/2$ 時，則代表所嵌入之 w 為−1。令調整後之 d 值為 d'，調整方式可表示為

$$d' = \begin{cases} d + \delta/2 & w = 1 \; and \; (d \bmod \delta) < \delta/2 \\ d - \delta/2 & w = -1 \; and \; (d \bmod \delta) \geq \delta/2 \\ d & else. \end{cases} \quad (8)$$

因為修改量並未超過其可忍受之誤差範圍，所以不影響資料之可用性。

3.2 版權浮水印偵測

在進行資料庫浮水印之偵測時，因為沒有原始資料庫可供參考，無法再以交集方式先剔除嫌疑資料庫中與原資料庫沒有關係之值組，但仍能以展頻概念，利用使用者識別碼 k、修改值組比例 θ、值組參考屬性之屬性值 p 進行雜湊運算以過濾出可能有嵌入浮水印訊號之值組。再由這些可能藏有浮水印訊號值組之目標屬性中，由其屬性值 d^*擷取出所嵌入之浮水訊號 w^*。擷取浮水訊號之方法可表示為

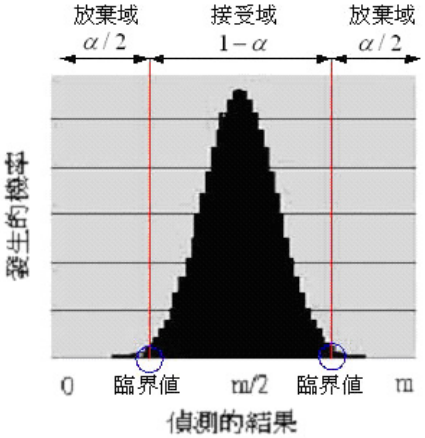
$$w^* = \begin{cases} +1 & if \; (d^* \bmod \delta) \geq \delta/2 \\ -1 & if \; (d^* \bmod \delta) < \delta/2 \end{cases} \quad (9)$$

擷取出之浮水印訊號 w^*與原應嵌入之浮水印訊號 w(以識別碼與參考屬性之屬性值，使用嵌入時之浮水印訊號產生函數得之)，再利用與前節之相似度計算方法比對。

本論文為了更精確設定門檻值，以判別所偵測結果是否為浮水印，因此將每筆值組比對之結果視為一次機率為 0.5 之柏努力試行(Bernoulli trails)，而總計 m 個值組比對之結果就是機率為 0.5 之二項機率分配(binomial probability distribution)或簡稱*二項分配*。機率為 0.5 之二項機率分配可表示為

$$P_{1/2}(m \mid n) = \binom{m}{n} (1/2)^n (1/2)^{m-n} = \frac{m!}{n!(m-n)!} (1/2)^m \quad (10)$$

其中 m 為比對之資料總筆數，n 為比對結果相符之資料筆數。本論文利用二項分配之機率空間，對浮水印訊號發生之機率，以所設定之顯著水準(level of significance) α，進行顯著性之檢定(test of significance)(如圖一)



圖一：在 m 筆值組中，檢定浮水印訊號之機率空間。

$$\begin{cases} H_0: & does\ not\ exist\ watermark\ \ signal \\ H_1: & exists\ watermark\ \ signal \end{cases} \quad (11)$$

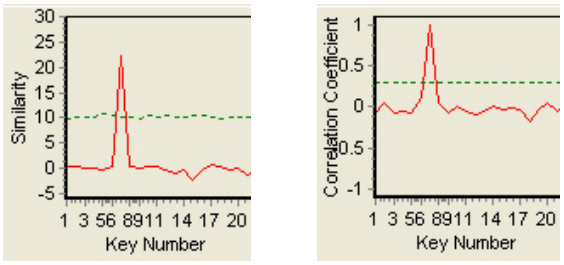
並以 $\alpha/2$ 計算出臨界值(critical value)，作為辨別浮水印訊號之門檻值。若此訊號發生之機率，落於接受域(accepted region)中，則檢定結果為接受 H_0 之假設，即認為此訊號不是合法之浮水印訊號。反之，如果落於拒絕域中，則檢定結果為拒絕 H_0 之假設，則認為此訊號為有效之浮水印訊號。若計算出結果認為可能為浮水印訊號，再利用計算 *p-value* 以了解誤判之機率。*p-value* 的計算方式為累計所偵測出的相符值組數為 n 之發生機率到所有值組 m 均相符之 n 所有發生機率，也就是

$$p-value=\sum_{x=n}^{m} b(x;m,\tfrac{1}{2}) = \sum_{x=n}^{m} C_x^m (\tfrac{1}{2})^x (1-\tfrac{1}{2})^{m-x} = \sum_{x=n}^{m} C_x^m (\tfrac{1}{2})^m \quad (12)$$

4. 實驗

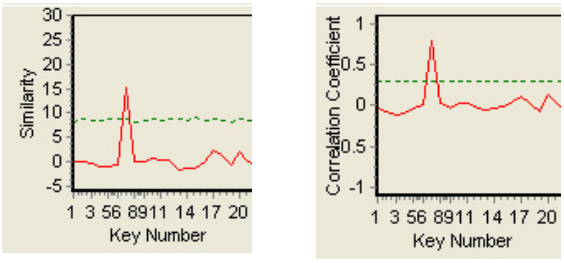
本研究以一個簡單的系統模擬測試所提方法。資料庫中建立了一萬筆值組之測試資料表，表內有兩項屬性 ID 和 DATA。ID 為主鍵屬性，其值不重複，而 DATA 之值為介於 0.00 到 99.99 之間的任意正數，取小點以下之第二位，做為可以容忍修改的部份，以嵌入浮水印訊號之用。實驗分無原始資料庫可供參考與有原始資料庫可供參考兩部份。無原始資料庫可供參考之實驗，是在資料庫中嵌入以識別碼 7、嵌入比例為 5%產生之版權保護訊號(圖二)。再連續以隨機刪除三千筆值組，新增三千筆不相干值組，最後在可容忍誤差範圍內任意修改三千筆值組之目標屬性的屬性值方式攻擊資料庫。資料庫被連續攻擊後之浮水印偵測結果(圖三)仍然可以看到明顯凸出之峰值，且相似度及相關係數結果都大於門檻值，故可證明本方法所嵌入浮水印之強韌性。

在有原始資料庫可供參考之實驗部份，同樣在具有一萬筆值組之資料庫中，先嵌入以識別碼 7、嵌入比例為 5%產生之版權保護訊號(圖四)，然後再進行連續之攻擊：隨機刪除三千筆值組、新增三千筆值組和在可容忍誤差範圍下任意修改三千值組之目標屬性之屬性值。由偵測之結果(圖五)可以看出，雖然相似度值下降，但仍有大於門檻值之峰值存在，因此可以證明所嵌入浮水印之強韌性。



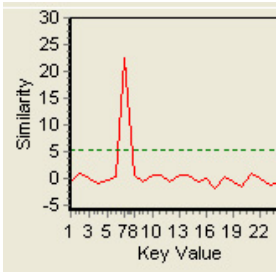
(a) (b)

圖二：在一萬筆值組之資料庫中嵌入識別碼 7 之浮水印後之偵測結果。(a) 相似度取 75%做為門檻值，(b) 相關係數取 0.3 做為門檻值。



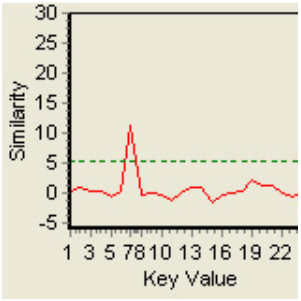
(a) (b)

圖三：資料庫被刪除、新增、修改連續攻擊後之浮水印偵測結果。(a) 相似度為 15.145，(b) 相關係數為 0.788。



圖四：在一萬筆值組之資料庫中嵌入識別碼 7

之浮水印，設定顯著水準 α=0.0000001 之偵測結果(相似度結果為 22.383，門檻值為 5.3，p-value 為 3.05×10^{-151})。



圖五：資料庫被刪除、新增、修改之連續攻擊後，以顯著水準 α=0.0000001 之偵測結果(相似度結果為 11.153，門檻值為 5.3，p-value 為 2.42×10^{-30})。

5. 結論

本論文利用資料本身可以容忍的誤差範圍，為個別的授權者嵌入專屬的浮水印，以證明資料庫的版權。本論文提出了有原始資料庫可供參考的資料庫版權保護方法，在偵測時除了可以比對正確的值組比例分析浮水印相似度外，更可以利用統計上計算相關係數的方式，來提高偵測浮水印之精確度。本論文也提出了沒有原始資料庫可供參考的資料庫版權保護方法，所偵測出浮水印可以利用假設檢定的方式進行浮水印分析，並以設定顯著水準 α 值的方式，控制誤判的可能性。

6. 致謝

本論文之部份經費為國科會計畫所支助，代號為 NSC93-2213-E-372-004 與 NSC94-2422-H-468-001。

7. 參考文獻

[1] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[2] I. J. Cox, Matthew L. Miller, Jeffrey A. Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers, 2002.

[3] D. Kundur and D. Hatzinakos, “Digital watermarking for telltale tamper-Proofing and authentication,” *Proceedings of the IEEE* (Special Issue on Identification and Protection of Multimedia Information), vol. 87, no. 7, pp. 1167-1180, July 1999.

[4] N. R. Wagner, R. L. Fountain, and R. J. Hazy, “The fingerprinted database,” *6th International Conference on Data Engineering*, pp. 330–336, 1990.

[5] Rakesh Agrawal, and Jerry Kiernan, “Watermarking relational databases,” *Proceedings of the 28th VLDB Conference*, Hong Kong, China, 2002.

[6] Rakesh Agrawal, Peter J. Haas, and Jerry Kiernan, “Watermarking relational data: framework, algorithms and analysis,” *The International Journal on Very Large Data Bases*, Vol. 12, Issue 2, August 2003.

[7] Radu Sion, Mikhail Atallah, and Sunil Prabhakar, ”Rights protection for relational data,” *IEEE Transactions on Knowledge and Data Engineering*, Vol. 16, Issue 12, 2004, pp. 1509-1525.

[8] R. Pickholtz, D. Schilling, and L. Milstein, “Theory of Spread-Spectrum Communications--A Tutorial,” *IEEE Transactions on Communications*, Vol. 30, Issue 5, pp. 855-884, May 1982.