

中國文化大學資訊管理研究所

碩士論文

檔案安全備份方法之探討



指導教授：李長彥
 蔡敦仁
研究生：鄭凱聰

中華民國 98 年 12 月

論文名稱：檔案安全備份方法之探討

總頁數：55

校(院)所組別：中國文化大學商學院資訊管理研究所

畢業時間及提要別：98 學年度第 1 學期碩士學位論文提要

研究生：鄭凱聰

指導教授：李長彥

蔡敦仁

論文提要內容：

為了確保檔案不會因為意外而損失，我們通常以備份的方式來防範，但是一般的備份方式僅僅是將檔案複製儲存到其它設備，並未考量備份後的檔案安全性和可能遇到的狀況，像是備份時磁碟空間不足、備份檔案可能遭到竊取等等。

本研究之目的在於提供一個分散式的備份方法，首先針對備份檔案的內容來建立紀錄表格，便於日後使用，接著加強備份時的安全性與機動性，我們將檔案或資料庫分割成數個範圍區，每個範圍包含記錄和區塊，加密後儲存到指定的各個磁碟中；當檔案執行新增、修改或刪除的操作時，我們只需要對有變動的範圍區檔案去做處理，這個備份方法的優點是可以帶來更高的安全性和更好的效能。

最後將此方法予以實作，設計程式去實際執行分散式備份的動作，使用不同的備份檔案去測試，觀察其效能記錄測試數據，以便日後評估改善方針與進一步的發展。

關鍵字：備份(backup)，分割(divide)，加密(encrypt)。

A Study of Secure File Backup Method

Student: Kai-Tsung Jheng

Advisor: Associate Prof. Tsang-Yean Lee

Associate Prof. Dwen-Ren Tsai

Chinese Culture University

ABSTRACT

Many companies use computer system to store files and process the applications. The files in the computer system may be destructed under abnormal condition. We must backup the files periodically. How to solve the large volume of data and security problem is our concern.

In this paper, we divide the file or database into several ranges. Each range contains records and fields. We backup ranges to different devices. When files process the operations of creation, insertion, update and deletion, we only backup the corresponding ranges. When the original file is destructed, we create it from the backup files.

For security, we have method to encrypt files before stored. These options of backup method make more secure and better performance.

Key word: backup, divide, encrypt.

誌 謝 辭

本論文能順利完成，首先要感謝恩師李長彥副教授對我的指導，不論是在論文內容還是程式設計上都給了我很有幫助的意見，每當論文完成一部分的時候，教授都會一一審視並給予修改和建議，真是辛苦了。

再來要感謝家人的支持，讓我在無後顧之憂的環境下作研究，感謝共同指導教授蔡敦仁博士和口試委員李中彥博士與陳武倚博士在口試中給予的建議，使論文能更加的充實。感謝好朋友阿彬、阿哲、宣凱在研究論文時給予的協助和幫忙。

完成這篇論文後，讓我學到了如何一步一步的作好研究，也希望將來能有更好的延伸發展。



內 容 目 錄

中文摘要	iii
英文摘要	iv
誌謝辭	v
內容目錄	vi
表目錄	viii
圖目錄	ix
第一章 緒論	1
第一節 研究動機	2
第二節 研究目的	3
第三節 研究範圍與限制	4
第二章 文獻探討	6
第一節 傳統檔案之備份考量	6
第二節 完全備份	7
第三節 依橫向區段來備份	7
第四節 依欄位縱向區段來備份	8
第五節 網格上的檔案備份	8
第六節 磁碟陣列備份(RAID)	8
第七節 一般備份軟體	9
第八節 資料庫備份軟體	10
第九節 密碼學	11
第十節 檔案系統	13
第十一節 分散式系統	18
第三章 研究方法	20
第一節 備份檔案的問題考量	20

第二節	檔案備份的方法描述	21
第三節	建立表格	22
第四節	加解密演算法	26
第五節	研究架構	29
第四章	系統實作	31
第一節	準備步驟	31
第二節	提供操作之方法	35
第三節	實作備份步驟	38
第四節	實作還原步驟	42
第五節	效能測試與比較	48
第五章	結論與未來發展	50
參考文獻		52



表 目 錄

表 2-1	常見的檔案類型	15
表 3-1	檔案資料表	22
表 3-2	檔案範圍表	23
表 3-3	範圍區表	23
表 3-4	範圍區大小表	24
表 3-5	範圍區磁碟表	24
表 3-6	檔案名稱表	25
表 3-7	範圍區控制資料表	25
表 3-8	RCIT內容表	25
表 3-9	範圍區檔案內容表	26
表 3-10	加密資料表	26
表 3-11	符號表	27
表 3-12	加密演算法使用的表格及長度	28
表 4-1	檔案資料表範例	31
表 4-2	檔案範圍表範例	32
表 4-3	範圍表範例	32
表 4-4	範圍區大小表範例	33
表 4-5	範圍區磁碟表範例	33
表 4-6	檔案名稱表範例	34
表 4-7	範圍區控制資料表範例	34
表 4-8	RCIT內容表範例	34
表 4-9	範圍區檔案內容表範例	35
表 4-10	加密資料記錄表範例	35
表 4-11	加密時的比較表	49

表 4-12 無加密時的比較表 49



圖 目 錄

圖 2-1	密碼系統示意圖	12
圖 2-2	分散式運算架構	19
圖 3-1	研究架構圖	30
圖 4-1	完全備份之設定畫面	39
圖 4-2	選擇是否加密之畫面	40
圖 4-3	選擇備份檔案之畫面	40
圖 4-4	顯示備份所花時間	41
圖 4-5	確認完全備份成功之畫面	42
圖 4-6	設定還原檔案儲存資料夾之畫面	43
圖 4-7	選擇索引檔之畫面	43
圖 4-8	還原完成顯示所花時間	44
圖 4-9	選擇要還原的檔案與筆數	45
圖 4-10	執行還原區塊之畫面	45
圖 4-11	顯示還原區塊所花時間	46
圖 4-12	單筆還原設定之畫面	47
圖 4-13	選擇索引檔之畫面	47
圖 4-14	顯示單筆還原成功時間	48