適用於醫療影像病歷快速簽章演算法之研究與實作

慈濟大學

指導教授：李添福 教授

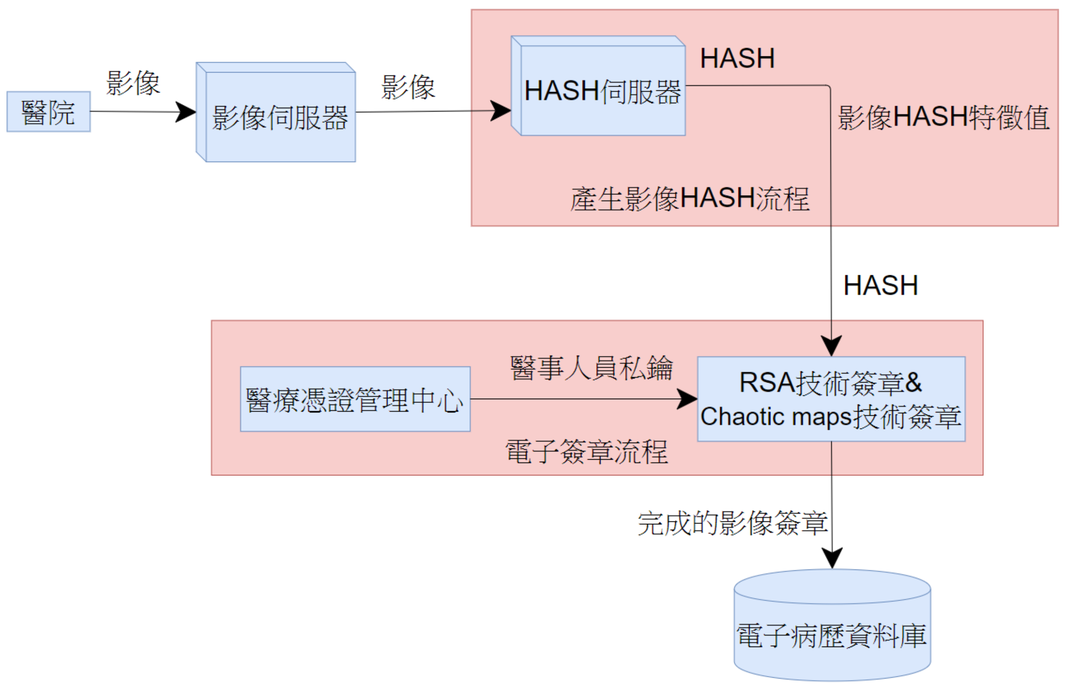
組員：蔡昀霖、李弘宇、田尚民

背景與目的

現在醫療技術愈來愈好，X光、CT、核磁、超聲波…等醫療器材，產生大量醫療影像，從一張到上千張，層層交疊的醫療影像，為了讓這些影像不被任意竄改，對這些醫療影像做簽章的動作是必要的，以確保這些醫療影像的擁有者及安全性。然而現階段的醫療影像簽章仍需要沉重的指數運算，為了使醫生在簽章上不要花太多時間，加速簽章之效率，讓醫療品質提升，是現今最需要探討的議題。

現今已有文獻證明利用混沌映射技術所開發的系統在運算效率上優於利用指數運算或橢圓曲線密碼技術所開發的系統。本專題計畫希望能針對醫療影像病歷內容與特徵進行分析與探討，利用chaotic maps簽章技術與現階段所使用之RSA簽章技術比較，發展一適用於醫療影像病歷之快速有效簽章演算法。

醫院簽章系統流程



Step 1 金鑰產生中心產生兩個亂數(rp, s)，利用切比雪夫產生私鑰及公鑰。

Step 2醫院將病患照射之醫療影像做儲存、整合，傳至影像伺服器。

Step 3將醫療影像做hash，取得hash特徵值。

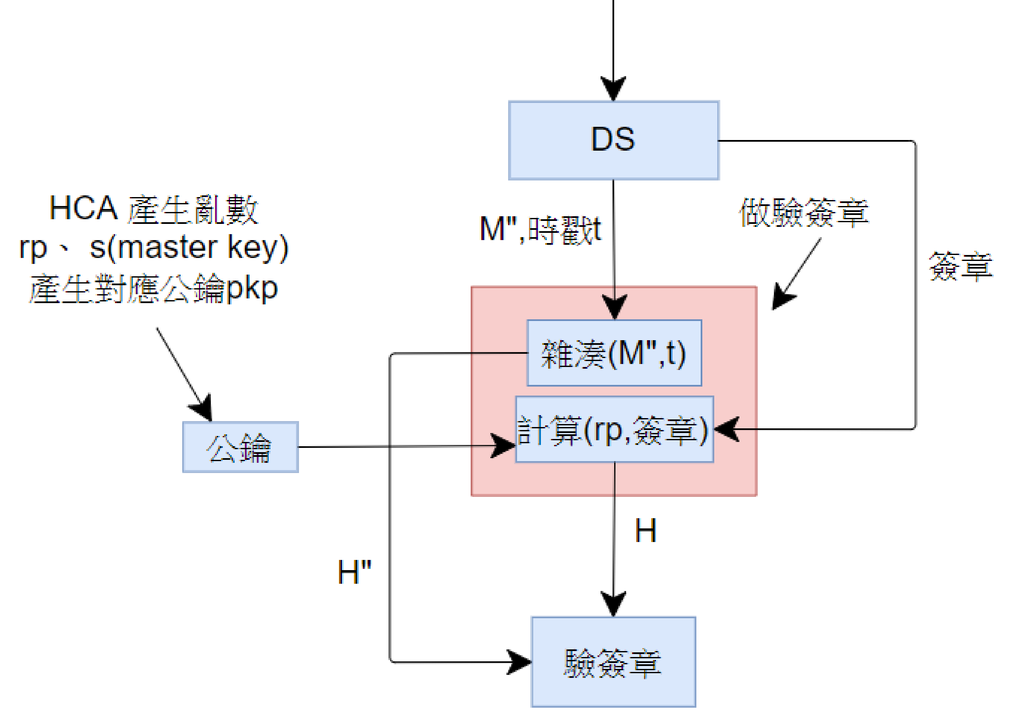
Step 4將醫療影像之特徵值取出。

Step 5從醫療憑證管理中心(HCA)或其他方法，取得醫事人員金鑰。

Step 6使用RSA或其他(chaotic maps)技術針對醫療影像之特徵值做簽章。

Step 7將影像簽章儲存並整合至電子病歷資料庫。

混沌映射簽章流程



(1)系統參數設定

(2)公/私金鑰產生

(3)醫療影像簽章

(4)醫療影像簽章驗證

開發環境與工具

1. 開發環境： Windows10、Visual studio 2012
2. 執行平台： PC
3. 簽章/驗簽章介面: C#語言
4. DICOM影像編輯及show出:Sante DICOM Viewer
5. 效能分析:Excel & Visual Studio內建

適用於醫療影像病歷快速簽章演算法之研究與實作

慈濟大學

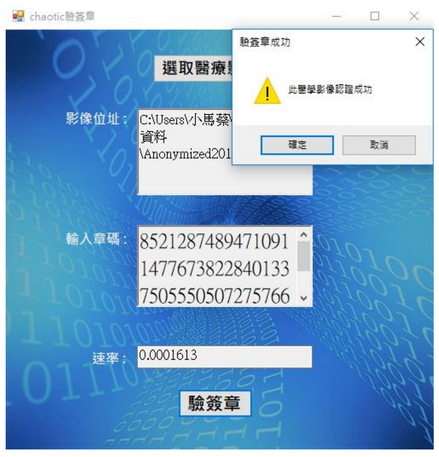
指導教授：李添福 教授

組員：蔡昀霖、李弘宇、田尚民

實作介面呈現

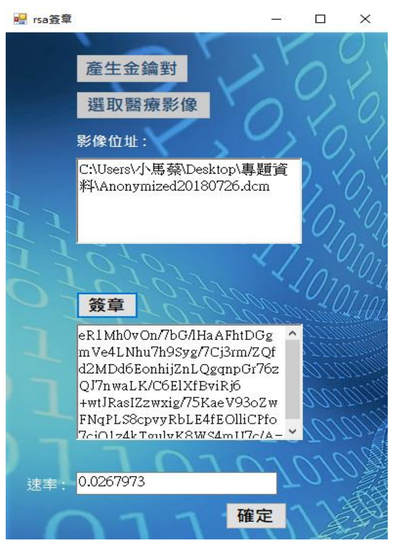
圖三:chaotic maps簽章介面

圖四:chaotic maps驗簽章介面



圖五:chaotic maps驗簽章成功

圖六:chaotic maps驗簽章失敗



圖七:RSA簽章介面

圖八:RSA驗簽章介面

圖九:RSA驗簽章成功

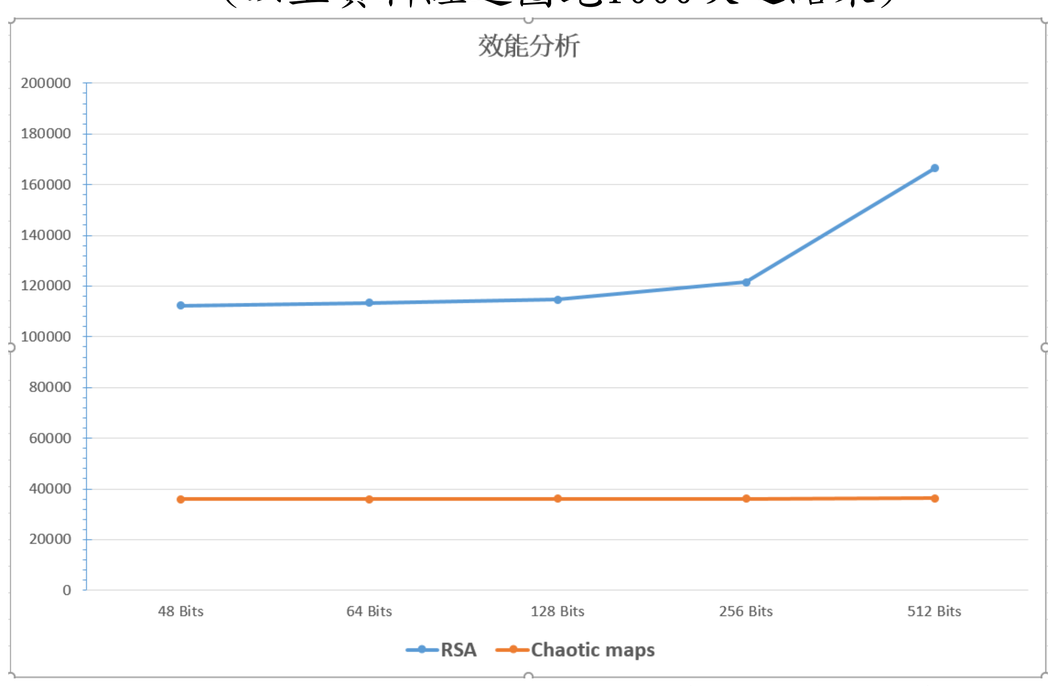
圖十:RSA驗簽章失敗

效能分析

分別以48-bits、64-bits、128-bits、256-bits、512-bits之key size去實測兩者簽章速率(如圖十一)，從折線圖(如圖十二)可以發現，對於醫療影像chaotic maps技術簽章之執行速率，遠遠超過RSA技術簽章之速率，這也證明chaotic maps技術簽章應用在醫院系統之影像簽章，效率高於現今醫院之傳統影像簽章。

	48 Bits	64 Bits	128 Bits	256 Bits	512 Bits
RSA	112316 ms	113450 ms	114716 ms	121552 ms	166387 ms
Chaotic maps	36005 ms	36013 ms	36175 ms	36210 ms	36253 ms

圖十一:chaotic maps&RSA醫療影像簽章速率分析
(以上資料經迴圈跑1000次之結果)



圖十二:效能分析折線圖(縱軸單位ms)

結論與未來展望

本專題計畫發展適用於醫療影像環境植基於混沌映射技術之簽章機制。透過理論上與實機測試的分析，所提之對於醫療影像之混沌映射技術簽章的確有其優越的效率及安全性。相較於現今醫療院所所使用之RSA簽章機制，在效率上所提簽章機制於醫療影像簽章的確有較優的表現。此也證實混沌映射技術應用在醫療影像上是可行的。

未來期望能夠將混沌映射技術簽章機制應用於現有醫療影像簽章，以及更進一步探討醫護人員對於醫療影像的多重標註簽章之應用，使醫療影像簽章技術能更具安全性與便利性，並更有效率。