適用於醫療影像病歷快速簽章演算法之研究與實作

指導老師：李添福教授
組員名單：田尚民、李弘宇、蔡昀霖

隨著時代改變，在台灣電子簽章法已立法通過，醫學界的病歷、診斷證明書、醫學影像等等數位化安全議題已漸漸受到重視。現階段電子病歷與醫療影像病歷之簽章(RSA)仍須依賴耗時之指數運算，然而醫療影像病歷為求清晰，往往為較大的檔案，與電子病歷檔案大小有著相當的差異。此外，醫療影像病歷內容與電子病歷文字檔案格式有著顯著的差異。在另外一方面，醫療影像病歷在特徵上又有別於一般影像。

近幾年，渾沌映射技術運算已被發現運算效能優於模指數或橢圓曲線點乘運算，並具有半群與交換率特性，及解離散對數特性，適合發展非對稱式之密碼系統。

本專題應用數位醫學影像的影像驗證機制分為二個部分: 第一部分是數位醫學影像擁有者的安全認證方面，利用傳統由 Rivest 、Shamir 及 Adleman 所提的 RSA 密碼系統來做為數位簽章。第二部分是使用 Chaotic 混沌映射的比特級數字圖像加密方法。

本專題的研究是以數位簽章證明該數位醫學影像擁有者和醫學影像的完整性，及對於大量醫院的病歷資料簽章，分析混沌映射技術及 RSA 技術之簽章效率，研究及實作適用於醫療影像病歷的快速簽章演算法。