封面格式

**國立臺北科技大學機械系專題製作成果四頁精簡報告**

（**智慧系統演算法開發**）

1、專題類別：□新創型專題　　□延續型專題

2、本版是否為最終版？請勾選 □是 □否

3、製作期間：110學年度第2學期至111學年度第1學期

4、指導老師姓名及職稱： 李仕宇副教授

5、指導老師簽名或蓋章處：

6、參與學生班級/姓名/學號：

機械四乙/張喻翔/109300219

機械四乙/賴群展/109300205

機械四乙/林柏帆/109300214

機械四乙/王致鈞/109300222

本實務專題製作依據（請勾選、可複選）：

□國科會計畫

□產學計畫

□業界需求

□參與競賽

□創新構想

□機械專業整合

□學碩一貫學程

繳交日期：中華民國110年 　月 日

**國立臺北科技大學機械系專題精簡報告**

**實務專題題目請置於此，是否需要英文名稱請與指導老師討論！**

製作期間：xx年x月x日至xx年x月x日

指導老師：李仕宇副教授

參與學生：

機械四乙/張喻翔/109300219

機械四乙/賴群展/109300205

機械四乙/林柏帆/109300214

機械四乙/王致鈞/109300222

**一、中文摘要**

本專題致力於深入研究混沌密碼學在資訊安全領域的應用，並評估其在數據保護方面的可行性、優勢和局限性。在當今數位化發展迅速的時代，資料的安全性和保護變得至關重要，這推動了加密技術不斷的發展。混沌加密法，作為一種新興的加密技術，具有對資料重新排列和擴散的能力。其高度複雜和無序的特性使其被稱為混沌算法，同時也因其對密鑰的參數靈敏度高而受到廣泛關注。混沌密碼學的研究不僅能夠加深我們對其在數據保護方面的理解，還有助於發現潛在的應用領域。本研究為開發加密演算法應用於手機通訊軟體並使用雲端伺服加密。我們期望本研究的結果能夠為資訊安全方面提供有力支持。**關鍵詞**：資訊安全、混沌演算法、雲端加密

**Abstract**

This research project delves into the application of chaos cryptography in the field of information security, assessing its feasibility, advantages, and limitations in data protection. In this era of rapid digitization, the security and protection of data have become paramount, driving the development of encryption technologies. Chaos cryptography, as an emerging encryption technique, possesses the ability to rearrange and diffuse data. Its highly complex and disordered nature has earned it the title of chaos algorithm, and it is highly sensitive to key variations, leading to extensive research in the past decade. Through an in-depth study and exploration of the application of chaos cryptography, this research aims to provide valuable insights and references for the establishment of more comprehensive and robust information security protection systems. The study of chaos cryptography not only deepens our understanding of its role in data protection but also aids in discovering potential application areas and addressing challenges existing in current encryption techniques. We anticipate that the outcomes of this research will contribute significantly to enhancing information security, ensuring the integrity and confidentiality of data in the digital environment.

**Keywords**:

information security、chaos algorithm、Cloud encryption

**二、緣由與目的**

因為大多數的加密軟體比較常在電腦上出現，所以才想實現在手機上做加密軟體。專題的目的是利用加密演算法結合手機的通訊軟體進行加密與解密的功能，可用手機將加密後的圖片傳送給對方以及獲得一組金鑰，且對方也可以使用這金鑰去解開加密的圖片，獲取解開後的清晰圖片°

**三、結果與討論**

因為此專題需開發一手機應用程式，以及使用一加套密演算法。所以這裡分兩組進行專題研究，一組為開發手機應用程式，主要使用android studio、Nodesjs；一組為研究演算法加密，主要使用matlab。

演算法研究的初期，著重在混沌演算法；混沌系統是一種將一系統模式化之後得出的數學模型，藉由不同的輸入參數會使得整體相對應的輸出會有所不同，在探討動態系統中無法用單一的資料關係，而必須用整體，連續的資料關係才能加以解釋及預測之行為。

之後我們找到一偏論文能夠能快速進行加密彩色圖片，此論文的主軸加密算法為3D Modular Chaotic Map(3DMCM)，主要是利用矩陣將原圖片的灰度值從一空間映射至另一空間使得像素位置被改變。而我們使用3DMCM類似的加密方式，從原本為從一空間映射至另一空間改為使用矩陣運運算將圖片像素位置做交換打亂的動作。

我們修改後的加密方式是先將清晰的彩色圖片拆解成分別為紅、藍、綠三種顏色的灰度圖，接著再以灰度圖的亮度由淺至深化為0至255的灰度級，再利用混沌演算法將像素值打亂，再利用3DMCM將像素的位置做打亂即可得出加密圖片。

手機軟體設計的部分，從原本的簡易預設專案中，開發出了需多功能，包括Fragment、RecyclerView、MediaPlayer、Service、BroadcastReceiver、HTTP通訊協定等等。剛開始觸碰android studio時，其實對所謂的手機設計概念完全不熟，尤其是對MVC的架構。設計一個頁面的過程很艱辛，還需要了解manifest、gradle是如何建構出整體架構的，對元件的屬性、特性也要一一摸熟，接者為了實現選取照片，需要透過系統自帶的file system(為content開頭的URL)呈現照片實體內容，接著會對照片的數據做處理，像是傳送至後端計算、前端呈現、資料庫存放等等，其中還使用WebSocket的技術來確保前後端的連線，這邊有牽扯到使用者的連線狀態，如果只要一方中斷，就更新Database中的登入狀態，並以Boolean來實現。

在這個手機設計中，我認為最困難的點在於要遵守TCP/IP的協定來傳送資料，專題中就是以HTTP的方式來傳送照片，實現方式以multipart/form-data的結構、格式完成並傳送至後端處理，並且等待Response，這邊有為了考慮照片處理時間而設定了Timeout以避免超時發生錯誤。

後端的部分是利用Nodejs的環境來實現並以Express框架去撰寫整體架構，同時使用框架下附贈的Router去寫API的部分給前端呼叫並Access data。

我們將Matlab也當作是一個Server，當後端傳過來需要加密的照片時，利用設計好的加密演算法，再透過Matlab平行運算將多張圖片做加密，這邊就有用到一個技術是Parallel Pool，可以比喻為有許多待工作的Worker，一但有任務進來，就會由系統分配工作給它們，而實際的技術是以Threads或Processes實現，而這次專題是用Processes為基礎，因為這樣Worker之間才不會因為太多任務而阻塞另一個正在進行加密的Process。

我們利用Google開發的GCP平台去實現Cloud server，在這次專題中租借了一台主機拿來做資料處理、運算，其實現方式是以三個Server，分別為Matlab Server和Backend Server以及MySQL Server，個別為獨立的Instance，所以並不會因為某一個Server阻塞而互相影響，它們擁有獨立的記憶體資源。另外有用到UUID的技術來區分出使用者資料以及新增排隊系統來分配資源，如此一來就不會一瞬間給Server太大的壓力以至於阻塞整個行程，同時也能依序的平行傳送結果給前端，一舉兩得!

**四、計畫成果自評**

專題內容:尋找一篇與加密演算法相關的論文，並使用Matlab實現混沌算法與此論文中演算法做結合得出創新的加密與解密方法，使用Android Studio製作手機app，透過雲端伺服器將Matlab與Android Studio做一個連接，實現在手機上加密完成並傳送給對方。

達成預期目標情況:完成在手機上將圖片加密後傳送給對方，並且對方可以使用密鑰解開加密圖片。

自評:

**五、參考文獻**