

3D 模型嵌入技術之研發與實作

系所／資訊工程學系

指導老師／李遠坤

組員／陳璋民、李正倫、趙俊彥、林志謙

智慧型手機的普及，使通訊 App 成為人們溝通的主要媒介。不論是朋友間的閒話家常、或是工作上的業務往來，幾乎都可以透過通訊 App 完成，導致通訊軟體公司掌握所有傳遞的內容。

機密訊息如果未經加密就進行傳遞，將有洩密的風險。然而密文(ciphertext)的不可閱讀性，使得密文傳送將秘密通訊的行為暴露無遺，在某些情況下，常使通訊人員身陷險境。

為了解決上述問題，可以使用數位媒體來掩護密文的傳送，如將密文隱藏在風景圖中，第三者將無法得知有訊息隱藏在其中，而只認為是單純的圖片傳輸。本研究將研發出能在 iOS 行動裝置上進行加密及隱藏訊息的 App，利用

密碼學 (cryptography) 與隱寫學 (steganography) 的技術，將訊息加密後隱藏在掩護媒體(cover-media)當中，藉由傳送偽裝媒體(stego-media)來進行秘密通訊，保護通訊人員的安全。

圖 1 為隱寫流程圖。首先，圖中左方的傳送者使用接收者的公開金鑰 (public-key) 對訊息進行 RSA 加密。接著，選擇一個 3D 模型作為掩護媒體後，透過嵌入金鑰(embedding-key)將密文嵌入其中。最後就可以把嵌有機密訊息的偽裝 3D 模型透過通訊 App 傳送給接收者。圖中右方的接收者收到偽裝 3D 模型後，首先使用同一把嵌入金鑰萃取出密文，接著使用私密金鑰 (private-key) 進行 RSA 解密，即可得到所傳送的訊息。

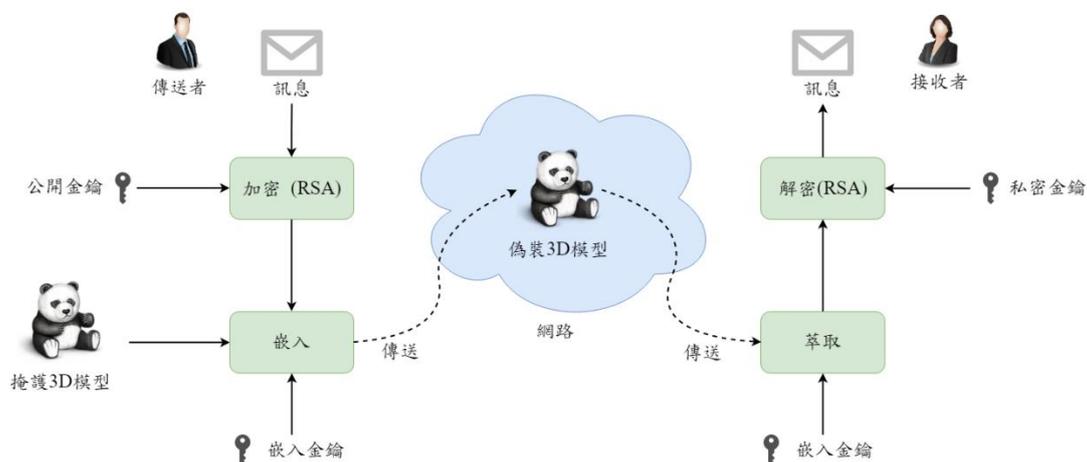


圖 1：隱寫流程圖