基於數位浮水印的 QR Code 驗證系統

林祝興 吳文琛 東海大學資訊工程系

摘　　要

QR Code (Quick Response Code) 是二維條碼的一種，於 1994 年由日本 Denso Wave 開發而來，初期用於汽車工業生產線。1999 年獲得日本工業規格標準 JIS X 0510，又於 2000 年時獲得國際 ISO 標準的 ISO/IEC18004。近年來因為手持式裝置愈來愈普及，QR Code 除了在工業生產線上，也適合一般個人使用者。

因為採用了 Reed-Solomon error correction，QR Code 有容錯的特性，若不慎遇到輕微 (7%~30%) 破損或髒汙的情況下，透過糾錯技術仍能順利讀取資料。

然而，QR Code 有許多潛在的危險，一般使用者不假思索地掃描來路不明之 QR Code 可能造成設備被入侵，或是遭受釣魚式攻擊 (Phishing) 等等問題。

由於 QR Code 有完善的糾錯能力，因此可以利用此特性嵌入浮水印以隱藏驗證資訊。如此一來，使用者掃描了傳統的 QR Code 之後，可透過浮水印中的隱藏資訊驗證此 QR Code 是否來自受信任的發布者，以降低在不知情的情況下掃描到惡意 QR Code 所帶來的風險。

然而最大的挑戰為：嵌入的浮水印同時也必須能抵抗印刷、掃描的破壞。

關鍵詞：QR Code、Reed-Solomon、Error Correction、Watermark

QR Code Authentication System Based on Digital Watermarking

Chu-Hsing Lin, Wen-Chen Wu, Dept. of Computer Science, Tunghai University

ABSTRACT

QR Code (Quick Response Code) is one of the widely used two-dimensional matrix barcode developed in 1994 by Denso Wave Japan, it was adopted in automotive industries in the early days. In 1999 QR Codes are approved as JIS (Japanese Industrial Standards) X 0510, and approved as ISO/IEC18004 standard in 2000. Despite the use in industries, QR Codes are also suitable for consumers, since mobile devices are more and more popular these days.

QR Codes are designed to be fault tolerant by adopting Reed-Solomon error correction, QR Codes with minor damages (7%~30%) should still render readable with the help of error correction.

However, there are many potential risks while scanning a specially designed malicious QR Code without users' knowledge. This may result the device being compromised, or the user may face Phishing attacks by using social engineering tricks.

QR Codes have good capability of fault tolerance, it is possible to use this particular characteristic to embed watermarks for the use of validation. With the proposed method, the system can validate if the QR Code is from a trusted source when users scan their QR Codes by reading the embedded watermark, so it is possible to reduce the risk of scanning malicious QR Codes without knowledge.

The biggest challenge is that embedded watermarks should be able to survive under the damage done by printing and scanning.

Keywords：QR Code、Reed-Solomon、Error Correction、Watermark

1. 簡介

由於 QR Code 在一般使用者之間愈來愈普及，因此各式惡意攻擊也開始出現。使用者可能在不知情的情況下掃描了惡意製作或被竄改過的 QR Code，導致裝置被入侵，目前已經有數個案例出現。

其中一例部分廠牌的 Android 手機掃描嵌入了惡意 USSD (Unstructured Supplementary Service Data) 指令或 MMI 指令的 QR Code 後不需經過使用者確認，直接送出 USSD 或 MMI 指令。〔**1**〕USSD 為手機與電信商雙向即時通訊的一種 GSM 協定，可提供各式服務，例如：手機付款、預付卡儲值、……等服務，若被惡意執行，可能造成使用者財務損失。除了 USSD 指令以外，各家手機廠商也會自訂特別的 MMI 指令，以提供一些進階手機功能。因此執行了惡意 MMI Code 後，可能導致系統被還原原廠設定、使 PIN 碼甚至是 PUK 碼失效、……等問題，這些問題存在 Android 4.1 (Jelly Bean) 及之前的版本。雖然此事件根本的漏洞不是在 QR Code 本身，而是部分廠商的系統設計問題。〔**2**〕但倘若 QR Code 本身提供驗證機制，則可以避免掃描到此類惡意製作的 QR Code 所帶來的問題。

而近期推出的 Google Glass 也出現了與 QR Code 相關的系統漏洞，Google Glass 提供了透過掃描 QR Code 自動設定 WiFi 網路的功能，然而此功能雖然看似方便，但未經使用者同意自動切換 WiFi 網路是非常危險的事情。直到 2013 年 6 月推出的 Glass XE6 新版韌體更新才改為在使用者主動要求設定 WiFi 時才啟動掃描 QR Code 切換無線網路的功能。

除了手持式裝置，IoT (Internet of Things)裝置與穿戴式裝置也愈來愈普及，以上的 Google Glass 即為此例。由於未來愈來愈多裝置具備掃描 QR Code 的功能，應用也愈來愈廣泛，因此設計上的疏忽可能會產生一些意想不到的漏洞，若 QR Code 能提供驗證發行者的功能，將可大幅降低隨意掃描 QR Code 可能帶來的風險。

2. 相關文獻

2.1 QR Code 基本介紹〔1〕

QR Code 除了早期的汽車工業相關應用之外，現今也延伸到個人使用的領域。隨處可見的海報、產品型錄、皆可看到 QR Code 的蹤影。

由於手機的數字鍵盤或虛擬鍵盤對於輸入網址等其他資訊較不便，因此 QR Code 在手機上的應用可以解決輸入緩慢的問題，只需掃描條碼即可取得資訊。

與手機相關的應用則包括掃描連結到網址、設定 WiFi 網路、交換 vCard 名片、掃描條碼登入網站……等等各式各樣的應用。

QR Code 的 Reed-Solomon 糾錯系統提供四種等級的容錯率可選擇，由低而高分別為：L、M、Q、H。此資訊儲存在 Format Information 區塊中。〔**3**〕

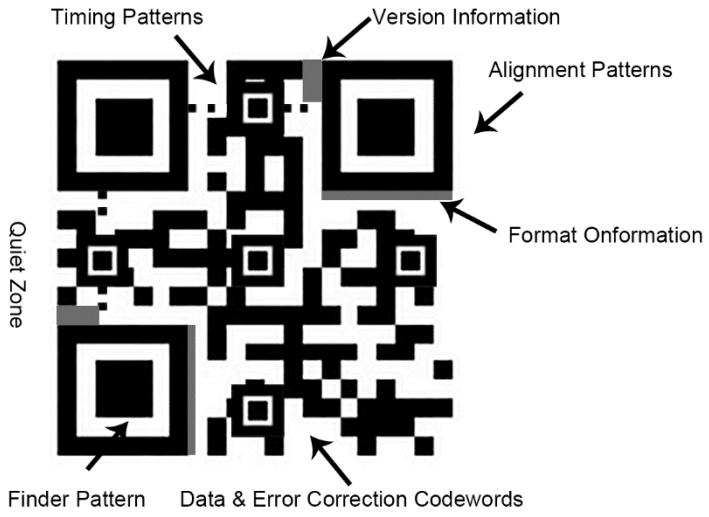

圖 1.QR Code 基本結構

2.2 Reed-Solomon Error Correction

Reed-Solomon Codes 是一種錯誤校正機制，由 Irving S. Reed 和 Gustave Solomon 於 1960 年提出。廣泛應用在網路傳輸、衛星資料傳輸、光碟儲存裝置、RAID 6 磁碟陣列、以及條碼掃描的錯誤校正上，它可以用來偵測並修復資料傳輸過程中或讀取時所發生的錯誤。〔**4**〕

2.3 數位浮水印

傳統浮水印最早在 13 世紀的義大利就已出現，而現今的數位浮水印可應用於智慧財產權保護、數位簽名，可套用在影像、影片、音訊、……等數位媒體上。

除此之外，Steganography 也是一種數位浮水印的應用，將訊息藏匿在 Cover Message (偽裝訊息)中，使第三者無法輕易察覺到隱藏的訊息，提供了比單純加密多一層的保護。

數位浮水印以可見度可分為兩類，可視浮水印(Visible Watermark)與不可見浮水印。〔5〕若隱藏在浮水印中的資訊與使用者所見的圖形無法分辨，則稱為不可視浮水印；若圖形與隱藏的資訊可輕易地辨別出來則稱為可視浮水印，如：論文上的校徽圖形浮水印、電視台的頻道 Logo 浮水印、紙鈔上的防偽浮水印。

數位浮水印可分為強韌型浮水印(Robust Watermark)、易碎型浮水印(Fragile Watermark)及半易碎型浮水印(Semi-Fragile Watermark)。

強韌型浮水印可抵抗攻擊、破壞，由於其適合保留痕跡作為證據的特性，常用於著作權保護、DRM (Digital Rights Management)上；相反地，易碎型浮水印只要稍經修改即被破壞，可用於偵測文件或圖片是否遭受竄改。〔6〕

影像、視訊、音訊經數位化後可轉至空間域(Spatial Domain)或頻率域(Frequency Domain)，若要增強強韌性則需要將資料由空間域轉換到頻率域，有以下幾種方式：FFT(Fast Fourier Transform)、DCT(Discrete Cosine Transform)、DWT(Discrete Wavelet Transform)、……等等〔7〕〔8〕〔9〕〔10〕，本論文採用 DWT 轉換。

Discrete Wavelet Transform(離散小波轉換)將影像從空間域轉換到頻率域，人眼對低頻

敏感。首先水平分割影像，由左而右取影像中左右相鄰的兩像素相加、相減；接著垂直分割，由上而下取影像中上下相鄰的兩像素相加、相減，將影像分割為 4 個不同頻率的頻段：LL1、HL1、LH1、HH1，接著取低頻的 LL1 再切割為第二階的 LL2、HL2、LH2、HH2，如此不斷地重複直到第 n 階。

3. 研究方法與實驗環境

由於 QR Code 的惡意攻擊愈來愈多，因此設計了此解決方案。本計畫以浮水印的方式將隱藏驗證資訊於 QRCode 中，透過程式驗證後，使用者可藉此確認 QRCode 是否來自可信任的發行者，屬於 Owner Identification 技術，以降低掃描到惡意 QR Code 所帶來的風險。

本章節介紹論文所使用的研究方法，即嵌入浮水印至 QR Code 以及從 QR Code 取出浮水印並驗證之過程。

程式以 Python 搭配科學運算套件 SciPy 及 NumPy 撰寫，在 64 位元版本的 Ubuntu 14.04 作業系統中執行，編碼浮水印條碼；解碼則由 Android 手機上的主鏡頭拍攝後交由以 JAVA 撰寫的程式處理，其中 QR Code 解碼使用 ZXing Library。

編碼環境 CPU 規格為：Intel Core i7-3770、GPU 規格為：NVIDIA 650 Ti、8GB RAM。

首先使用 Windows 系統下的 Psytec QR Code Editor 軟體產生 QR Code，使用 Plain Text 模式，內文為：Hello World、錯誤校正的等級設定為 High(30%)、Version 設定為 5，產生的 QR Code 解析度為 225×225 px。

圖 2. 使用 Psytec QR Code Editor 產生 QR Code

產生出來的 QR Code 以手機掃描，可讀取 QR Code 中編碼的 Hello World 字串。

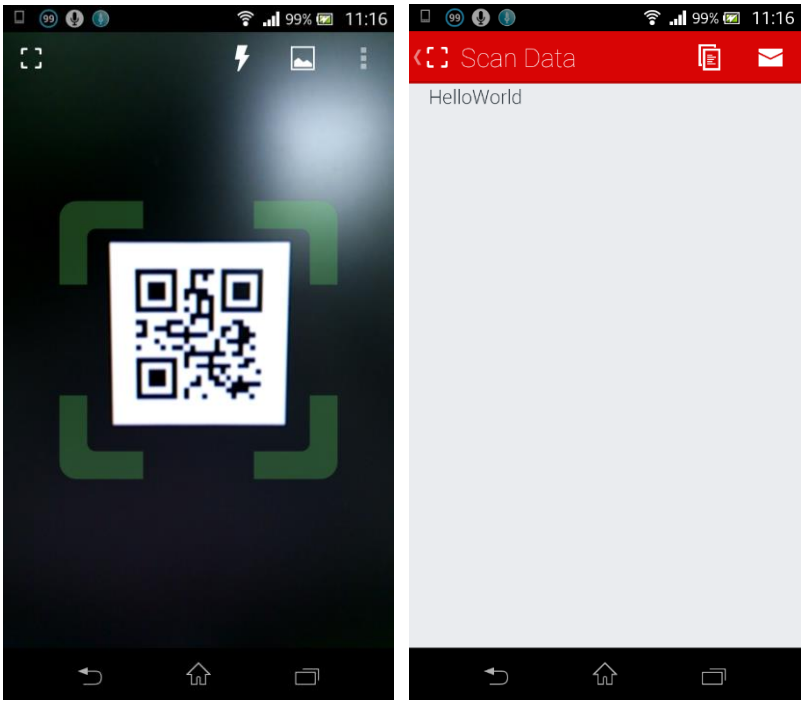

圖 3. 左圖為掃描 QR Code 之畫面，右圖為 QR Code 掃描結果

本實驗採用頻率域的 DWT (Discrete Wavelet Transform)嵌入浮水印，由於需要將 QR Code 印刷成紙本，再經由相機掃描，如此會被雜訊影響，因此不適合採用 Spatial Domain(空間域)嵌入，而 DFT(離散傅立葉)轉換可存放隱藏浮水印的頻段太少，不適合本實驗的需求。為了解決以上問題，最後選擇使用 DWT 嵌入。

手機端讀取 QR Code 中的 Hello World 訊息後，接著取出浮水印中的驗證訊息，經比對若與原發布者相同，即完成驗證步驟。

4. 實驗結果

以下為本實驗運作的流程圖：

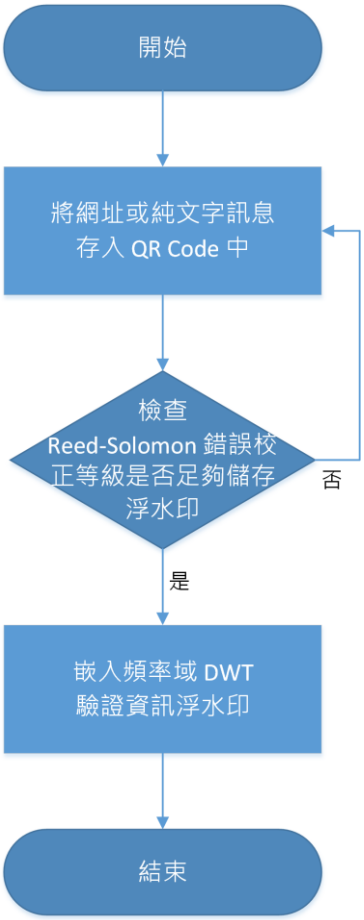

圖 4. 電腦端嵌入 QR Code 流程圖

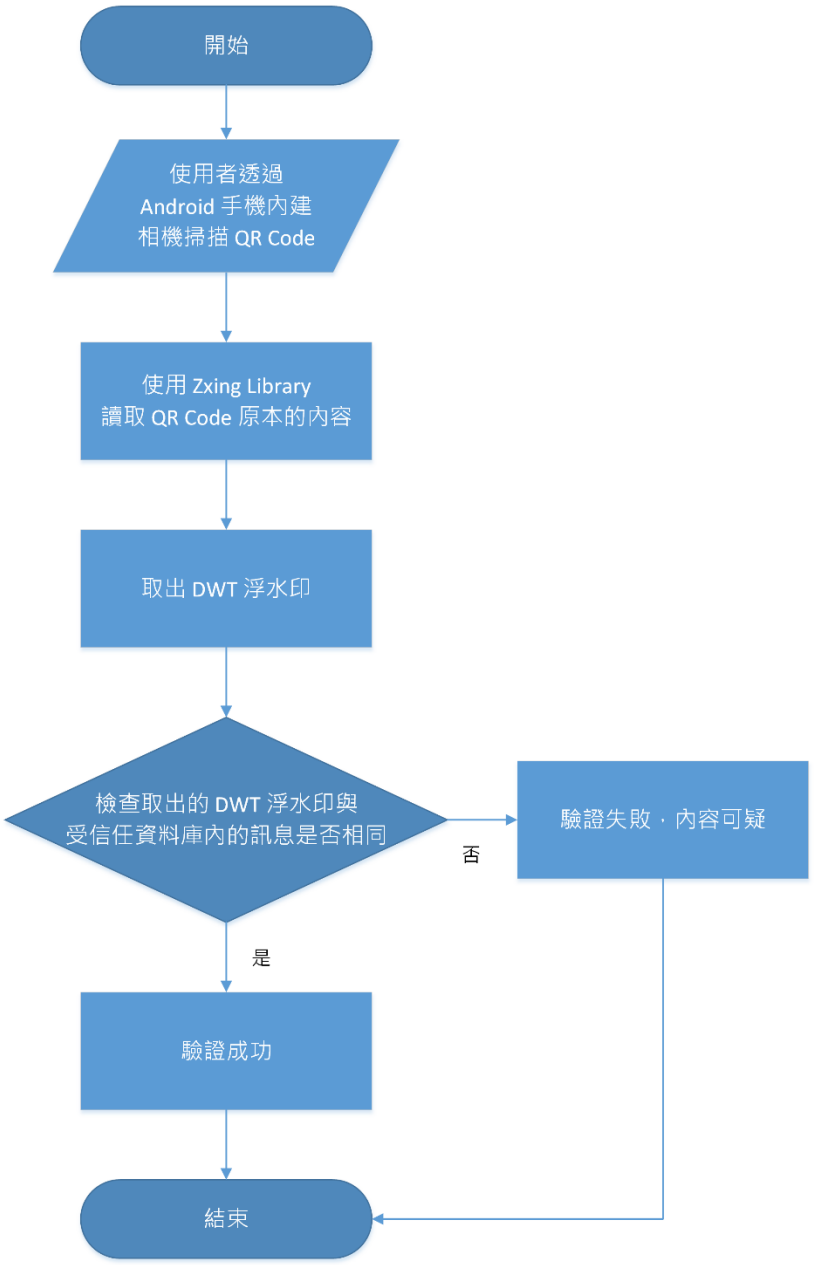

圖 5.　手機端取出 QR Code 浮水印流程圖

經過以上的測試，純文字 Hello World 的 QR Code 以 DWT 嵌入浮水印後由手機拍攝仍可讀取原本 QR Code 中的內容，即：Hello World。而其中的驗證訊息抽取出後可確保該 QR Code 為信任者所發行，且未經竄改過。

表 1. 原始與嵌入隱藏浮水印驗證訊息後的 QR Code

原始 Hello World QR Code	嵌入驗證資訊後的 QR Code
	

5. 結論

本論文將傳統的 QR Code 結合了浮水印驗證機制，確保掃描的條碼來源是可靠的。採用不可視浮水印嵌入驗證資訊比起直接將驗證資訊加在原始 QR Code 內容中有以下好處：不會讓使用者或入侵者起疑、提供更好的相容性。

由前人提出的 DWT 浮水印嵌入可解決印刷、掃描使嵌入的浮水印經過拍攝造成變形或模糊……等等失真、受損的問題。採用此種改良過的 DWT 浮水印搭配 QR Code 原有的糾錯功能可成功完成驗證工作。〔**11**〕〔**12**〕〔**13**〕〔**14**〕〔**15**〕〔**16**〕〔**17**〕

而未來若需要更進一步地提升安全性，則可結合數位簽章。如此就算驗證資訊浮水印被有心者發現並抽取出來嵌在其惡意製作的 QR Code 上，經過軟體掃描後也不會通過驗證。

參考文獻

1. R. Borgaonkar, "Dirty use of USSD codes in cellular networks", Mar, 2013.
2. C. Woo Bong, H. Keon il, L. Won Gyu, P. Won Hyung, and C. Tai Myoung, "The New Vulnerability of Service Set Identifier (SSID) Using QR Code in Android Phone", in Information Science and Applications (ICISA), International Conference on, 2011.
3. ISO, "IEC 18004: 2006", Information technology.“Automatic identification and data capture techniques. Bar code symbology, QR code, Sep, 2006.
4. I. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields", Journal of the Society for Industrial and Applied Mathematics, vol. 8, 1960.
5. A. Z. Tirkel, G. Rankin, R. Van Schyndel, W. Ho, N. Mee, and C. F. Osborne, "Electronic watermark", Digital Image Computing, Technology and Applications, 1993.
6. I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital watermarking and steganography: Morgan Kaufmann, 2007.
7. A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, vol. 90, Mar, 2010.
8. S. Vongpradhip and S. Rungraungsilp, "QR code using invisible watermarking in frequency domain", in ICT and Knowledge Engineering (ICT & Knowledge Engineering), 2011 9th International Conference on, 2012.
9. S. Rungraungsilp, M. Ketcham, and P. Surakote, "Data Hiding Method for QR Code Based on Watermark by comparing DCT with DFT Domain", in International Conference on Computer and Communication Technologies (ICCCT'2012), 2012.
10. V. Kumar and D. Kumar, "Performance evaluation of DWT based image steganography", in Advance Computing Conference (IACC), 2010 IEEE 2nd International, 2010.
11. M. W. Islam and S. AlZahir, "A novel QR code guided image stenographic technique", in Consumer Electronics (ICCE), 2013 IEEE International Conference on, 2013.
12. A. Keskinarkaus, A. Pramila, and T. Seppänen, "Image watermarking with feature point based synchronization robust to print–scan attack", Journal of Visual Communication and Image Representation, vol. 23, 2012.
13. C. Culnane, H. Treharne, and A. T. S. Ho, "Authenticating Binary Text Documents Using a Localising OMAC Watermark Robust to Printing and Scanning", in Digital Watermarking. vol. 5041, 2012.

14. A. Pramila, A. Keskinarkaus, and T. Seppänen, "Toward an interactive poster using digital watermarking and a mobile phone camera", Signal, Image and Video Processing, vol. 6, Jun, 2012.
15. K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, and I. El-Khalil, "'Print and Scan' Resilient Data Hiding in Images", Information Forensics and Security, IEEE Transactions on, vol. 1, 2006.
16. S. Pholsomboon and S. Vongpradhip, "Rotation, scale, and translation resilient digital watermarking based on complex exponential function", in TENCON 2004. 2004 IEEE Region 10 Conference, Vol. 1, 2004.
17. W.-C. Wu, Z.-W. Lin, and W.-T. Wong, "Application of QR-Code Steganography Using Data Embedding Technique", in Information Technology Convergence. vol. 253, 2013.